

INTERNÁ SMERNICA č. 1/2018

prevádzkovateľ'a

KOVOHUTY SK s.r.o.

Československých tankistov 2/C, 841 06 Bratislava

IČO: 44 015 747

zast. konateľom Ing. Eduardom Hanuskom

k ochrane osobných údajov pre

INFORMAČNÝ SYSTÉM:

LIKVIDÁCIA DOKUMENTOV S OBSAHOM OSOBNÝCH ÚDAJOV

v SÚLADE S NARIADENÍM EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej aj „nariadenie“, „GDPR“)

a ZÁKONON 18/2018 Z. z. z 29. novembra 2017 o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj „zákon“).

OBSAH

PRVÁ ČASŤ Opis spracúvania osobných údajov

- Článok I** Názov spracovateľskej činnosti
- Článok II** Účel spracúvania
- Článok III** Právny základ spracúvania
- Článok IV** Dotknuté osoby pri spracúvaní
- Článok V** Rozsah osobných údajov
- Článok VI** Prijemcovia
- Článok VII** Obdobie spracúvania
- Článok VIII** Funkčný opis spracovateľskej operácie
- Článok IX** Identifikácia aktív
- Článok X** Kódex správania

DRUHÁ ČASŤ Analýza rizík

- Článok I** Riziká v objektovej bezpečnosti
- Článok II** Riziká v dokumentárnom informačnom systéme
- Článok III** Riziká v automatizovanom informačnom systéme
- Článok IV** Zvyškové riziká

TRETIA ČASŤ Primerané bezpečnostné opatrenia

- Článok I** Technické opatrenia
- Článok II** Personálne a organizačné opatrenia
- Článok III** Opatrenia k zabezpečeniu práv dotknutých osôb

ŠTVRTÁ ČASŤ Prílohy

- Príloha č. 1** Kódex správania
- Príloha č. 2** Záznamy o spracovateľských činnostiach
- Príloha č. 3** Poučenia oprávnených osôb
- Príloha č. 4** Záznam o bezpečnostnom incidente
- Príloha č. 5** Záznam z kontrolnej činnosti prevádzkovateľa

PRVÁ CAST

Opis spracúvania osobných údajov

Článok I

Názov spracovateľskej činnosti

Názov spracovateľskej činnosti resp. názov informačného systému je: Likvidácia dokumentov s obsahom osobných údajov (ďalej aj „IS“).

Článok II

Účel spracúvania

Účelom spracúvania osobných údajov je zabezpečenie likvidácie skartovaním sprievodnej dokumentácie RTG snímku obsahujúcich osobné údaje - výmenné lístky, obálky a iné sprievodné dokumenty.

Článok III

Právny základ spracúvania

Právnym základom spracúvania je zmluva s poskytovateľom osobných údajov.

Článok IV

Dotknuté osoby pri spracúvaní

Dotknuté osoby pri spracúvaní osobných údajov sú pacienti poskytovateľa osobných údajov.

Článok V

Rozsah osobných údajov

Osobné údaje sú prevádzkovateľom spracúvané v tomto rozsahu: meno, priezvisko, adresa bydliska, rodné číslo.

Článok VI

Príjemcovia

K osobným údajom v informačnom systéme majú prístup len tieto oprávnené osoby:

Ing. Eduard Hanusek, konateľ

Karol Písařík, skladník

Osobné údaje z informačného systému sa neposkytujú iným príjemcom (sprostredkovateľom, tretím stranám).

Článok VII

Obdobie spracúvania

Osobné údaje sa spracúvajú odo dňa získania osobných údajov po dobu potrebnú na zabezpečenie účelu spracúvania, max. 30 kalendárnych dní.

Článok VIII

Funkčný opis spracovateľskej operácie (schéma)

Získavanie
dokumentov s
osobnými údajmi
od
prevádzkovateľa

Uchovávanie
uloženie
dokumentov
s osobnými údajmi
na max. 30 dní



Likvidácia
skartácia
dokumentov
s osobnými údajmi

Osobné údaje pri týchto spracovateľských činnostiach sa spracúvajú neautomatizovanými prostriedkami spracúvania.

