BEZPEČNOSTNÁ SMERNICA GDPR č.01/23

Podľa nariadenia 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) a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Smernica č.:

Účinná od: Verzia č. -

Počet strán: Posledná aktualizácia:

Vypracoval: MG GDPR, s.r.o.

MG GDPR

Schválil: Dňa:

GDPR

Táto smernica je duševným majetkom spoločnosti. Zamestnanci, ktorí ju pri svojej činnosti používajú, zodpovedajú za to, že nebude odovzdaná mimo spoločnosť. Nesmie sa kopírovať, ani iným spôsobom rozmnožovať. Porušenie týchto zásad sa považuje za hrubé porušenie pracovnej disciplíny.

Obsah

POUŽITÉ POJMY A SKRATKY: ..... - 3 -
I. IDENTIFIKÁCIA PREVÁDZKOVATEĽA IS: ..... - 5 -
II. ÚVOD ..... - 8 -
III. ZÁKLADNÉ POJMY ..... - 9 -
IV. ZÁKLADNÉ CIELE A ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV ..... - 9 -
V. PRÁVA DOTKNUTÝCH OSÔB ..... - 11 -
VI. SŤAŽNOSTI A NÁVRH NA ZAČATIE KONANIA ..... - 12 -
VII. SPÔSOB ZÍSKAVANIA OSOBNÝCH ÚDAJOV ..... - 13 -
VIII. INFORMAČNÁ POVINNOSŤ ..... - 14 -
IX. ZÁZNAMY O SPRACOVATEĽSKÝCH ČINNOSTIACH ..... - 14 -
X. USTANOVENIE ZODPOVEDNEJ OSOBY ..... - 15 -
XI. KONTROLNÉ ČINNOSTI – SPÔSOB, PERIODICITA, FORMA ..... - 17 -
XII. RIEŠENIE BEZPEČNOSTI SPRACÚVANIA OSOBNÝCH ÚDAJOV ..... - 17 -
XIII. BEZPEČNOSTNÉ INCIDENTY ..... - 21 -

Použité pojmy a skratky:

Za účelom vyvrátenia akýchkoľvek nejasností pri výklade jednotlivých pojmov uvádzame bližší popis jednotlivých pojmov pre účely výkladu tejto dokumentácie:

1. „Zamestnanec“: fyzická osoba vykonáva závislú prácu pre prevádzkovateľa na základe pracovnej zmluvy.

2. „Dohodár“: fyzická osoba vykonávajúca závislú prácu pre prevádzkovateľa na základe dohody o výkone práce mimo pracovného pomeru.

3. „Dotknutá osoba:“ každá fyzická osoba, ktorej osobné údaje sa spracúvajú

4. „Externista“: fyzická osoba – podnikateľ vykonávajú činnosť pre prevádzkovateľa na základe obchodnoprávneho vzťahu.

5. „Informačný systém“: akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe,

6. „Klient“ fyzická alebo právnická osoba, ktorej prevádzkovateľ predáva tovar/poskytuje službu.

7. „Majiteľ“: fyzická osoba, vlastniaca obchodný podiel v spoločnosti prevádzkovateľa.

8. „Miestnosť“: priestor prevádzkovateľa /vo výlučnom vlastníctve alebo nájomné/, nachádzajúca sa v Objekte, v ktorom je umiestnený informačný systém v listinnej podobe a počítače, prostredníctvom ktorých je uložený prístup k informačnému systému v elektronickej podobe. V množnom čísle „miestnosti“

9. „Oprávnená osoba“: každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru alebo vymenovania u prevádzkovateľa.

10. „Ovládajúca osoba“: fyzická alebo právnická osoba, ktorá vlastní obchodný podiel v spoločnosti prevádzkovateľa.

11. „Porušenie ochrany osobných údajov“: porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim.

12. „Objekt“: sídlo prevádzkovateľa, priestory nachádzajúce sa na Bzenov 38 08242 Bzenov, kde sú fyzické nosiče osobných údajov uložené.

13. „Smernica“: táto smernica o bezpečnosti osobných údajov.

14. „Sprostredkovateľ“: každý, kto spracúva osobné údaje v mene prevádzkovateľa.

15. „Štatutár“: člen štatutárneho orgánu prevádzkovateľa – konateľ.

16. „Uchádzači o zamestnanie“: osoby uchádzajúce sa o prácu u prevádzkovateľa.

17. „Usmernenie týkajúce sa posúdenia vplyvu na ochranu údajov“: Usmernenie Pracovnej skupiny pre ochranu osobných údajov zriadenie podľa článku 29 GDPR prijaté dňa 4.4.2017 týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku“.

18. „Usmernenie týkajúce sa zodpovedných osôb“: Usmernenie Pracovnej skupiny pre ochranu osobných údajov zriadenie podľa článku 29 GDPR prijaté dňa 13.12.2016 týkajúce sa zodpovedných osôb.

19. „Zákon“: zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

20. „Nariadenie“: Nariadenie 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) a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

21. „Zodpovedná osoba“: osoba určená prevádzkovateľom alebo Sprostredkovateľom podľa ustanovenia § 44 -46 Zákona, ktorá plní úlohy podľa Zákona.

I. IDENTIFIKÁCIA PREVÁDZKOVATEĽA IS:

Názov:	Obec Bzenov
Sídlo:	Bzenov 38 08242 Bzenov
IČO:	00326895
Riadi a kontroluje spracúvanie OÚ: *nie je zodpovednou osobou / je zodpovednou osobou* Zodpovedná osoba:	

(Ďalej aj ako „prevádzkovateľ“ alebo „spoločnosť“)

(1) Prevádzkovateľ je obchodná spoločnosť založená a podnikajúca podľa právnych predpisov Slovenskej republiky.
(2) Prevádzkovateľ zamestnáva zamestnancov a dohodárov. prevádzkovateľ nevyužíva služby Externistov.
(3) Prevádzkovateľ spracúva osobné údaje v nasledovných IS:

	Názov informačného systému:	Označenie IS
	IS Personálna a mzdová agenda zamestnancov	1
	IS Ekonomicko-účtovná agenda	2
	IS Právne vzťahy	3
	IS Zmluvné vzťahy	4
	IS Správa registratúry	5
	IS Evidencia SZČO	6
	IS Evidencia zástupcov dodávateľov a odberateľov	7
	IS Uplatňovanie práv dotknutých osôb	8
	IS Oznamovanie protispoločenskej činnosti	9
	IS Poslanci obecného zastupiteľstva	10
	IS Evidencia členov komisií (Neposlanci)	11
	IS Organizácia obecného zastupiteľstva	12
	IS Monitorovanie kamerovým systémom	13
	IS Verejné obstarávanie	14
	IS Obchodná verejná súťaž	15
	IS Zverejňovanie zmlúv	16
	IS Žiadosti o sprístupnenie informácií podľa zákona o slobodnom prístupe k informáciám	17

	IS Konanie o opravných prostriedkoch podľa zákona o slobodnom prístupe k informáciám	18
	IS Sťažnosti	19
	IS Petície	20
	IS Kontrola a audit	21
	IS Kontrolná činnosť útvarom hlavného kontrolóra	22
	IS Zmluvné vzťahy z nájmu pozemkov a stavieb	23
	IS Zmluvné vzťahy z nájmu ostatných nehnuteľností	24
	IS Kolízny opatrovník v rámci obmedzenia spôsobilosti na právne úkony	25
	IS Kolízny opatrovník vo veciach maloletých	26
	IS Daň z nehnuteľností	27
	IS Daň za užívanie verejného priestranstva	28
	IS Miestny poplatok za komunálne odpady a drobné stavebné odpady	29
	IS Agenda daňové exekúcie	30
	IS Vyjadrenia obce k žiadostiam na prevádzku hazardných hier	31
	IS Civilná ochrana obyvateľstva	32
	IS Evidencia osôb, ktoré sa v čase krízovej situácie nachádzajú na území obce	33
	IS Evidencia osôb za účelom uloženia povinnosti poskytnúť ubytovanie v čase vojny alebo vojnového stavu	34
	IS Evidencia osôb za účelom uloženia pracovnej povinnosti v čase vojny alebo vojnového stavu	35
	IS Hospodárska mobilizácia	36
	IS Náhrady v oblasti hospodárskej mobilizácie	37
	IS Evidencia kandidátov a kandidátnych listín	38
	IS Miestna volebná komisia	39

	IS Evidencia obyvateľov	40
	IS Osvedčovanie listín a podpisov	41
	IS Matrika	42
	IS Evidencia samostatne hospodáriacich roľníkov	43
	IS Evidencia hrobových miest	44
	IS Základná škola s materskou školou	45
	IS Obecná školská rada	46
	IS Rada školy	47
	IS Štatistické výkazy	48
	IS Údržba zelene	49
	IS Oznámenia o nezákonne umiestnenom odpade	50
	IS Súhlasy pre malé zdroje znečistenia ovzdušia	51
	IS Stanoviská podľa stavebného zákona	52
	IS Výrub a výsadba cestnej zelene	53
	IS Určenia dopravných značiek a dopravných zariadení na miestnych a účelových komunikáciách	54
	IS Povolenie pripojenia na miestnu komunikáciu a zariadenie zjazdu z miestnej komunikácie	55
	IS Povolenie zvláštneho užívania miestnej komunikácie	56
	IS Povolenie uzávierky miestnej komunikácie	57
	IS Správa pozemných komunikácií	58
	IS Dozor nad miestnymi komunikáciami	59
	IS Stavebný úrad	60
	IS Nakladanie s komunálnymi odpadmi a drobnými stavebnými odpadmi	61
	IS Priestupky	62

	IS Územné plánovanie	63
	IS Predaj a zámena pozemkov a stavieb	64
	IS Zmluvné vzťahy z vecných bremien	65
	IS Podujatia	66
	IS Kontaktný formulár	67
	IS Fotografie	68
	IS Sociálne siete	69

(4) Informácie o právnych základoch, účele, likvidácii údajov, kategórii dotknutých osôb, kategórii osobných údajov a pod. sa nachádzajú v dokumente „Záznamy o spracovateľských činnostiach prevádzkovateľa“ .

