

Dokumentácia k ochrane osobných údajov

**názov združenia: Slovenská spoločnosť všeobecného
praktického lekárstva, so sídlom: Stredná 17435/80, 821 04
Bratislava-Ružinov, IČO: 35 607 131, registrácia: Evidencia
občianskych združení, Ministerstvo vnútra Slovenskej
republiky, sekcia verejnej správy**

OBSAH	
ČASŤ A	6
VYMEDZENIE A POPIS INFORMAČNÝCH SYSTÉMOV	6
I. ÚVOD	6
II. NÁZOV INFORMAČNÉHO SYSTÉMU: EVIDENCIA ČLENOV SPOLOČNOSTI	7
III. NÁZOV INFORMAČNÉHO SYSTÉMU: PLATENIE ČLENSKÉHO PRÍSPEVKU	8
IV. NÁZOV INFORMAČNÉHO SYSTÉMU: MZDOVÁ AGENDA	10
V. NÁZOV INFORMAČNÉHO SYSTÉMU: PERSONÁLNA AGENDA	14
VI. NÁZOV INFORMAČNÉHO SYSTÉMU: AGENDA BEZPEČNOSTI A OCHRANY ZDRAVIA PRI PRÁCI	17
VII. NÁZOV INFORMAČNÉHO SYSTÉMU: EVIDENCIA PRIJATEJ A ODOSLANEJ POŠTY	19
VIII. NÁZOV INFORMAČNÉHO SYSTÉMU: HLASOVANIE ČLENOV SPOLOČNOSTI	20
IX. NÁZOV INFORMAČNÉHO SYSTÉMU: ÚČTOVNÉ DOKLADY	22
X. NÁZOV INFORMAČNÉHO SYSTÉMU: SÚSTAVNÉ VZDELÁVANIE ZDRAVOTNÍCKYCH PRACOVNÍKOV	24
XI. NÁZOV INFORMAČNÉHO SYSTÉMU: USPORADÚVANIE PODUJATÍ	26
XII. NÁZOV INFORMAČNÉHO SYSTÉMU: AUTORSKÉ A LICENČNÉ ZMLUVY	28
XIII. NÁZOV INFORMAČNÉHO SYSTÉMU: HLÁSENIE POSKYTNUTIA PEŇAŽNÉHO/NEPEŇAŽNÉHO PLNENIA	29
XIV. NÁZOV INFORMAČNÉHO SYSTÉMU: VYHOTOVOVANIE ZÁZNAMOV Z PODUJATÍ	32
XV. NÁZOV INFORMAČNÉHO SYSTÉMU: ZVEREJŇOVANIE ZÁZNAMOV Z PODUJATÍ	33
XVI. NÁZOV INFORMAČNÉHO SYSTÉMU: MARKETING	35
XVII. NÁZOV INFORMAČNÉHO SYSTÉMU: ZVEREJŇOVANIE ÚDAJOV O ČLENOCH ORGÁNOV SPOLOČNOSTI	37
XVIII. NÁZOV INFORMAČNÉHO SYSTÉMU: SÚDNE SPORY	38
XIX. NÁZOV INFORMAČNÉHO SYSTÉMU: UPLATŇOVANIE PRÁV DOTKNUTÝCH OSÔB	40
XX. VYMEDZENIE OKOLIA INFORMAČNÉHO SYSTÉMU	41
XXI. ZÁVEREČNÉ USTANOVENIA	41
ČASŤ B	43
KVALITATÍVNA ANALÝZA RIZÍK BEZPEČNOSTI INFORMAČNÝCH SYSTÉMOV	43
I. ÚVOD	43
II. METODIKA ANALÝZY RIZÍK	43
III. IDENTIFIKÁCIA A OHODNOTENIE INFORMAČNÝCH AKTÍV	43
IV. IDENTIFIKÁCIA A OHODNOTENIE HROZIEB	44
V. IDENTIFIKÁCIA A OHODNOTENIE ZRANITEĽNOSTI	44
VI. STANOVENIE RIZIKA	45
VII. ANALÝZA A VYHODNOTENIE RIZIKA ZLYHANIA BEZPEČNOSTI	46
VIII. VYHODNOTENIE ANALÝZY RIZÍK BEZPEČNOSTNÉHO SYSTÉMU	49
IX. ZÁVEREČNÉ USTANOVENIA	50
ČASŤ C	51
ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA OSOBNÝCH ÚDAJOV	51
I. TECHNICKÉ OPATRENIA	51
II. PERSONÁLNE OPATRENIA	53
III. LIKVIDÁCIA OSOBNÝCH ÚDAJOV A DÁTOVÝCH NOSIČOV	55
IV. KONTROLNÁ ČINNOSŤ	55
V. ZÁVEREČNÉ USTANOVENIA	55
ČASŤ D	57
ZÁKLADNÉ ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV	57
I. ÚVOD	57
II. ZÁKONNOSŤ, SPRAVODLIVOSŤ A TRANSPARENTNOSŤ	57
III. OBMEDZENIE ÚČELU	58
IV. MINIMALIZÁCIA ÚDAJOV	58
V. ZÁSADA SPRÁVNOSTI	58
VI. MINIMALIZÁCIA UCHOVÁVANIA	59
VII. INTEGRITA A DÔVERNOSŤ	59
VIII. ZODPOVEDNOSŤ	59
IX. ZÁVEREČNÉ USTANOVENIA	60
ČASŤ E	61