Článok IX

Identifikácia aktív

Neautomatizované aktíva (papierová podoba listín):

- výmenné lístky, obálky a iné súvisiace listiny zapečatené a uložené v nepriehľadných plastových vreciach.

Článok X

Kódex správania

Zavádzajú sa primerané politiky (kódex správania) ochrany osobných údajov u prevádzkovateľa: **Príloha č. 1**

Prevádzkovateľ resp. osoby ním poverené spracúvaním osobných údajov fyzických osôb v rámci prevádzky akceptujú tieto všeobecné pravidla ochrany osobných údajov.

DRUHÁ ČASŤ

Analýza rizík

- 1) Identifikácia rizík založená na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužitelných hrozbami a na identifikácii dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti.**

Riziká v objektovej bezpečnosti:

- Strata alebo odcudzenie kľúčov od prevádzky,
- Neuzamknutie vstupných dverí do chránených priestorov po odchode z týchto priestorov,
- Prekonanie mechanických zábranných prostriedkov nepovolnou osobou,
- Živelná pohroma.

Riziká v dokumentárnom informačnom systéme:

- Šírenie chránených informácií zamestnancami prevádzkovateľa,
- Šírenie chránených informácií nezlikvidovanými nepotrebnými písomnosťami,
- Cielené získanie informácií o osobných údajoch cudzou osobou,
- Strata alebo odcudzenie dokumentácie obsahujúcej osobné údaje tretími osobami, prípadne zamestnancami prevádzkovateľa.

Riziká v automatizovanom informačnom systéme:

a) Riziká preniknutia osobných údajov k nepovolaným osobám:

- Preniknutie nepovolaných osôb k počítačovému systému,
- Odcudzenie počítačového systému,
- Riziko prieniku do pevného disku počítača, v ktorom sú uložené osobné údaje, neoprávnenými osobami z lokálnej počítačovej siete, resp. Jeho sprístupnenie týmto osobám,
- Prienik do pevného disku počítača, v ktorom sú uložené osobné údaje, neoprávnenými osobami z internetu, resp. Jeho sprístupnenie týmto osobám.

b) Riziká straty osobných údajov a narušenia integrity:

- Narušenie objektovej bezpečnosti prienikom nepovolaných osôb do priestorov s informačným systémom,
- Riziko nezabezpečeného prenosu prostredníctvom aplikácie,
- Riziko poškodenia serverov a aktívnych sieťových prvkov požiarom,
- Poškodenie pevného disku počítača mechanickou závadou,
- Poškodenie pevného disku alebo údajových štruktúr vplyvom výpadku elektrického napájania,
- Poškodenie pevného disku alebo údajových štruktúr vplyvom počítačových vírusov,

- Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov lokálnej siete,
- Poškodenie pevného disku alebo údajových štruktúr z vonkajšieho prostredia neoprávneným prístupom iných používateľov internetu.

2) Analýza a ohodnotenie rizík založených na určení dopadov, ktoré môžu vyplývať zo zlyhania bezpečnosti

Druhým krokom analýzy bezpečnosti je stanovenie rozsahu rizika, že daná hrozba spôsobí narušenie bezpečnosti alebo funkčnosti informačného systému. Riziko sa ohodnocuje podľa nasledovnej tabuľky:

		PRAVDEPODOBNOSŤ		
		Nízka	Stredná	Vysoká
DOPAD	Nulový	nulové	nulové	nulové
	Nízky	nízke	nízke	stredné
	Stredný	nízke	stredné	vysoké
	Vysoký	stredné	vysoké	vysoké

- 3) Určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti s odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovni rizika

		PRAVDEPODOBNOSŤ		
		Nízka	Stredná	Vysoká
DOPAD	Nulový	nulové	nulové	nulové
	Nízky	nízke	nízke	stredné.
	Stredný	nízke	stredné	vysoké
	Vysoký	stredné	vysoké	vysoké

Ak je riziko **nulové**, **nie je potrebné prijať** žiadne opatrenie za účelom eliminácie rizika.

Ak je riziko **nízke**, **môže byť prijaté** opatrenie za účelom eliminácie rizika.

Ak je riziko **stredné**, opatrenie za účelom eliminácie rizika **by malo byť prijaté**.