II. ÚVOD

Za účelom chodu spoločnosti je potrebné, aby dochádzalo ku toku osobných údajov, či už zamestnancov, zákazníkov, alebo iných fyzických osôb, pričom sa prirodzene vynára otázka ochrany pred zneužitím, stratou, zverejnením alebo iným narušením takýchto údajov. Osobné údaje sú kategóriou, ktoré spadajú pod základné ľudské práva a slobody, ktoré chráni okrem iných predpisov i samotná Ústava SR, čo svedčí o tom, že ide o kategóriu vysoko citlivú a intímnu, ktorá patrí každému jednému človeku ako jeho právo.

Prevádzkovateľ zodpovedá za bezpečnosť údajov, ktoré spracúva. Z daného dôvodu je povinný spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom, sprístupnením, poskytnutím, zverejnením, alebo pred akýmikoľvek inými neprípustnými formami spracúvania chrániť.

Prevádzkovateľ spracúva osobné údaje dotknutých osôb v informačných systémoch, ktoré sa navzájom líšia nielen formou, ako prichádza k samotnému spracúvaniu, ale aj použitými prostriedkami spracúvania, ktoré môžu mať osobitný charakter. Túto smernicu treba chápať ako základný dokument (manuál) pre všetkých užívateľov informačných systémov.

Prevádzkovateľ vydáva túto bezpečnostnú smernicu za účelom zaistenia bezpečnosti a ochrany informačných systémov a osobných údajov v nich spracúvaných osobami na to poverenými.

Bezpečnostná smernica je aplikáciou, resp. Implementáciou záverov Analýzy rizík v spoločnosti. Tieto pravidlá je potrebné rešpektovať a dodržiavať za účelom zachovania bezpečného chodu a spracúvania osobných údajov prevádzkovateľom v praxi.

Súčasťou bezpečnostnej dokumentácie GDPR sú v Prílohe č. 1 navrhované primerané personálne, technické a organizačné opatrenia zodpovedajúce spôsobu spracúvania osobných údajov, zohľadňujúc najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných

osobných údajov ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.

Medzi základné pramene práva v oblasti ochrany osobných údajov patrí primárne :

- Nariadenie 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 ako „nariadenie GDPR")
- Zákon 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej aj ako „zákon")

III. ZÁKLADNÉ POJMY

1. **Osobné údaje** sú akékoľvek informácie týkajúce sa fyzickej osoby, na základe ktorých ju možno priamo alebo nepriamo identifikovať. Osobnými údajmi sú napríklad meno, priezvisko, druh a adresa pobytu, dátum narodenia, rodné číslo, email, tel. č., podpis, ale aj lokalizačné údaje, či online identifikátor. Za osobný údaj sa považuje každý údaj, ktorý je špecifický pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

2. **Spracúvanie osobných údajov** je akákoľvek operácia, činnosť alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov. Za spracúvanie osobných údajov sa považuje napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia. Spracúvaním je každá takáto operácia s osobnými údajmi bez ohľadu na to, akými prostriedkami je vykonávaná.

3. **Prevádzkovateľ**je osoba, ktorá spracúva osobné údaje a určí účely a prostriedky spracúvania. Prevádzkovateľom môže byť fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt. Prevádzkovateľ sa odlišuje od iných subjektov, ktoré spracúvajú osobné údaje (napr. sprostredkovateľ) tým, že určí účely a prostriedky spracúvania osobných údajov. Prevádzkovateľom je vaša firma.

4. **Sprostredkovateľ** je osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa, na základe jeho poverenia. Sprostredkovateľom je napríklad externý účtovník, ktorý pre vás spracúva osobné údaje za účelom vedenia účtovníctva.

5. **Dotknutá osoba**je fyzická osoba, ktorej sa osobné údaje týkajú, resp. ktorej osobné údaje sa spracúvajú. Dotknutými osobami súnapr. vaši zamestnanci, zákazníci alebo osoby, ktoré vám dali súhlas na zasielanie newsletter-a.

6. **Informačný systém** je akýkoľvek usporiadaný súbor osobných údajov spracúvaných podľa určitých kritérií na vymedzený účel.

7. **Príjemca** každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov.

IV. ZÁKLADNÉ CIELE A ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

1. **Prevádzkovateľ stanovuje základné ciele v oblasti ochrany osobných údajov:**

1.1. Spracúvanie osobných údajov poverenými osobami v súlade s pokynmi prevádzkovateľa a pri dodržaní všetkých prijatých bezpečnostných opatrení;

1.2. Spracúvanie osobných údajov v súlade so zásadou zákonnosti;

1.3. Spracúvanie len tých osobných údajov, ktoré sú pre dosiahnutie presne vymedzeného účelu spracúvania osobných údajov považované za nevyhnutné;

1.4. Zabezpečenie likvidácie osobných údajov zo všetkých nosičov dát po uplynutí nevyhnutnej doby na ich uchovávanie;

1.5. Naplnenie informačnej povinnosti voči dotknutým osobám vyplývajúcej z článkov 12 a nasl. Nariadenia GDPR. Pri spracúvaní osobných údajov je prevádzkovateľ povinný dodržiavať zásadu transparentnosti. V rámci tejto zásady prevádzkovateľ dotknutú osobu musí informovať o podmienkach spracúvania osobných údajov a následne jej údaje skutočne spracúvať v súlade s týmito informáciami;

1.6. Zabezpečenie zachovávania mlčanlivosti zamestnancov a osôb prítomných v objekte / objektoch;

1.7. Uzatvorenie zmluvného vzťahu so sprostredkovateľom a zabezpečenie naplnenia všetkých legislatívnych požiadaviek upravujúcich vzťah prevádzkovateľ-sprostredkovateľ;

1.8. Rešpektovanie základných práv dotknutých osôb a zabezpečenie ich dodržiavania.

2. Medzi základné zásady spracúvania osobných údajov patrí:

*2.1. **ZÁSADA ZÁKONNOSTI***

Spracúvať osobné údaje môže prevádzkovateľ len na niektorom z právnych základov stanovených nariadením GDPR, pričom táto povinnosť sa vzťahuje na dodržiavanie nie len nariadenia GDPR a zákona o ochrane osobných údajov ale aj iných relevantných právnych predpisov.

*2.2. **ZÁSADA OBMEDZENIA ÚČELU***

osobné údaje môže prevádzkovateľ získavať len na konkrétne určený, výslovne uvedený a legitímny účel. Ďalej spracúvať takto získané osobné údaje na iný účel, ktorý nie je zlučiteľný s pôvodným účelom, je zakázané.

*2.3. **ZÁSADA MINIMALIZÁCIE ÚDAJOV***

Prevádzkovateľ je oprávnený spracúvať len tie osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie. Spracúvať také osobné údaje, ktoré sú nadbytočné, nepotrebné a nie sú nevyhnutné na dosiahnutie stanoveného účelu je zakázané.

*2.4. **ZÁSADA SPRÁVNOSTI***

Ak zistíte, že osobné údaje nie sú správne, musíte prijať všetky dostupné opatrenia na ich opravu alebo vymazanie.

*2.5. **ZÁSADA MINIMALIZÁCIE UCHOVÁVANIA***

V zmysle nariadenia GDPR sa môžu osobné údaje spracúvať len po dobu, ktorá je nevyhnutná na dosiahnutie stanoveného účelu. Po ukončení spracúvania osobných údajov na daný účel je potrebné osobné údaje zlikvidovať.

*2.6. **ZÁSADA INTEGRITY A DÔVERNOSTI***

Prevádzkovateľ je povinný zabezpečiť ochranu osobných údajov, ktoré spracúva. Za týmto účelom je povinný prijať primerané technické a organizačné opatrenia.

*2.7. **ZÁSADA ZODPOVEDNOSTI***

Súlad spracúvania osobných údajov s nariadením GDPR a zákonom o ochrane osobných údajov a dodržiavanie všetkých svojich povinností je prevádzkovateľ povinný zdokumentovať, aby splnenie jednotlivých povinností vedel prevádzkovateľ preukázať v prípade kontroly.

V. PRÁVA DOTKNUTÝCH OSÔB

1. Prevádzkovateľ kladie dôraz na rešpektovanie práv dotknutých osôb. Dotknuté osoby majú tieto práva:

   1.1. Právo na informácie
   Každá osoba, ktorej osobné údaje prevádzkovateľ spracúva, má právo na informácie, ktoré stanovuje nariadenie GDPR a zákon o ochrane osobných údajov. Za týmto účelom je prevádzkovateľ povinný prijať vhodné opatrenia, aby tieto informácie dotknutej osobe poskytol. Informácie môžu byť poskytnuté prostredníctvom webovej stránky, emailom alebo v listinnej forme. Informácie musia byť poskytnuté v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho.

   Prevádzkovateľ uvedené informácie zverejnil / sprístupnil: na obecnom úrade

   1.2. Právo na prístup k údajom
   Každá osoba, ktorej osobné údaje prevádzkovateľ spracúva, má právo získať potvrdenie o tom, či konkrétny prevádzkovateľ spracúva jej osobné údaje. Ak osobné údaje tejto osoby spracúva, má dotknutá osoba právo na prístup k týmto údajom a informácie o ich spracúvaní stanovené zákonom.

   1.3. Právo na opravu
   Každá osoba má právo, aby prevádzkovateľ spracúval iba jej správne a aktuálne údaje. Ak dotknutá osoba o to prevádzkovateľa požiada, tak musí nesprávne a neaktuálne údaje opraviť.