PRÁVA DOTKNUTEJ OSOBY	61
I. VŠEOBECNÉ PRAVIDLÁ PRE POSTUP PRI VÝKONE PRÁV DOTKNUTEJ OSOBY	61
II. PRÁVO NA PRÍSTUP K ÚDAJOM	62
III. PRÁVO NA OPRAVU A VYMAZANIE	62
IV. PRÁVO NA OBMEDZENIE SPRACÚVANIA	63
V. INFORMAČNÁ POVINNOSŤ PRI OPRAVE, VYMAZANÍ ALEBO OBMEDZENÍ SPRACÚVANIA	64
VI. PRÁVO NA PRENOSNOSŤ ÚDAJOV	64
VII. PRÁVO NAMIETAŤ	64
VIII. AUTOMATIZOVANÉ ROZHODOVANIE A PROFILOVANIE	65
IX. ZÁVEREČNÉ USTANOVENIA	65
ČASŤ F	66
POVINNOSTI SPOLOČNOSTI PRI PLNENÍ INFORMAČNÝCH POVINNOSTI	66
I. ROZSAH INFORMAČNEJ POVINNOSTI	66
II. REALIZÁCIA INFORMAČNEJ POVINNOSTI	66
III. ZÁVEREČNÉ USTANOVENIA	67
ČASŤ G	68
POVINNOSTI SPOLOČNOSTI PRI UPLATŇOVANÍ PRÁV DOTKNUTÝCH OSÔB	68
I. ÚVOD	68
II. PRIJATIE ŽIADOSTI ZO STRANY DOTKNUTEJ OSOBY	68
III. POSTÚPENIE ZODPOVEDNÉMU ZAMESTNANCOVI NA VYBAVENIE ŽIADOSTI DOTKNUTEJ OSOBY	68
IV. PREVERENIE OPRÁVNENOSTI ŽIADOSTI	68
V. ČINNOSŤ ZODPOVEDNÉHO ZAMESTNANCA PRE ZABEZPEČENIE ODPOVEDE PRE DOTKNUTÚ OSOBU	68
VI. ZÁVEREČNÉ USTANOVENIA	69
ČASŤ H	70
HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV	70
I. VŠEOBECNÉ PRAVIDLÁ	70
II. HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV DOZORNÉMU ORGÁNU	70
III. HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV DOTKNUTEJ OSOBE	71
IV. ODPORÚČANÉ POSTUPY PRI HAVÁRIÁCH, PORUCHÁCH A INÝCH MIMORIADNYCH SITUÁCIÁCH	71
V. ZÁVEREČNÉ USTANOVENIA	73
ČASŤ I	75
KLÚČOVÝ REŽIM SPOLOČNOSTI A POVINNOSTI DRŽITEĽOV KLÚČOV	75
I. KLÚČOVÝ REŽIM PREVÁDZKOVATEĽA A POVINNOSTI DRŽITEĽOV KLÚČOV	75
II. ZÁVEREČNÉ USTANOVENIA	75
ČASŤ J	77
SMERNICA O ROZSAHU PRÁV, POVINNOSTÍ A ZODPOVEDNOSTI SPOLOČNOSTI A OPRÁVNENÝCH OSÔB	77
I. VŠEOBECNÉ USTANOVENIA	77
II. PRÁVA A POVINNOSTÍ SPOLOČNOSTI (PREVÁDZKOVATEĽA)	77
III. PRÁVA A POVINNOSTÍ OPRÁVNENÝCH OSÔB	77
IV. ROZSAH OPRÁVNENÍ A POPIS POVOLENÝCH ČINNOSTÍ OPRÁVNENÝCH OSÔB	78
V. ROZSAH ZODPOVEDNOSTÍ OPRÁVNENÝCH OSÔB	79
VI. ZÁVEREČNÉ USTANOVENIA	79
ČASŤ K	81
PRAVIDLÁ POUŽÍVANIA ZÁKLADNÝCH DOKUMENTOV V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV	81
I. VŠEOBECNÉ PRAVIDLÁ PRE POUŽÍVANIE DOKUMENTOV	81
II. INFORMÁCIE PRE ÚČASTNÍKOV ODBORNÉHO PODUJATIA O SPRACOVANÍ OSOBNÝCH ÚDAJOV	81
III. INFORMÁCIE PRE ZAMESTNANCOV O SPRACOVANÍ OSOBNÝCH ÚDAJOV	82
IV. ZÁZNAM O SPRACOVATEĽSKÝCH ČINNOSTIACH	82
V. POUČENIE O POVINNOSTI ZACHOVÁVAŤ MLČANLIVOSŤ A OCHRANU OSOBNÝCH ÚDAJOV PRE ZAMESTNANCA SPOLOČNOSTI	83
VI. ZÁZNAM O POUČENÍ OPRÁVNENÝCH OSÔB	83
VII. ZMLUVA O SPRACOVANÍ OSOBNÝCH ÚDAJOV	84
VIII. ZÁZNAM O NUTNOSTI VYPRACOVAŤ POSÚDENIE VPLYVU NA OCHRANU OSOBNÝCH ÚDAJOV	84