Ak je riziko **vysoké**, bezpečnostné opatrenie za účelom eliminácie rizika **musí byť prijaté**.

4) Riadenie rizík pre práva a slobody dotknutých osôb

Zhodnotil sa pôvod, povaha, osobitosť a závažnosť rizík alebo, konkrétnejšie, každé riziko sa posúdilo z pohľadu dotknutých osôb, ďalej sa zohľadnili sa zdroje rizík, identifikovali sa prípadné dôsledky na práva a slobody dotknutých osôb v súvislosti s určitými prípadmi vrátane neoprávneného prístupu, neželaných

úprav a straty údajov, identifikovali sa hrozby, ktoré by mohli viesť k neoprávnenému prístupu, neželaným úpravám a strate údajov, odhadla sa pravdepodobnosť a závažnosť a stanovili sa opatrenia na riešenie uvedených rizík.

Identifikácia s ohodnotením možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany

Chránený priestor je priestor prevádzkovateľa, v ktorom dochádza k spracovateľským činnostiam s osobnými údajmi či už automatizovaným alebo neautomatizovanými prostriedkami spracúvania (od získavania cez archiváciu až po ich likvidovanie).

Článok I

Riziká v objektovej bezpečnosti

Riziko straty alebo odcudzenia kľúčov od chránených priestorov

Prijaté opatrenie:

- správa kľúčov
- individuálne pridelenie kľúčov od chránených priestorov (prevádzka, archív, kancelárie, skrine, zásuvky) oprávneným osobám,
- bezpečné uloženie rezervných kľúčov do uzamykateľného trezora, kľúčmi od ktorého disponuje len prevádzkovateľ resp. ním poverená osoba,

Vyhodnotené riziko:

Stredné (táto hodnota je určená kombináciou hodnoty aktív a nízkou pravdepodobnosťou uplatnenia hrozby straty alebo odcudzenia kľúčov).

Odporúčané opatrenia:

Záznam o pridelení kľúčov od chránených priestorov oprávnenej osobe.

Riziko neuzamknutia dverí do chránených priestorov

Prijaté opatrenie

pravidelné uzamykanie dverí s použitím kľúčov, ak v chránenom priestore nie je prítomná žiadna oprávnená osoba,

správa kľúčov,

individuálne pridelenie kľúčov od chránených priestorov (prevádzka, archív, kancelárie, skrine, zásuvky)

oprávneným osobám,

bezpečné uloženie rezervných kľúčov do uzamykateľného trezora, kľúčmi od ktorého disponuje len prevádzkovateľ resp. ním poverená osoba.

Vyhodnotené riziko:

Stredné (táto hodnota je určená kombináciou hodnoty aktív a nízkou pravdepodobnosťou uplatnenia hrozby straty alebo odcudzenia kľúčov).

Odporúčané opatrenia:

Záznam o pridelení kľúčov od chránených priestorov oprávnenej osobe.

Riziko násilného prekonania mechanických zábranných prostriedkov nepovolanou osobou

Prijaté opatrenie:

- mechanické zabezpečenie chráneného priestoru- uzamykateľné bezpečnostné dvere a uzamykateľné okná do chráneného priestoru,
- dokumenty s osobnými údajmi sa nachádzajú v zabezpečenom uzamykateľnom objekte,
- dokumenty s osobnými údajmi sú uchovávané v uzamykateľnej miestnosti bez prístupu iných ako oprávnených osôb,
- technické zabezpečenie chráneného priestoru- alarm, kamerový systém.

Vyhodnotené riziko:

Nízke.

Odporúčané opatrenia:

Žiadne

Článok II

Riziká v dokumentárnom informačnom systéme

Riziko straty dôvernosti dokumentov obsahujúcich osobné údaje, únik osobných údajov zo strany zamestnancov, cielene nepovolanými osobami

Prijaté opatrenie:

- k listinám obsahujúcim osobné údaje majú prístup len prevádzkovateľa ním poverené oprávnené osoby,
- prevádzkovateľ a oprávnené osoby ukladajú listiny v priestore prístupnom tretím osobám iba v ich sprievode,
- záväzok mlčanlivosti oprávnených osôb a zákaz predkladať a sprístupniť tretej osobe dokumenty obsahujúce osobné údaje,
- dokumenty s osobnými údajmi sú zabalené do nepriehľadných zapečatených vriec,
- krátkodobá úschova (max. 30 dní) a následná likvidácia písomností obsahujúcich osobné údaje.