   1.4. Právo na vymazanie
   V určitých prípadoch má osoba, ktorej údaje prevádzkovateľ spracúva, právo na vymazanie jej osobných údajov. Ak sú splnené zákonné podmienky, prevádzkovateľ je povinný jej údaje vymazať.

   1.5. Právo na obmedzenie spracúvania
   V určitých prípadoch má osoba, ktorej údaje prevádzkovateľ spracúva, právo na obmedzenie spracúvania jej osobných údajov. Počas obmedzenia spracúvania môže prevádzkovateľ jej údaje len uchovávať, iným spôsobom ich spracúvať nemôžete.

   1.6. Právo na prenosnosť údajov
   Pokiaľ prevádzkovateľ spracúva osobné údaje v elektronickej forme na základe súhlasu danej osoby, môže ho požiadať, aby jej osobné údaje poskytol vo forme, ktorá umožňuje prenos inému prevádzkovateľovi.

   1.7. Právo namietať
1. Dotknutá osoba má za určitých okolností právo namietať proti spracúvaniu jej údajov.

2. Dotknutým osobám prevádzkovateľ zabezpečí bezporuchový výkon ich práv, v čo najjednoduchšej podobe, nekladie im prekážky. Preto vytvoril systém, prostredníctvom ktorého by mohli dotknuté osoby uplatňovať svoje práva.

3. Dotknutej osobe sú vždy poskytnuté informácie o spracúvaní jej osobných údajov a sú poučené o svojich právach. Prevádzkovateľ poskytuje tieto informácie vhodným spôsobom podľa okruhu dotknutých osôb, napríklad písomne v listinnej forme, mailom alebo zverejnením na webovom sídle.

4. Dotknuté osoby môžu uplatňovať svoje práva e-mailom na starostabzenov@gmail.com alebo poštou.

5. Pri uplatnení práv dotknutou osobou telefonicky dotknutú osobu kompetentná osoba prevádzkovateľa upovedomí o vhodnej forme, akou môže svoje práva uplatniť.

6. Prevádzkovateľ každú žiadosť zaeviduje a vybaví bez zbytočného odkladu, najneskôr však do jedného mesiaca. V tejto lehote informuje dotknutú osobu, ktorá žiadosť podala, o opatreniach, ktoré na základe jej žiadosti prijali. Uvedená lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. O predĺžení lehoty dotknutú osobu informuje do jedného mesiaca od podania žiadosti spolu s odôvodnením zmeškania lehoty. Oznámenie o spôsobe vybavenia žiadosti sa podáva rovnakým spôsobom, akým bola podaná žiadosť, pokiaľ dotknutá osoba nepožiada o iný spôsob.

7. Pri použití ktoréhokoľvek z vyššie uvedených spôsobov uplatnenia práv dotknutých osôb, je potrebné zabezpečiť nasledovné:

   a) presnú identifikáciu žiadateľa. Jeho autenticitu. Preukázateľné zabezpečenie skutočnosti, že žiadosť o poskytnutie informácii je skutočne od DO alebo osoby, ktorá je oprávnená žiadať v mene DO o poskytnutie informácií.

   b) nepopierateľnosť odoslania žiadosti, preukázateľné zabezpečenie nemožnosti poprieť skutočnosť, že žiadosť o poskytnutie informácii bola odoslaná DO.

   c) zabezpečenie dôvernosti a integrity odosielaných informácii počas ich prenosu k DO.

   d) preukázateľné zabezpečenie toho že informácie boli dotknutej osobe komunikačným kanálom doručené.

VI. SŤAŽNOSTI A NÁVRH NA ZAČATIE KONANIA

1. V prípade doručenia sťažnosti je povinná osoba, ktorá sťažnosť prijala oboznámiť vedenie spoločnosti / zodpovednú osobu o prijatí tejto sťažnosti a odovzdať jej všetky informácie, ktoré vo vzťahu ku sťažnosti a konkrétnemu sťažovateľovi má k dispozícii. Vedenie spoločnosti / zodpovedná osoba poverí vybavením sťažnosti konkrétnu oprávnenú osobu, alebo sťažnosť vybaví sama.

2. Sťažnosti sa podávajú v zmysle Nariadenia GDPR, resp. Zákona č. 18/2018 Z. z. o ochrane osobných údajov a zákona č. 9/2010 Z. z. o sťažnostiach. Zodpovedný pracovník prijímajúci sťažnosť okamžite vyrozumie zodpovednú osobu prevádzkovateľa, ako aj samotného prevádzkovateľa. Sťažnosti sa vybavujú v zmysle Zákona č. 9/2010 Z.z. o sťažnostiach.

3. Dotknutá osoba má právo podať návrh na začatie konania v zmysle ustanovenia § 100 zákona o ochrane osobných údajov.

4. Dotknutá osoba, ktorá má podozrenie, že dochádza k neoprávnenému spracúvaniu jej osobných údajov alebo došlo k zneužitiu jej osobných údajov, môže podať na Úrade pre ochranu osobných údajov Slovenskej republiky (ďalej len „Úrad") návrh na začatie konania o ochrane osobných údajov.

5. Návrh na začatie konania možno podať písomne, osobne ústnou formou do zápisnice, elektronickými prostriedkami, pričom musí byť podpísaný zaručeným elektronickým podpisom, telegraficky alebo telefaxom, ktorý však treba písomne alebo ústne do zápisnice doplniť najneskôr do 3 dní.

6. Predmetný návrh musí v zmysle ustanovenia § 100 zákona o ochrane osobných údajov obsahovať:
   - meno, priezvisko, adresu trvalého pobytu a podpis navrhovateľa,
   - označenie toho, proti komu návrh smeruje; názov alebo meno a priezvisko, sídlo alebo trvalý pobyt, prípadne právnu formu a identifikačné číslo,
   - predmet návrhu s označením, ktoré práva sa podľa tvrdenia navrhovateľa pri spracúvaní osobných údajov porušili,
   - dôkazy na podporu tvrdení uvedených v návrhu,
   - kópiu listiny preukazujúcej uplatnenie práva podľa § 28 zákona, ak sa takéto právo mohlo uplatniť, alebo uvedenie dôvodov hodných osobitného zreteľa.

7. Úrad následne rozhodne o návrhu navrhovateľa v lehote do 60 dní odo dňa začatia konania. V odôvodnených prípadoch môže Úrad túto lehotu primerane predĺžiť, najviac však o 6 mesiacov. O predĺžení lehoty Úrad písomne informuje účastníkov konania.

VII. SPÔSOB ZÍSKAVANIA OSOBNÝCH ÚDAJOV

1. Oprávnené osoby sú povinné dbať na kontrolu dodržiavania zásady zákonnosti a pri získavaní osobných údajov od dotknutých osôb získavať len tie osobné údaje, ktoré sú nevyhnutné na dosiahnutie vopred stanoveného účelu a v súlade s konkrétnym právnym základom.
2. **Oprávnené osoby pri získavaní osobných údajov dodržiavajú nasledovný postup:**
   2.1. ***osobné údaje nevyžiadané*** – oprávnená osoba je povinná zhodnotiť, či údaje, o ktoré nepožiadala sú nevyhnutné na dosiahnutie účelu, na ktorý ich dotknutá osoba poskytla. Údaje, ktoré prevádzkovateľ nepožiadal a k naplneniu účelu nie sú nevyhnutné je potrebné preukázateľne dotknutej osobe vrátiť a zo všetkých nosičov dát ich zlikvidovať.
      - *napr. poštou (žiadosť o zamestnanie) v prípade, že nedôjde k podpisu pracovnej zmluvy je tieto potrebné preukázateľne vrátiť žiadateľovi alebo skartovať (s výnimkou osobných údajov zaslaných v elektronickej podobe, ktoré je potrebné bezpečne vymazať). Pokiaľ sa budú z nejakých dôvodov (napr. možnosť zamestnania v blízkej budúcnosti) uchovávať niektoré osobné údaje, je potrebné zabezpečiť ich ochranu, súhlas so spracúvaním osobných údajov a nakladať s nimi ako s ostatnými osobnými údajmi,*

   2.2. ***ostatné osobné údaje*** - oprávnená osoba, ktorá získava osobné údaje v mene prevádzkovateľa, alebo sprostredkovateľa, preukáže na požiadanie tomu, od koho osobné údaje dotknutej osoby požaduje, svoju totožnosť a bez vyzvania mu vopred poskytne informácie podľa čl. 13 nariadenia GDPR, prípadne predloží dokument „informačná povinnosť prevádzkovateľa – zásady spracúvania osobných údajov“ alebo informuje dotknutú osobu, kde sa tieto informácie nachádzajú. Dodržanie tejto povinnosti považuje prevádzkovateľ za nevyhnutné a jej porušenie zo strany oprávnenej osoby môže prevádzkovateľ ako zamestnávateľ považovať za hrubé porušenie pracovnej disciplíny. V prípade ak dotknutej osobe oprávnená osoba neposkytne informácie podľa čl. 13, je povinná o tejto skutočnosti bezodkladne oboznámiť nadriadeného, alebo zamestnávateľa, aby túto skutočnosť mohol bez zbytočného odkladu napraviť.

3. Za nepravdivosť osobných údajov zodpovedá ten, kto ich do informačného systému poskytol. Zamestnanec je povinný aktualizovať osobné údaje, ktoré poskytol zamestnávateľovi.

4. Ak je spracúvanie osobných údajov založené na súhlase dotknutej osoby, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že dotknutá osoba poskytla súhlas so spracúvaním svojich osobných údajov.

5. Ak prevádzkovateľ žiada o udelenie súhlasu na spracovanie osobných údajov dotknutú osobu, tento súhlas musí byť odlíšený od iných skutočností a musí byť vyjadrený jasne a v zrozumiteľnej a ľahko dostupnej forme.

6. Dotknutá osoba má právo kedykoľvek odvolať súhlas so spracovaním osobných údajov, ktoré sa jej týkajú. Odvolanie súhlasu nemá vplyv na zákonnosť spracúvania osobných údajov založeného na súhlase pred jeho odvolaním; pred poskytnutím súhlasu musí byť dotknutá osoba o tejto skutočnosti informovaná. Dotknutá osoba môže súhlas odvolať rovnakým spôsobom, akým súhlas udelila.

7. Pri posudzovaní, či bol súhlas poskytnutý slobodne, sa najmä zohľadní skutočnosť, či sa plnenie zmluvy vrátane poskytnutia služby podmieňuje súhlasom so spracúvaním osobných údajov, ktorý nie je na plnenie tejto zmluvy nevyhnutný.

8. Pri poskytovaní súhlasu dotknutej osoby nesmie oprávnená osoba na dotknutú osobu vyvíjať nátlak ani iným spôsobom ovplyvňovať jej rozhodovanie. *Nátlakom sa rozumie taká hrozba, kedy neudelenie súhlasu dotknutou osobou bude mať za následok odmietnutie poskytnutia zmluvného vzťahu, neposkytnutie služby, alebo zamedzenie predaja či dostupnosti tovaru pre danú dotknutú osobu, za predpokladu, že sa súhlas netýka spracúvania osobných údajov nevyhnutných pre takéto uzatvorenie zmluvného vzťahu, poskytnutie služby alebo predaja tovaru, ale ide o taký súhlas na spracúvanie osobných údajov požadovaný od dotknutej*

osoby, ktorý so zmluvným vzťahom, poskytnutím služby alebo predajom tovaru nemá priamy súvis (napríklad súhlas požadovaný prevádzkovateľom na účely marketingu).

9. Oprávnená osoba je povinná dotknutú osobu predtým, než požiada o udelenie súhlasu so spracovaním jej osobných údajov, poskytnúť informácie v nevyhnutnom rozsahu, najmä identitu prevádzkovateľa, účel spracúvania osobných údajov a ďalšie informácie uvedené v jednotlivých vzorových dokumentoch – Súhlas dotknutej osoby. Oprávnená osoba v každom prípade nesmie zabudnúť na informačnú povinnosť prevádzkovateľa.

VIII. INFORMANČNÁ POVINNOSŤ

1. Nariadenie v ustanovení článku 12 a nasl. stanovuje prevádzkovateľovi tzv. informačnú povinnosť. V súlade s touto povinnosťou, prevádzkovateľ informuje dotknuté osoby v požadovanom rozsahu vhodným spôsobom.

2. V prípade zamestnancov a dohodárov je toto oznámenie vykonané vždy pri uzavretí pracovnej zmluvy, resp. dohody o výkone práce mimo pracovného pomeru. Dotknutá osoba potvrdí oboznámenie sa so zásadami spracúvania osobných údajov svojim podpisom na písomnom vyhotovení oznámenia.

3. Oznámenie voči Zákazníkom je dotknutým osobám poskytnuté vhodným spôsobom pri vzniku záväzkového vzťahu.

IX. ZÁZNAMY O SPRACOVATEĽSKÝCH ČINNOSTIACH

1. Podľa ustanovení nariadenia je každý prevádzkovateľ povinný viesť záznamy o spracovateľských činnostiach (ďalej aj ako „záznamy").

2. Povinnosť vedenia záznamov sa netýka takého prevádzkovateľa, ktorý je podnikom alebo organizáciou, zamestnávajúcou menej ako 250 osôb, a výlučne v takom prípade, kedy bude dochádzať ku spracúvaniu osobných údajov takým spôsobom, ktorý nie je možné považovať za rizikový a nebude závažným spôsobom zasahovať do práv a slobôd fyzických osôb.

3. Vychádzajúc z ustanovení nariadenia, bez ohľadu na počet zamestnancov musí záznamy viesť prevádzkovateľ:

   a. pokiaľ spracovanie, ktoré vykonáva, pravdepodobne predstavuje riziko pre práva a slobody dotknutých osôb;
   b. spracovanie nie je príležitostné, alebo;
   c. spracovanie zahŕňa spracovanie osobitých kategórií osobných údajov alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku

4. S ohľadom na skutočnosť, že prevádzkovateľ spracúva osobné údaje zamestnancov, dohodárov a uchádzačov o zamestnanie, ktoré zahŕňajú aj citlivé osobné údaje (o zdravotnom stave), prevádzkovateľ vedie záznamy o spracovateľských činnostiach v oblasti personálnej a mzdovej agendy.

5. Záznam o spracovateľských činnostiach obsahuje:
   a. identifikačné údaje a kontaktné údaje prevádzkovateľa a zodpovednej osoby, ak je určená,
   b. účel spracúvania osobných údajov,
   c. opis kategórií dotknutých osôb a kategórií osobných údajov,
   d. kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii
   e. označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos,
   f. predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,

g. všeobecný opis technických a organizačných bezpečnostných opatrení

6. Zákon umožňuje vedenie záznamov v písomnej alebo elektronickej podoby. Prevádzkovateľ bude viesť záznamy v elektronickej podobe.

X. USTANOVENIE ZODPOVEDNEJ OSOBY

1. Podľa ustanovenia článku 37 nariadenia je prevádzkovateľ povinný určiť zodpovednú osobu, ak je naplnená aspoň jedna z týchto podmienok stanovených alternatívne:
   a. spracúvanie osobných údajov vykonáva orgán verejnej moci alebo verejnoprávna inštitúcia okrem súdov pri výkone ich súdnej právomoci,
   b. hlavnými činnosťami prevádzkovateľa alebo Sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu, alebo
   c. hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií osobných údajov podľa ustanovenia článku 9 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku podľa článku 10 nariadenia.

   Ad. a.: Prevádzkovateľ nevykonáva spracúvanie osobných údajov ako /v postavení/ orgánu verejnej moci alebo verejnoprávnej inštitúcie. Na základe uvedeného, táto podmienka nie je naplnená.

   Ad. b.: Podľa odôvodnenia 97 GDPR v súkromnom sektore sa hlavné činnosti prevádzkovateľa týkajú jeho primárnych činností, a nie spracúvania osobných údajov ako vedľajšej činnosti. Podľa Usmernenia týkajúceho sa zodpovedných osôb, za hlavné činnosti možno považovať **kľúčové operácie nevyhnutné na dosiahnutie cieľov prevádzkovateľa.**

   Podľa Usmernenia týkajúceho sa zodpovedných osôb sa pri určovaní, či sa spracúvanie vykonáva voveľkom rozsahu, majú zohľadniť predovšetkým tieto faktory:
   - počet dotknutých osôb, ktorých sa spracúvanie týka, vyjadrený buď ako konkrétne číslo, alebo ako podiel príslušnej populácie,
   - objem údajov a/alebo rozsah rôznych položiek údajov, ktoré sa spracúvajú,
   - dĺžka trvania alebo stálosť (trvalosť) činnosti spracúvania údajov,
   - geografický rozsah spracovateľskej činnosti

   Podľa Usmernenia týkajúceho sa zodpovedných osôb, výklad výrazu „*pravidelné*“ zahŕňa jeden alebo viacero z týchto významov:
   - prebiehajúce alebo vyskytujúce sa v určitých intervaloch počas určitého obdobia,
   - opakovane sa vyskytujúce alebo opakované v pevne stanovených časoch,
   - odohrávajúce sa nepretržite alebo pravidelne

   Podľa Usmernenia týkajúceho sa zodpovedných osôb, výklad výrazu „*systematické*“ zahŕňa jeden alebo viacero z týchto významov:
   - vyskytujúce sa v súlade so systémom,
   - vopred naplánované, organizované alebo metodické,
   - odohrávajúce sa ako súčasť všeobecného plánu zberu údajov,
   - vykonávané v rámci stratégie

   Monitorovanie jednoznačne však zahŕňa všetky formy sledovania a profilovania na internete vrátane sledovania a profilovania na účely behaviorálnej reklamy.

   Pri hlavnej činnosti prevádzkovateľ spracúva osobné údaje klientov – fyzických osôb nepodnikateľov .Súčasne prevádzkovateľ spracúva osobné údaje zamestnancov, dohodárov, bývalých zamestnancov a dohodárov, uchádzačov o zamestnanie, externistov, konateľov.

   Hlavnými činnosťami prevádzkovateľa teda **niesú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah alebo účel vyžadujú pravidelné a systematické monitorovanie dotknutej osoby vo veľkom rozsahu**, a teda prevádzkovateľ **nespĺňa podmienku** podľa ustanovenia § 37 ods. 1 písm. b) Zákona.

Ad c.: Spracúvanie osobitných kategórií osobných údajov vo veľkom rozsahu alebo osobných údajov týkajúcich sa uznania viny za spáchanie trestného činu alebo priestupku:

Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby. Prevádzkovateľ spracúva osobné údaje týkajúce sa zdravia zamestnancov a dohodárov, a to potvrdenie o invalidite a potvrdenie o tehotenstve zamestnankyne. Prevádzkovateľ spracúva osobné údaje týkajúce sa zdravia svojich klientov a to vo veľkom rozsahu vzhľadom na hlavný predmet jeho činnosti. Vychádzajúc z Usmernenia týkajúceho sa zodpovedných osôb, v prípade prevádzkovateľa, s ohľadom na počet dotknutých osôb, rozsah spracúvaných osobných údajov, skutočnosť, že tieto osobné údaje týkajúce sa zdravia dotknutých osôb sa spracúvajú v súvislosti s jeho hlavným predmetom činnosti, ide o spracúvanie vo veľkom rozsahu.

Prevádzkovateľ vôbec nespracúva osobné údaje týkajúce sa uznania viny za spáchanie trestného činu alebo priestupku podľa vyššie uvedených ustanovení.