Vyhodnotenú riziko:

Stredné.

Odporúčané opatrenia:

Písomné poučenie oprávnených osôb.

Strata alebo odcudzenie dokumentov obsahujúcich osobné údaje

Prijaté opatrenie:

- k listinám obsahujúcim osobné údaje majú prístup len oprávnené osoby,
- oprávnené osoby ukladajú listiny v priestore prístupnom tretím osobám iba v ich sprievode,
- listinné dokumenty s osobnými údajmi sa nachádzajú v zabezpečenom uzamykateľnom priestore,
- listinné dokumenty s osobnými údajmi sú uchovávané v uzamykateľnej miestnosti bez prístupu iných ako oprávnených osôb,
- bezpečnostné dvere do chráneného priestoru,
- alarm,
- kamerový systém,
- krátkodobá úschova (max. 30 dní) a následná likvidácia písomností obsahujúcich osobné údaje,
- prenos dokumentov obsahujúcich osobné údaje po ich získaní od prevádzkovateľa len oprávnenou osobou, ďalší prenos dokumentov sa nevykonáva.

Vyhodnotenú riziko:

Nízke.

Odporúčané opatrenia:

Žiadne.

Článok III

Riziká v automatizovanom informačnom systéme

K automatizovanému spracúvaniu osobných údajov u prevádzkovateľa nedochádza.

Článok IV

Zvyškové riziká

Riziko úmyselného spôsobenia škody

- prípady, kedy škodca vedome porušuje príkaz prevádzkovateľa, pričom škodcom je poučený zamestnanec (napr. riziko zneužitia osobných údajov nepovoleným použitím tlačových výstupov, nepovoleným kopírovaním osobných údajov, fotením obrazovky počítača, nepovoleným, prenosom osobných údajov mimo priestorov prevádzkovateľa) alebo,
- prípady, keď škodca vedome porušuje všeobecne záväzný právny predpis, (napr. riziko vlámania a pod.)

Prevádzkovateľ **akceptuje tieto zvyškové riziká.**

Pôsobenie prírodných živlov

- v prípade dopadu pôsobenia prírodných živlov na aktíva prevádzkovateľa.

Prevádzkovateľ **akceptuje s obmedzením tieto zvyškové riziká.**

TRETIA CAST

Primerané bezpečnostné opatrenia

Prevádzkovateľ pri prijímaní primeraných bezpečnostných opatrení a záruk dodržiava nasledujúce zásady spracúvania osobných údajov:

zákonnosť, spravodlivosť, transparentnosť, obmedzenie a kompatibilita účelov spracúvania, minimalizáciu údajov, pseudonymizáciu alebo šifrovanie, minimalizáciu uchovávaní údajov, správnosť údajov, integrita, dôvernosť, dostupnosť údajov, nevyhnutnosť a primeranosť spracúvania s ohľadom na účel spracovateľskej operácie.

Pri prijímaní primeraných bezpečnostných opatrení a záruk prevádzkovateľ zohľadnil:

primeranosť a nutnosť spracúvania na základe:

- a) konkrétne určeného, výslovne uvedeného a legitímneho účelu,
- b) zákonnosti spracúvania,
- c) primeranosti, relevantnosti a obmedzenia na to, ktoré údaje sú potrebné,
- d) obmedzenej doby uchovávaní,

(PRVÁ ČASŤ)

Článok I

Technické opatrenia

Prevádzkovateľ zabezpečí prijatie týchto technických opatrení v konkrétnych podmienkach:

Zabezpečenie objektu pomocou mechanických zábranných prostriedkov uzamykateľné bezpečnostné dvere a uzamykateľné okná

Zabezpečenie objektu pomocou technických zabezpečovacích prostriedkov- alarm, kamerový systém.

Protipožiarne opatrenia- hasiace prístroje, požiarne hlásiče, protipožiarne dvere.