Prevádzkovateľ spĺňa podmienku podľa ustanovenia § 37 ods. 1 písm. c) Zákona.

2. **<u>Na základe vyššie uvedených úvah zastávame názor, že prevádzkovateľ je povinný ustanoviť tzv. zodpovednú osobu.</u>**

3. V prípade, že prevádzkovateľ určí / poverí zodpovednú osobu a registruje ju na Úrade pre ochranu osobných údajov sa uvádzajú nasledovné oprávnenia a povinnosti zodpovednej osoby, ktorých nositeľom v situácii nevymenovania zodpovednej osoby je štatutárny orgán spoločnosti.
4. V prípade, že prevádzkovateľ poveril dohľadom nad ochranou osobných údajov zodpovednú osobu, alebo viaceré zodpovedné osoby (v súlade s čl. 37 Nariadenia GDPR, resp. §44 a nasl. zákona), ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov, sú oprávnené osoby povinné dodržiavať príkazy tejto/týchto zodpovednej/zodpovedných osôb.
5. **Zodpovedná osoba zabezpečuje:**
   - poskytuje informácie a poradenstvo prevádzkovateľovi alebo sprostredkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie osobných údajov, o ich povinnostiach podľa Nariadenia GDPR, resp. zákona, osobitných predpisov alebo medzinárodných zmlúv, ktorými je Slovenská republika viazaná, týkajúcich sa ochrany osobných údajov,
   - monitoruje súlad s Nariadením GDPR, zákonom, osobitnými predpismi alebo medzinárodnými zmluvami, ktorými je Slovenská republika viazaná, týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa súvisiacimi s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy osôb, ktoré sú zapojené do spracovateľských operácií a súvisiacich auditov ochrany osobných údajov,
   - poskytuje na požiadanie poradenstvo, ak ide o posúdenie vplyvu na ochranu osobných údajov a monitorovanie jeho vykonávania podľa čl. 35 Nariadenia GDPR, resp. § 42 zákona,
   - spolupracuje s Úradom pri plnení svojich úloh,
   - plní úlohy kontaktného miesta pre úrad v súvislosti s otázkami týkajúcimi sa spracúvania osobných údajov vrátane predchádzajúcej konzultácie podľa čl. 36 Nariadenia GDPR, resp. § 43 zákona a podľa potreby aj konzultácie v iných veciach,
   - zodpovedná osoba pri výkone svojich úloh náležite zohľadňuje riziko spojené so spracovateľskými operáciami, pričom berie do úvahy povahu, rozsah, kontext a účel spracúvania osobných údajov,
   - dotknutá osoba môže kontaktovať zodpovednú osobu s otázkami týkajúcimi sa spracúvania jej osobných údajov a uplatňovania jej práv podľa Nariadenia GDPR, resp. zákona,
   - zodpovedná osoba je v súvislosti s výkonom svojich úloh viazaná povinnosťou mlčanlivosti v súlade s Nariadením GDPR, zákonom alebo osobitným predpisom,

   zodpovedná osoba môže plniť aj iné úlohy a povinnosti; prevádzkovateľ alebo sprostredkovateľ sú povinní zabezpečiť, aby žiadna z takýchto iných úloh alebo povinností neviedla ku konfliktu záujmov.
6. **Zodpovedná osoba zodpovedá za:**
   - aktualizáciu bezpečnostnej politiky,
   - údržbu bezpečnostnej dokumentácie a autorizáciu ich zmien príslušnými riadiacimi pracovníkmi a následnú aktualizáciu súvisiacej dokumentácie,

- riadenie školení pracovníkov - zodpovedná osoba, alebo iná poverená osoba vykoná poučenie pracovníkov o ich oprávneniach, právach a povinnostiach, o prístupoch do zamestnania v pracovnom čase a mimo pracovného času a o spôsobe narábania s údajmi, ktoré obsahujú osobné údaje; poučené musia byť aj osoby, ktoré nenarábajú s údajmi osobného charakteru, ak sú zamestnancami spoločnosti, alebo ak majú voľný prístup do priestorov spoločnosti (napr. upratovačka, údržbár a pod.).

7. **Zodpovedná osoba kontroluje:**
   - dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov,
   - dodržiavanie a plnenie bezpečnostnej dokumentácie,
   - pravidelnosť a dodržiavanie termínov údržby a profylaxie systému,
   - pravidelnosť a dodržiavanie termínov zálohovania,
   - správne uloženie záloh,
   - správne umiestnenie kľúčových prvkov.

XI. KONTROLNÉ ČINNOSTI – SPÔSOB,PERIODICITA, FORMA

1. **Kontrola informačného systému:**

1.1. Kontrola IS je vykonávaná na viacerých úrovniach:

a) kontrola miery rizika vzniku nebezpečenstva narušenia práv a slobôd dotknutých osôb začatím spracúvania zamýšľaných osobných údajov;

b) kontrola dodržiavania zásad spracúvania osobných údajov oprávnenými osobami;

c) kontrola prevádzky automatizovaného IS;

d) kontrola zabezpečenia objektu a miestností, v ktorých dochádza k spracúvaniu osobných údajov.

Ad a) Pred začatím spracúvania osobných údajov v informačnom systéme konateľ spoločnosti preverí, či vykonaním zamýšľaných spracovateľských operácií nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím alebo v priebehu spracúvania osobných údajov konateľ spoločnosti bezodkladne odstráni.

Ad b) Kontrola dodržiavania zásad spracúvania osobných údajov sa vykonáva v pravidelnej perióde, minimálne raz za rok.

Ad c) Kontrola Prevádzky automatizovaného informačného systému sa vykonáva nepretržite.

Ad d) Kontrola zabezpečenia miestností pred nedovoleným prístupom v mimopracovnom čase je vykonávaná denne osobou, ktorá posledná opúšťa priestory miestnosti v objekte.

XII. RIEŠENIE BEZPEČNOSTI SPRACÚVANIA OSOBNÝCH ÚDAJOV

1. Cieľom riešenia bezpečnosti je vytvoriť s minimálnymi nákladmi maximálnu ochranu informačného systému pred jeho možným narušením. Bezpečnosť informačného systému je nutné riešiť tak, aby riziká, ktorým je informačný systém vystavený, boli pomocou vhodných opatrení znížené na prijateľnú úroveň. Takéto riešenie potom zabezpečí elimináciu prevažnej časti rizík v kombinácii s vhodnými preventívnymi opatreniami ešte pred ich vznikom.
2. **Bezpečnosť zabezpečuje prevádzkovateľ na úrovni:**
   - ✓ **Personálnej**
     – *s citlivými informáciami sa zoznamuje iba osoba, ktorá ich potrebuje k výkonu svojej činnosti (oprávnená/poverená osoba).*
   - ✓ **Administratívnej**
     – *pomocou organizačných opatrení sa dosiahne výrazné zvýšenie bezpečnosti.*
   - ✓ **Fyzickej**

– chráni prostredie, v ktorom sa informačný systém prevádzkuje.

- ✓ **Počítačovej**
  – ochrana informačného systému a dát spracovávaných a prenášaných medzi počítačmi.
- ✓ **Vývojového prostredia**
  – bezpečný vývoj aplikácií, ktoré budú pracovať s citlivými informáciami.

3. Prevádzkovateľ a sprostredkovateľ sú povinní prijať so zreteľom na najnovšie poznatky, na náklady na vykonanie opatrení, na povahu, rozsah, kontext a účel spracúvania osobných údajov a na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva fyzických osôb primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej tomuto riziku, pričom uvedené opatrenia môžu zahŕňať najmä:

- *pseudonymizáciu a šifrovanie osobných údajov,*
- *zabezpečenie trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov spracúvania osobných údajov,*
- *proces obnovy dostupnosti osobných údajov a prístup k nim v prípade fyzického incidentu alebo technického incidentu,*
- *proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania osobných údajov.*

4. Pri posudzovaní **primeranej úrovne** bezpečnosti je potrebné prihliadať na riziká, ktoré predstavuje spracúvanie osobných údajov, a to najmä náhodné zničenie alebo nezákonné zničenie, strata, zmena alebo neoprávnené poskytnutie prenášaných osobných údajov, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo neoprávnený prístup k takýmto osobným údajom.

5. Zamestnanec prevádzkovateľa môže spracúvať osobné údaje dotknutých osôb len na základe pokynov prevádzkovateľa alebo podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

6. Prevádzkovateľ zabezpečí, aby neoprávneným osobám bol znemožnený akýkoľvek nedovolený prístup k spracúvaným osobným údajom.

7. Na základe informácií získaných analýzou spracúvania osobných údajov prevádzkovateľom bola analyzovaná primeranosť a stav personálnych, organizačných a technických opatrení. Stav a aktuálnosť jednotlivých opatrení ako i odporúčania prijatia sa nachádzajú v prílohe č. 1 k tejto smernici.

8. Analýza bezpečnosti informačného systému je rozbor, analyzovanie stavu bezpečnosti informačných systémov z hľadiska hrozieb, ktoré pôsobia na jednotlivé aktíva.

   8.1. Kvalitatívna analýza rizík:

   8.1.1. Vykonanou analýzou bezpečnosti informačných systémov obsahujúcich osobné údaje dotknutých osôb je **odhalenie bezpečnostných rizík**, ktorými v rámci informačných systémov môžu byť potenciálne útoky na:
   a. **dôvernosť IS**– zabezpečenie ochrany pred neoprávneným prístupom nepovolaných - neoprávnených osôb – napríklad hackerov, vlamačov, PC vírusov, odpočúvania, zneužitia, neoprávneného vyhotovovania rozmnožení,
   b. **integritu IS** – ochrana proti poškodeniu, zmene, vymazaniu a neplánovanému zničeniu,
   c. **dostupnosť IS** – ochrana proti výpadkom napájania a iným havarijným stavom.

   8.1.2. Analýzou vyššie spomínaných potenciálnych útokov akobezpečnostných rizík boli **identifikované hrozby**, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov:
   a. Neoprávnené prístupy zo strany nepovolaných osôb – hackerov
   - *návrh eliminácie hrozby: zabránenie prístupu do informačných systémov z internetu neoprávneným osobám, heslovanie počítačov, používanie antivírového programu.*
   b. Neoprávnený prístup zo strany nepovolaných osôb – vlamačov
   - *návrh eliminácie hrozby: bezpečnostné zámky na dverách, elektronická signalizácia narušenia objektu, riešenie kontrolovaného, evidovaného alebo obmedzeného prístupu zamestnancov, konateľov, návštevníkov a klientov* do objektu spoločnosti
   c. Poškodenie integrity informačných systémov počítačovými vírusmi

- *návrh eliminácie hrozby: antivírový program, firewall, zálohovanie dát*

d. Zneužitie rozsahu oprávnení oprávnenej osoby v rozsahu neoprávneného konania, ako napr. neoprávnené rozmnožovanie a rozširovanieosobných údajov

- *návrh eliminácie hrozby: vypracovanie tejto smernice, preškolenie oprávnených osôb, dostatočné poučenie o právach a povinnostiach oprávnenej osoby v rámci poverenia.*

e. Ochrana proti poškodeniu, zmene, vymazaniu a zničeniu osobných údajov v informačných systémoch

- *návrh eliminácie hrozby: dodržiavanie opatrení uvedených v prílohe č. 1*

f. Ochrana proti výpadkom napájania

- *návrh eliminácie hrozby: napojenie serveru a aktívnych prvkov siete na záložné zdroje*

g. Ochrana spracúvaných údajov pri likvidácii

- *návrh eliminácie hrozby: dodržiavanie opatrení uvedených v prílohe č. 1*

h. Ochrana proti požiaru:

- *návrh eliminácie hrozby: vypracovanie požiarneho plánu ochrany objektov*

8.1.3. Riziká, ktoré nie sú vyššie uvedené a nie je možné ich v uvedenom čase identifikovať – tzv. nepokryté riziká: nepokrytými rizikami sú udalosti, ktoré môžu nastať, a to z objektívnych alebo subjektívnych príčin, a ktoré v súčasnosti nie je možné dostatočne objektívne predvídať.

8.2. Bezpečnostné štandardy, metódy a prostriedky:

8.2.1. Ochrana pred neoprávneným prístupom zo strany nepovolaných osôb – hackerov: Technické vybavenie a prijaté opatrenia v Smernici dostatočne eliminujú riziko.

8.2.2. Ochrana pred neoprávneným prístupom zo strany nepovolaných osôb – vlamačov: Fyzická ochrana objektov je dostatočná, zabezpečujú ju mechanické zábrany vstupu. Vchod do budovy je zabezpečený spôsobom špecifikovaným v Prílohe č. 1.

8.2.3. Ochrana pred poškodením integrity informačných systémov počítačovými vírusmi: Súčasné vybavenie je dostatočné.

8.2.4. Ochrana pred zneužitím rozsahu oprávnení oprávnenej osoby, najmä k neoprávnenému rozmnožovaniu a rozširovaniu osobných údajov:

a. sú prijaté primerané opatrenia,
b. oprávnené osoby sú poučené o svojich povinnostiach v oblasti ochrany osobných údajov v zmysle zákona ako aj o povinnosti mlčanlivosti,
c. riešenia prístupových práv do informačného systému zabezpečuje nemožnosť tlačenia, resp. kopírovania dokumentov obsahujúcich osobné údaje neoprávnenou osobou. Dokument môžu vytlačiť, resp. kopírovať len tie oprávnené osoby, ktoré majú oprávnenie s údajmi pracovať – prístup k údajom v automatizovanej forme je zabezpečený vstupným heslom, v manuálnej forme umožnením prístupu do skríň (trezoru), kde sa informačný systém nachádza, iba oprávneným osobám,
d. zabezpečenie školenia všetkých oprávnených osôb k spracúvaniu osobných údajov v informačných systémoch (interné pravidlá, ustanovenia predpisov v konkrétnej oblasti) a stanovenie zodpovednosti oprávnenej osoby za porušenie povinností ochrany osobných údajov pri manipulácii s nimi a za porušenie povinnosti mlčanlivosti,
e. určenie oprávnených osôb na získavanie osobných údajov a spôsobu ich získavania,
f. miesta uloženia komponentov informačných systémov v manuálnej a automatizovanej podobe sú zabezpečené mechanickými zábranami.

8.2.5. Ochrana proti poškodeniu, zmene, vymazaniu a zničeniu osobných údajov v informačných systémoch: zálohovanie, prístup do informačných systémov, dátových nosičov i zariadení, v ktorých sa osobné údaje nachádzajú, alebo prostredníctvom ktorých je možný prístup do servera je chránený heslom. Bližší opis jednotlivých opatrení a návrhov je uvedený v Prílohe č. 1.

8.2.6. Ochrana informačných systémov v manuálnej podobe: Sú stanovené bezpečné miesta v kontrolovaných priestoroch, ako aj stanovené povinnosti zamestnancov chrániť údaje pred možnosťou nahliadnutia do nich inou neoprávnenou osobou prítomnou na pracovisku.

8.2.7. Ochrana proti výpadkom napájania:

a. je zabezpečené ukladanie spracúvaných dát v určenej periodicite na externý server *(všetky informačné systémy, v ktorých sa spracúvajú osobné údaje, sú umiestňované na externý server)*

b. ochrana proti požiaru spĺňa náležitosti zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov v zmysle vypracovaného požiarneho plánu ochrany objektu

8.2.8. Určenie a zabezpečenie miesta uschovávania osobných údajov v manuálnej podobe a zabezpečenie oddelenia prvkov informačných systémov v automatizovanej forme obsahujúcich osobné údaje od iných prvkov automatizovaných systémov, ktoré sú prístupné v rámci siete aj iným ako oprávneným osobám: nachádzajúce sa v Prílohe č. 1.

8.2.9. Určenie termínov a spôsobu likvidácie nepotrebných údajov po skončení účelu, na ktorý boli získavané a osôb zodpovedných za likvidáciu: Uvedené v prílohe č. 1. Ochrana spracúvaných údajov pri likvidácii je dostatočne zabezpečená, likvidujú sa protokolárne, za prítomnosti oprávnenej osoby a konateľa spoločnosti alebo ním poverenej osoby, v počítačovej podobe likviduje oprávnená osoba v spolupráci s osobou zodpovednou za výpočtovú techniku. O likvidácii je vyhotovený písomný záznam.

8.2. Posúdenie zhody bezpečnostných opatrení s použitými bezpečnostnými štandardami, metódami a prostriedkami:

a. Objekty, v ktorých sa nachádzajú komponenty informačných systémov, sú v rámci kontroly prístupu dostatočne zabezpečené pred vstupom nepovolaných osôb.

b. Objekt, v ktorom má sídlo Spoločnosť je z hľadiska požiarnej bezpečnosti vybavené zodpovedajúcimi hasiacimi prístrojmi a je spracovaný požiarny plán v zmysle zákona č. 314/2001 Z. z. o ochrane pred požiarmi v znení neskorších predpisov a spĺňa požiadavky stanovené týmto zákonom.

c. Fyzická bezpečnosť komponentov informačných systémov je štandardná. Ochrana osobných údajov v Spoločnosti je v súlade so Zákonom.

d. Neprijatie potrebných personálnych, organizačných a technických opatrení alebo nevykonanie vyššie uvedených navrhovaných opatrení môže u prevádzkovateľa viesť k vzniku bezpečnostného incidentu, ktorý môže viac či menej významne narušiť bezpečnosť spracúvaných osobných údajov u prevádzkovateľa a spôsobiť nemalé problémy, zvýšiť riziká pre dotknuté osoby a znížiť bezpečnosť spracúvaných osobných údajov.

e. Vzhľadom na súčasný stav a spôsob prevádzky informačných systémov a po prijatí potrebných opatrení vyplývajúcich z prílohy č. 1 nevzniká pre spoločnosť potreba ďalšieho financovania. Informačné systémy v spoločnostisú dôveryhodnými výpočtovými systémami.

XIII. BEZPEČNOSTNÉ INCIDENTY

1. **Týmto zavádzame postupy pri haváriách, poruchách a iných mimoriadnych situáciách (ďalej aj ako „bezpečnostný incident") vrátane preventívnych opatrení na zníženie pravdepodobnosti vzniku mimoriadnych situácií a možností efektívnej obnovy stavu z pred havárie. Štandardne zaužívanými postupmi pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému prevádzkovateľa s periodicitou najmenej raz ročne.**
2. Prevádzkovateľ je povinný oznámiť Úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel. To neplatí, ak **nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.**
   2.1. Zmeškanie uvedenej lehoty, resp. nesplnenie oznamovacej povinnosti je prevádzkovateľ povinný náležite odôvodniť.
   2.2. Oznámenie musí obsahovať najmä:
   - opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
   - kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
   - opis pravdepodobných následkov porušenia ochrany osobných údajov,
   - opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