Umiestnenie informačného systému v chránenom priestore, ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.

Uloženie dokumentov s osobnými údajmi do zabezpečeného uzamykateľného objektu.

Uloženie dokumentov s osobnými údajmi v rámci uzamykateľného objektu do uzamykateľnej miestnosti bez prístupu iných ako oprávnených osôb.

Dokumenty s osobnými údajmi zabaliť do nepriehľadných zapečatených vriec.

Úschova dokumentov s osobnými údajmi maximálne 30 dní a následná likvidácie týchto dokumentov.

Likvidácia dokumentov s osobnými údajmi technickým zariadením- skartovačka.

Ďalšie súvisiace bezpečnostné opatrenia sú uvedené v požiarnych poplachových smerniciach prevádzkovateľa.

Článok II

Personálne a organizačné opatrenia

Prevádzkovateľ zabezpečí prijatie týchto personálnych a organizačných opatrení v konkrétnych podmienkach:

Vedenie písomných záznamov o spracovateľských činnostiach s osobnými údajmi oprávnených osôb a prevádzkovateľa.

(Príloha č. 2)

Riadenie prístupu oprávnených osôb k osobným údajom, stanovenie úrovne prístupu oprávnených osôb>

Písomné poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi

- poučenie o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie,
- vymedzenie IS a osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh,
- určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov,
- vymedzenie zakázaných postupov alebo operácií s osobnými údajmi,
- vymedzenie zodpovednosti za porušenie zákona,
- poučenie o povinnosti mlčanlivosti oprávnenej osoby,
- poučenie oprávnených osôb o ich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov,
- odovzdanie pridelených aktív, kľúčov, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby.

(Príloha č. 3)

Prevádzkovateľ a oprávnené osoby zabezpečia dodržiavanie práv dotknutej osoby. (Článok III Opatrenia k zabezpečeniu práv dotknutých osôb)

Kontrola vstupov oprávnených osôb do informačného systému. Identifikácia, autentizácia a autorizácia oprávnených osôb pri informačnom systéme prevádzkovateľom.

Vzdelávanie oprávnených osôb v právnej oblasti.

Prístup tretích strán k osobným údajom nie je.

Zapojenie zainteresovaných strán. Prevádzkovateľom nemusí byť poverená zodpovedná osoba pri spracúvaní osobných údajov, pre účely ochrany osobných údajov je kontaktnou a osobou zodpovednou prevádzkovateľ.

Podľa potreby prevádzkovateľ vynaloží úsilie na získanie názorov dotknutých osôb alebo ich zástupcov - pomocou dotazníkov.

Zamedzenie náhodného odpozerania osobných údajov z listín pri ich skartácii neoprávneným osobám

Vedenie zoznamu aktív a jeho aktualizácia prevádzkovateľom.

Správa kľúčov.

Individuálne pridelenie kľúčov od chránených priestorov (prevádzka, archív, kancelárie, skrine, zásuvky) oprávneným osobám.

Bezpečné uloženie rezervných kľúčov do uzamykateľného trezora, kľúčmi od ktorého disponuje len prevádzkovateľ resp. ním poverená osoba.

Pravidelné uzamykanie dverí s použitím kľúčov, ak v chránenom priestore nie je prítomná žiadna oprávnená osoba.

Vzájomné zastupovanie oprávnených osôb- v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru.

Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby.

Režim údržby a upratovania chránených priestorov sa vykonáva oprávnenou osobou.

Likvidovanie osobných údajov oprávnenou osobou skartovaním.

Zamedzenie náhodného odpozerania pri skartovaní osobných údajov z listín neoprávneným osobám,

Vykonáva sa ohlasovanie bezpečnostných incidentov oprávnenými osobami a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení.

Realizácia evidencie bezpečnostných incidentov a použitých riešení. **(Príloha č. 4)**

Postup pri riešení jednotlivých typov bezpečnostných incidentov sa stanovuje podľa pokynov prevádzkovateľa pri konkrétnom type incidentu.

Identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov.

Vykonáva sa kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení, uskutočňuje osobne prevádzkovateľom, resp. ním poverenou osobou.