   2.3. Prevádzkovateľ je povinný poskytnúť informácie v rozsahu, v akom sú mu známe v čase oznámenia. Ak v čase oznámenia nie sú prevádzkovateľovi známe všetky informácie, poskytne ich bezodkladne po tom, čo sa o nich dozvie.
3. Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.
4. Oznamovaciu povinnosť v čase vzniku bezpečnostného incidentu alebo hrozby vzniku bezpečnostného incidentu má i sprostredkovateľ voči prevádzkovateľovi, pričom je tak povinný vykonať bez zbytočného odkladu po tom, ako sa o danej skutočnosti dozvedel.
5. Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.
   5.1. Medzi obligatórne náležitosti oznámenia vzniku bezpečnostného incidentu patrí jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a informácie a opatrenia uvedené v čl. 33 ods. 3 nariadenia GDPR.
   5.2. Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, Úrad môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil, alebo môže rozhodnúť, že je splnená niektorá z vyššie uvedených podmienok.
   5.3. Oznámenie sa nevyžaduje, ak:
   a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
   b) prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia právdotknutej osoby,
   c) by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.
6. **Narušenie personálnej bezpečnosti:**

Narušenie personálnej bezpečnosti		
Bezpečnostný incident	**Hrozba**	**Navrhované riešenia**
Strata, vyzradenie alebo krádež hesiel pre vstup do	Môže dôjsť k narušeniu integrity, alebo zneužitiu osobných údajov	Zmena všetkých prihlasovacích hesiel do informačného systému a to ajadministrátorských; vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS; vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou.
Neoprávnený vstup neoprávnenej osoby	môže dôjsť k narušeniu integrity	Zmena všetkých prihlasovacích hesiel do

	alebo zneužitiu osobných údajov	informačného systému a to aj administrátorských; vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS; vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou.
Narušenie fyzickej bezpečnosti		
Bezpečnostný incident	**Hrozba**	**Navrhované riešenia**
Krádež počítača	môže dôjsť k zneužitiu osobných údajov	Zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran; zakúpenie nového počítača s vyššími bezpečnostnými prvkami, inštalácia systému a obnova dát zo záloh; zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.
Krádež, alebo strata kľúčov	môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi	Okamžitá výmena zámkov; prípadne doplnenie bezpečnostných ochrán IS - napr. inštalovaním senzorov; kamerových systémov; doplnkových mechanických zábran.
Strata záložných médií	môže dôjsť k zneužitiu osobných údajov	Zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
Krádež záložných médií	môže dôjsť k zneužitiu osobných údajov	Zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním senzorov, kamerových systémov, doplnkových mechanických zábran; zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
Narušenie technicko-softvérovej bezpečnosti		
Bezpečnostný incident	**Hrozba**	**Preventívne opatrenia**
Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača- serveru	X	Zabezpečiť záložné zdroje s automatickým shutdownom; monitorovať činnosť serverov, kontrolovať chybové hlásenia; v serveroch používať diskové polia s hotswap diskami; zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať server každé tri roky; zachovávať pravidlo - novší server sa stáva hlavným a starší záložným; zálohovať **Postup na zabezpečenie stavu obnovy** Pri výpadku servera presmerovať prevádzku na záložný server; obnova zo zálohy; presmerovať aplikácie a užívateľov na záložný server; odstrániť poruchu na hlavnomserveri; po odstránení poruchy presmerovať prevádzku na hlavný server.
Vírusová infiltrácia	môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi	Zabezpečiť antivírovú ochranu; inštalovať len autorizované programy oprávnenými zamestnancami; preverovať cudzie nosiče (FD, CD ROM, USB...); nepripájať nepreverené PC bez vedomia admin do LAN; nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN; neotvárať nevyžiadané e-mailové prílohy; sledovať aktuálne dianie na LAN a v sieti internet, **Postup na zabezpečenie stavu obnovy** odpojiť každého užívateľa; okamžitá kontrola aktualizácie antivírového programu, prípadná inštalácia aktualizácii, alebo zakúpenie kvalitnejšieho (z hľadiska bezpečnosti) antivírového programu; kontrola všetkých počítačov zapojených do spoločnej LAN siete, aktualizovaným antivírovým programom; detekovať spôsob narušenia; odstrániť príčiny; opraviť narušenú funkčnosť; opätovne skontrolovať systém antivírovým programom; prekontrolovať všetky PC; nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie; znovu spustiť systém a pripojiť užívateľov; inštalácia doplnkových programov, ktoré eliminujú možnosť napadnutia počítača.
Neautorizovaný vstup z internetu	môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými	nespúšťať programy z prostredia internetu nepodpísane certifikačnou autoritou; nesťahovať neautorizované programy z prostredia internetu,

	údajmi	**Postup na zabezpečenie stavu obnovy**
		kontrola log súborov firewallu, routerov, antivírového programu a pod. a ich vyhodnotenie; zabezpečiť súborovú integritu OS a obnovu poškodených alebo infikovaných údajov zo záloh; zvýšenie bezpečnosti firewallov; nastavenie kryptovaných prenosov v LAN sieti; pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite, prípadne využiť zabezpečenú VPN; inštalácia doplnkových programov, ktoré eliminujú možnosť napadnutia počítača z internetu.
Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS	pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát	v prípade vykazovania podozrivého správania je nutná výmena
	procesor - môže dôjsť k narušeniu integrity alebo strate dát	Nutná výmena
	CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát	v prípade že sa zistí že na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia
	harddisk – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát	v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh
	wifi zariadenie - môže dôjsť k úniku informácií a neautorizovanému vstupu do systému	nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia
Porucha napájania, strata dodávky elektrickej energie	x	dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia
		Postup na zabezpečenie stavu obnovy
		V čase výpadku sa musí záložný zdroj automaticky aktivovať; pri dlhodobejšom výpadku sa server musí automaticky korektne vypnúť (shutdown); po nábehu el. energie je nutné server spustiť a skontrolovať.
Porucha prostriedkov demilitarizovanej zóny	x	monitorovať činnosť zariadení; monitorovať funkčnosť všetkých zariadení; zabezpečiť prístup len pre pracovníkov s oprávnením; periodicky meniť administrátorské a užívateľské prístupy s heslami; zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu; zabezpečiť programovú aktuálnosť; zabezpečiť technickú aktuálnosť; kontrolovať súbory zaznamenávajúce činnosť systému; kontrolovať súbory;
		V prípade narušenia:
		odpojiť LAN od prostriedkov demilitarizovanej zóny; vyhľadať príčinu nefunkčnosti; odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku; preveriť prostriedky firewallu, prekladu adries (DNS) a proxy; po otestovaní funkčnosti pripojiť LAN
Porucha aktívnych prvkov siete	x	monitorovať činnosť; zabezpečiť dostatočnú kapacitu; pripájať ich prostredníctvom záložného zdroja; zabezpečiť dostatočnú ochranu pred nepovolaným prístupom; postup na zabezpečenie stavu obnovy: vymeniť nefunkčnú časť
Porucha pasívnej časti siete	x	Premeranie kabeláže, zásuviek a konektorov; postup na zabezpečenie stavu obnovy: opraviť, prípadne vymeniť chybnú časť
Havária databáz	x	Sledovať konfiguračné súbory; monitorovať hlásenia programov a včas na ne reagovať; denne kontrolovať chybové hlásenia aplikácie a databázy; postup na zabezpečenie stavu obnovy: po odstránení nedostatkov a kontrole spätne inštalovať databázu zo

		zálohy.
Havária aplikácie	x	Sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov; sledovať konfiguračné súbory; monitorovať hlásenia a včas na ne reagovať; denne kontrolovať chybové hlásenia aplikácie; Postup na zabezpečenie stavu obnovy: preinštalovať aplikáciu; nainštalovať novšiu verziu aplikácie; konzultovať chyby s dodávateľom.
Porucha pracovných staníc	x	Inštalovať antivírové programy; inštalovať nové programy smie len poverený zamestnanec; užívatelia nesmú zasahovať do konfiguračných súborov; chybové hlásenia sú povinný hlásiť správcovi systému; zálohovať dáta na určené média; za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec. Používať len autorizované programy; inštalovať antivírové programy; inštalovať nové programy smie len poverený zamestnanec; užívatelia nesmú zasahovať do konfiguračných súborov; chybové hlásenia sú povinný hlásiť správcovi systému; zálohovať dáta na určené média; za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec.
		Postup na zabezpečenie stavu obnovy
		Technická chyba – zabezpečiť opravu nefunkčnej časti; softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.
Narušenie dverí, okien	x	Pravidelne sledovať funkčnosť aktív
		Postup na zabezpečenie stavu obnovy
		neodkladne zabezpečiť opravu; hľadať príčinu a odstrániť
Narušenie monitorovaného objektu	x	pravidelne sledovať funkčnosť
		Postup na zabezpečenie stavu obnovy
		Hľadať a eliminovať príčinu narušenia.
Mimoriadne udalosti spôsobené vplyvom zvyškových rizík	x	Zabezpečiť niekoľkonásobné záložne kópie; zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti ; kontrolovať, či sú splnené protipožiarne opatrenia; kontrolovať osoby pri vstupe do budovy; vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere; zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov V prípade vyradenia aktív IS z činnosti: zvolať krízový štáb; koordinovať činnosť podľa bezpečnostnej dokumentácie – smernice; aktivovať záložne pracovisko; skontrolovať úplnosť systému na záložnom pracovisku; spustenie záložnej prevádzky; odstránenie škôd na pôvodnom pracovisku; po obnovení funkčnosti vrátenie činnosti na pôvodné pracovisko; v prípade napadnutia len časti aktív IS: presunúť aktíva do vyhovujúcich priestorov; inštalovať záložné databázy a pripojenia ak sú nutné; spustiť prevádzku, po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

GDPR

NAVRHOVANÉ OPATRENIA A ZHODNOTENIE NEDOSTATKOV PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV PREVÁDZKOVATEĽOM

GDPR

p.č.	Návrh opatrenia, odporúčanie alebo zhodnotenie nedostatku		Implementované dňa:	Podpis
1	PRIJMITE PRIMERANÉ PERSONÁLNE, TECHNICKÉ A ORGANIZAČNÉ OPATRENIA NAVRHOVANÉ V PRÍLOHE Č. 1 SMERNICE GDPR			
2	USKUTOČNITE VŠETKY POSTUPY IMPLEMENTÁCIE DOKUMENTÁCIE UVEDENÉ V DORUČENOM MANUÁLI IMPLEMENTÁCIE GDPR, A TO NAJMÄ:			
2.1	UPRAVTE SPRACÚVANIE OSOBNÝCH ÚDAJOV VOČI ZAMESTNANCOM A POTENCIONÁLNYM ZAMESTNANCOM	Oboznámte súčasného zamestnanca so zásadami spracúvania osobných údajov a jeho právami podľa čl. 13 nariadenia GDPR		
		Upravte pracovné zmluvy a jednotlivé dohody podľa navrhovaného doplnenia za účelom naplnenia informačnej povinnosti podľa čl. 13 nariadenia GDPR voči novým zamestnancom a dohodárom		
		Zlikvidujte kópie a scany občianskych a vodičských preukazov zamestnancov, ktoré evidujete.		
		Zlikvidujte osobné údaje uchádzačov o zamestnanie, na ktorých evidenciu nedisponujete súhlasom a v konkrétnom výberovom konaní boli neúspešní.		
		Zlikvidujte osobné údaje uchádzačov o zamestnanie, ktoré ste prijali mimo výberového konania a nedisponujete súhlasom dotknutej osoby na ich evidenciu.		
		V prípade, ak spracúvate také osobné údaje zamestnancov, ktorých právnym základom je súhlas, ktorý vám zamestnanec neudelil, ste povinní takéto údaje ďalej nespracúvať a zabezpečiť likvidáciu. To isté platí i po odvolaní súhlasu. Zákonnosť spracúvania po dobu, kedy ste súhlasom disponovali nie je dotknutá.		
2.2	NAPLŇTE INFORMAČNÉ POVINNOSTI VOČI DOTKNUTÝM OSOBÁM To, ako uplatníte informačné povinnosti, je už na Vás, dbajte však na povinnosť preukázať naplnenie tejto povinnosti.			
2.3	SPRACÚVAJTE OSOBNÉ ÚDAJE V SÚLADE SO ZÁSADOU ZÁKONNOSTI			
2.4	POVERTE A POUČTE OPRÁVNENÉ OSOBY			
2.5	UZATVORTE ZMLUVY SO SPROSTREDKOVATEĽOM Na základe analýzy bola zistená skutočnosť, že spolupracujete s externými dodávateľmi rôznych služieb. Takéto subjekty voči Vám vystupujú ako sprostredkovateľ (ustanovenie čl. 28 Nariadenia GDPR). So sprostredkovateľmi ste povinní uzatvoriť zmluvu upravujúcu jednotlivé práva a povinnosti pri spracúvaní osobných údajov. Pre každý účel je pripravená samostatná zmluva. Ak bude potrebné uzatvoriť zmluvu s ďalším sprostredkovateľom, môžete (po príslušných úpravách) použiť niektorú z nami pripravených zmlúv. Sprostredkovateľské zmluvy, ktoré už máte uzatvorené, meniť nemusíte, rozdiely na úrovni právneho názoru posudzovať nebudeme. Je teda na Vás, pre ktoré znenia zmlúv sa rozhodnete (pre naše / pre Vaše / pre kombináciu). My, samozrejme, odporúčame používať nami pripravené texty.			
2.6	POUČTE NEOPRÁVNENÉ OSOBY O POVINNOSTI ZACHOVÁVAŤ MLČANLIVOSŤ			
2.7	ZAVEĎTE PROCESY KONTROLY SPRACÚVANIA OSOBNÝCH ÚDAJOV OPRÁVNENÝMI OSOBAMI A VAŠIMI SPROSTREDKOVATEĽMI			
2.8	OZNAČTE PRIESTORY MONITOROVANÉ KAMERAMI NÁLEPKAMI			
2.9	PRAVIDELNE AKTUALIZUJTE ZÁZNAMY O SPRACOVATEĽSKÝCH ČINNOSTIACH PREVÁDZKOVATEĽA			
3	DODRŽIAVAJTE ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV			

4	AKÉKOĽVEK KOPÍROVANIE ALEBO SKENOVANIE OSOBNÝCH DOKLADOV ZAMESTNANCOV ALEBO KLIENTOV JE V ROZPORE SO ZÁSADOU MINIMALIZÁCIE OSOBNÝCH ÚDAJOV, ČO ZNAMENÁ, ŽE I V ROZPORE S NARIADENÍM GDPR. TAKÉTO VYHOTOVOVANIE ROZMNOŽENÍN NEODPORUJE ZÁSADÁM OCHRANY OSOBNÝCH ÚDAJOV V TÝCH PRÍPADOCH, KEDY JE PREVÁDZKOVATEĽ K TAKÉMUTO KONANIU ZAVIAZANÝ PRÁVNYMI PREDPISMI, NAPR. PRI IDENTIFIKÁCII KLIENTA PODĽA ZÁKONA Č. 297/2008 Z.Z. O OCHRANE PRED LEGALIZÁCIOU PRÍJMOV Z TRESTNEJ ČINNOSTI A O OCHRANE PRED FINANCOVANÍM TERORIZMU A O ZMENE A DOPLNENÍ NIEKTORÝCH ZÁKONOV V ZNENÍ NESKORŠÍCH PREDPISOV.		
	V ANALÝZE UVÁDZATE, ŽE NEVEDIETE EVIDENCIU UCHÁDZAČOV O ZAMESTNANIE A ŽIVOTOPISY PO UKONČENÍ VÝBEROVNÉHO KONANIA LIKVIDUJETE. PO UKONČENÍ VÝBEROVÉHO KONANIA MÁTE POVINNOSŤ ŽIVOTOPISY AKO AJ INÉ NOSIČE OSOBNÝCH ÚDAJOV LIKVIDOVAŤ S VÝNIMKOU PRÍPADU, AK DISPONUJETE VÝSLOVNÝM SÚHLASOM DOTKNUTEJ OSOBY (UCHÁDZAČA O ZAMESTNANIE) SO SPRACOVANÍM JEJ OSOBNÝCH ÚDAJOV ZA ÚČELOM VEDENIA EVIDENCIE UCHÁDZAČOV O ZAMESTNANIE A MOŽNOSTI JEJ NÁSLEDNÉHO KONTAKTOVANIA V PRÍPADE UVOĽNENIA ĎALŠIEHO MIESTA. KAŽDÝ SÚHLAS DOTKNUTEJ OSOBY MUSÍ MAŤ VŠETKY NÁLEŽITOSTI POŽADOVANÉ PREDPISMI. AK EVIDENCIU UCHÁDZAČOV O ZAMESTNANIE NEVEDIETE A TAK, AKO STE UVIEDLI, ŽIVOTOPISY LIKVIDUJETE, SPRACÚVATE OSOBNÉ ÚDAJE NA INOM PRÁVNOM ZÁKLADE NEŽ SÚHLASE. Z DANÉHO DÔVODU SI SÚHLAS PÝTAŤ NEMUSÍTE (ZA NAPLNENIA VYŠŠIE SPOMENUTÝCH PODMIENOK)		
	ZÁZNAMY Z KAMEROVÉHO SYSTÉMU ODPORUČAME LIKVIDOVAŤ V LEHOTE NAJNESKÔR DO 72 HODÍN ODO DŇA ICH VYHOTOVENIA. DLHŠIA LEHOTA MÔŽE BYŤ POSUDZOVANÁ ZA NEPRIMERANÚ, AK VŠAK POTREBUJETE Z URČITÉHO DÔVODU DLHŠIE UCHOVÁVAŤ ZÁZNAMY Z KAMEROVÉHO SYSTÉMU, MUSÍTE TO PODLOŽIŤ DOSTATOČNÝMI ODÔVODNENÝMI ARGUMENTAMI.		
	UPOZORŇUJEME VÁS NA OBMEDZENIA, TÝKAJÚCE SA SPRACÚVANIA RODNÉHO ČÍSLA. V zmysle ustanovenia § 78, ods. 4 Zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov (ďalej len „Zákon o ochrane osobných údajov") je možné použiť rodné číslo iba vtedy, ak je to nevyhnutné na dosiahnutie daného účelu spracúvania. To znamená, že v prípade, že takéto spracúvanie potrebné nie je (napr. pri uzatváraní bežnej zmluvy), nie je dovolené spracúvať rodné číslo.		

UPOZORNENIE:

JEDNOTLIVÉ ODOVZDANÉ DOKUMENTY BOLI VYPRACOVANÉ ZA ÚČELOM NAPLNENIA POVINNOSTÍ, KTORÉ VÁM Z PREDPISOV V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV VYPLÝVAJÚ. POVINNOSTI SME VYGENEROVALI NA ZÁKLADE PREDLOŽENÝCH DOKUMENTOV, VYKONANEJ ANALÝZY A POSKYTNUTÝCH INFORMÁCIÍ. VZHĽADOM NA SKUTOČNOSŤ, ŽE DOKUMENTY VYPRACUVÁVAME K AKTUÁLNEMU STAVU, DOKUMENTÁCIA NEOBSAHUJE INFORMÁCIE O ÚČELOCH SPRACÚVANIA, KTORÉ NEVYKONÁVATE, RESP. BUDETE MAŤ ZÁUJEM VYKONÁVAŤ V BUDÚCNOSTI (AKO NAPR. MARKETING, UBYTOVACIE SLUŽBY A POD.). AKÉKOĽVEK ZMENY, DOPLNENIA ÚČELOV SPRACÚVANIA OSOBNÝCH ÚDAJOV A POD. JE POTREBNÉ KONZULTOVAŤ A DOKUMENTY O TIETO SKUTOČNOSTI AKTUALIZOVAŤ. DOKUMENTÁCIA REFLEKTUJE STAV KU DŇU VYKONANIA ANALÝZY.

Dňa:	GDPR