Prevádzkovateľ počas spracúvania osobných údajov pravidelne kontroluje jednotlivé prístupy k informačnému systému, raz za 1 týždeň resp. náhodne.

Prevádzkovateľ informuje oprávnené osoby o kontrolnom mechanizme.

Vyhotovovanie záznamu z kontrolnej činnosti prevádzkovateľa.

(Príloha č. 5)

Článok III

Opatrenia k zabezpečeniu práv dotknutých osôb

Prevádzkovateľ zabezpečí prijatie týchto opatrení k zabezpečeniu práv dotknutých osôb:

- a) informácie poskytnuté dotknutej osobe,
- b) právo na prístup k údajom a právo na prenosnosť údajov,
- c) právo na opravu a právo na vymazanie,
- d) právo namietat' a právo na obmedzenie spracúvania,
- e) vzťah so sprostredkovateľom,
- f) záruky v súvislosti s medzinárodným prenosom,
- g) predchádzajúca konzultácia.

INFORMAČNÁ POVINNOSŤ PREVÁDZKOVATEĽA

Prevádzkovateľ osobné údaje nezískava priamo od dotknutej osoby

Informačnú povinnosť prevádzkovateľ neuplatňuje keďže poskytnutie informácií dotknutej osobe za účelom likvidácie jej osobných údajov sa ukázalo ako nemožné alebo by si vyžadovalo neprimerané úsilie. najmä ak sa spracúvajú osobné údaje na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel...)

PRÁVA DOTKNUTEJ OSOBY

Prevádzkovateľ zabezpečí dodržanie práva dotknutej osoby- **na prístup k údajom a právo na prenosnosť údajov:**

Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ takéto osobné údaje spracúva, dotknutá osoba má právo získať prístup k týmto osobným údajom a informácie o

- a) účele spracúvania osobných údajov,
- b) kategórii spracúvaných osobných údajov,
- c) identifikácii príjemcu alebo o kategórii príjemcu, ktorému boli alebo majú byť osobné údaje poskytnuté, najmä o príjemcovi v tretej krajine alebo o medzinárodnej organizácii, ak je to možné,

- d) dobe uchovávanía osobných údajov; ak to nieje možné, informáciu o kritériách jej určenia,
- e) práve požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby, ich vymazanie alebo obmedzenie ich spracúvania, alebo o práve namietat' spracúvanie osobných údajov,
- f) práve podať návrh na začatie konania na ochranu osobných údajov
- g) zdroji osobných údajov, ak sa osobné údaje nezískali od dotknutej osoby,
- h) existencii automatizovaného individuálneho rozhodovania vrátane profilovania, v týchto prípadoch poskytne prevádzkovateľ dotknutej osobe informácie najmä o použitom postupe, ako aj o význame a predpokladaných dôsledkoch takeého spracúvania osobných údajov pre dotknutú osobu.

Dotknutá osoba má právo byť informovaná o primeraných zárukách týkajúcich sa prenosu, ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii.

Prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva. Za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požíada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.

Právo získať osobné údaje nesmie mať nepriaznivé dôsledky na práva iných fyzických osôb.

Dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte a má právo preniesť tieto osobné údaje ďalšiemu prevádzkovateľovi, ak je to technicky možné a ak

dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel, výslovný súhlas so spracovaním osobitných kategórií osobných údajov aspoň na jeden konkrétny účel alebo je to potrebné na účely plnenia zmluvy a spracúvanie osobných údajov sa vykonáva automatizovanými prostriedkami.

Uplatnením tohto práva nie je dotknuté právo na výmaz osobných údajov. Právo na prenosnosť sa nevzťahuje na spracúvanie osobných údajov nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi.

Toto právo nesmie mať nepriaznivé dôsledky na práva iných osôb.

Prevádzkovateľ zabezpečí dodržanie práva dotknutej osoby- **na opravu a právo na vymazanie:**

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo na doplnenie neúplných osobných údajov.

Dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú.

Prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak dotknutá osoba uplatnila právo na výmaz, ak

- a) osobné údaje už nie sú potrebné na účel, na ktorý sa získali alebo inak spracúvali,
- b) dotknutá osoba odvolá súhlas, na základe ktorého sa spracúvanie osobných údajov vykonáva, a neexistuje iný právny základ pre spracúvanie osobných údajov,
- c) dotknutá osoba namieta spracúvanie osobných údajov a neprevažujú žiadne oprávnené dôvody na spracúvanie osobných údajov alebo dotknutá osoba namieta spracúvanie osobných údajov pri prevažujúcich oprávnených záujmoch prevádzkovateľa,
- d) osobné údaje sa spracúvajú nezákonne,
- e) je dôvodom pre výmaz splnenie povinnosti podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo
- f) sa osobné údaje získavali v súvislosti s ponukou služieb informačnej spoločnosti.

Ak prevádzkovateľ zverejnil osobné údaje a je povinný ich vymazať, je zároveň povinný prijať primerané bezpečnostné opatrenia vrátane technických opatrení so zreteľom na dostupnú technológiu a náklady na ich vykonanie na účel informovania ostatných prevádzkovateľov, ktorí spracúvajú osobné údaje dotknutej osoby o jej žiadosti, aby títo prevádzkovatelia vymazali odkazy na jej osobné údaje a ich kópie alebo odpisy.

Vyššie sa neuplatňuje, ak je spracúvanie osobných údajov potrebné

- a) na uplatnenie práva na slobodu prejavu alebo práva na informácie,
- b) na splnenie povinnosti podľa tohto zákona, osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- c) z dôvodov verejného záujmu v oblasti verejného zdravia,
- d) na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je pravdepodobné, že právo podľa odseku 1 znemožní alebo závažným spôsobom sťažuje dosiahnutie cieľov takého spracúvania, alebo
- e) na uplatnenie právneho nároku.

Prevádzkovateľ zabezpečí dodržanie práva dotknutej osoby - **namietat' a právo na obmedzenie spracúvania**:

Dotknutá osoba má právo namietat' spracúvanie jej osobných údajov z dôvodu týkajúceho sa jej konkrétnej situácie, ak dochádza k spracúvaniu osobných údajov nevyhnutných na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh, taktiež vrátane profilovania založeného na týchto ustanoveniach. Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, ak nepreukáže nevyhnutné oprávnené záujmy na spracúvanie osobných údajov, ktoré prevažujú nad právami alebo záujmami dotknutej osoby, alebo dôvody na uplatnenie právneho nároku.

Dotknutá osoba má právo namietat' spracúvanie osobných údajov, ktoré sa jej týkajú, na účel priameho marketingu vrátane profilovania v rozsahu, v akom súvisí s priamym marketingom. Ak dotknutá osoba namieta spracúvanie osobných údajov na účel priameho marketingu, prevádzkovateľ ďalej osobné údaje na účel priameho marketingu nesmie spracúvať.

Dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie osobných údajov, ak

- a) dotknutá osoba namieta správnosť osobných údajov, a to počas obdobia umožňujúceho prevádzkovateľovi overiť správnosť osobných údajov,
- b) spracúvanie osobných údajov je nezákonné a dotknutá osoba namieta vymazanie osobných údajov a žiada namiesto toho obmedzenie ich použitia,
- c) prevádzkovateľ už nepotrebuje osobné údaje na účel spracúvania osobných údajov, ale potrebuje ich dotknutá osoba na uplatnenie právneho nároku, alebo
- d) dotknutá osoba namieta spracúvanie osobných údajov pri prevažujúcich oprávnených záujmoch prevádzkovateľa, a to až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby.

Ak sa spracúvanie osobných údajov obmedzilo, okrem uchovávanía môže osobné údaje prevádzkovateľ spracúvať len so súhlasom dotknutej osoby alebo na účel uplatnenia právneho nároku, na ochranu osôb alebo z dôvodov verejného záujmu.

Dotknutú osobu, ktorej spracúvanie osobných údajov sa obmedzí, je prevádzkovateľ povinný informovať pred tým, ako bude obmedzenie spracúvania osobných údajov zrušené.

Oznamovacia povinnosť v súvislosti s opravou, vymazaním alebo obmedzením spracúvania osobných údajov:

Vypracoval: **SOKOL trade s.r.o.**