IX.	ZÁZNAM O NUTNOSTI URČIŤ ZODPOVEDNÚ OSOBU	84
X.	SÚHLAS SO SPRACOVANÍM OSOBNÝCH ÚDAJOV	85
XI.	VZOROVÝ FORMULÁR PRE ZDOKUMENTOVANIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV	86
XII.	ZÁVEREČNÉ USTANOVENIA	86

Vážený klient,

ďakujeme Vám za prejavenu dôveru pri vypracovaní dokumentácie k ochrane osobných údajov.

Dokumentácia, ktorá je pre Vás vypracovaná zahŕňa minimálne štandardy, ktoré je potrebné dodržiavať pri práci s osobnými údajmi, ako aj odporúčania pri zabezpečení osobných údajov a ich správnom spracúvaní vo Vašom združení Slovenská spoločnosť všeobecného praktického lekárstva (ďalej v celom dokumente aj ako „spoločnosť“).

Majte na pamäti, že dodržiavanie pravidiel ochrany osobných údajov nekončí pri podpise tejto Dokumentácie k ochrane osobných údajov (ďalej v celej dokumentácii budeme označovať len ako „dokumentácia“ alebo „smernica“) a podrobnom oboznámení sa s ňou, ale pravidlá obsiahnuté v tejto dokumentácii je nevyhnutné aplikovať v každodennej praxi vo Vašej spoločnosti. Rovnako je nevyhnutné, aby ste dohliadali aj na prácu osôb oprávnených spracúvať osobné údaje, pretože za zákonné zaobchádzanie s osobnými údajmi zodpovedá prevádzkovateľ (spoločnosť).

Vymedzenie informačných systémov sa uskutočnilo prostredníctvom vstupných informácií, ktoré ste nám poskytli. V prípade ak dôjde k akejkoľvek zmene činnosti vykonávaných v spoločnosti alebo ste na nejaký informačný systém zabudli, je potrebné upraviť popis informačných systémov, aby zodpovedali skutočnému stavu spoločnosti a splniť si povinnosti prislúchajúce informačnému systému.

Hodnotenie rizík informačných systémov, ktoré sa nachádza v Časti B je potrebné si nezamieňať s povinnosťou vykonať posúdenie vplyvu na ochranu osobných údajov v zmysle § 35 GDPR. V prípade, že na základe vykonanej analýzy rizík spoločnosť dospeje k záveru, že spracúvanie osobných údajov vo Vašej spoločnosti povedie k vysokému riziku ochrany osobných údajov je nevyhnutné vypracovať posúdenie vplyvu na ochranu osobných údajov.

Odporúčame Vám dodržiavať špecificky navrhnutú a štandardnú ochranu osobných údajov spôsobom vymedzeným v Časti C a implementovať zásady spracúvania osobných údajov vo Vašej spoločnosti, ktorých výsledkom je eliminácia a prípadne odstránenie rizík ochrany osobných údajov. Nevyhnutnú pozornosť je potrebné venovať aj právam dotknutých osôb a povinnostiam spoločnosti a pravidelnému preškoľovaniu personálu spoločnosti ako zaobchádzať s osobnými údajmi.

Opätovne si Vás dovoľujeme upozorniť, že vypracovaním dokumentácie, jej podpisom príslušnými osobami, nekončí Vaša práca v oblasti ochrany osobných údajov. Máte pripravené všetky potrebné podklady s návodom ako ich správne používať a s popisom ako sa správať vo vybraných situáciách, napriek tomu dodržiavanie zákonných predpisov a ich uplatňovanie v praxi spoločnosti je už na samotnom prevádzkovateľovi (spoločnosť).

Prajeme Vám veľa šťastia pri uplatňovaní pravidiel ochrany osobných údajov a tešíme sa na ďalšiu spoluprácu.

V tomto čase Úrad na ochranu osobných údajov ako aj Európsky výbor pre ochranu osobných údajov (EDPB) vydáva usmernenia a metodické pokyny pri aplikácii novej právnej úpravy týkajúcej sa ochrany osobných údajov, názory na niektoré otázky sú doposiaľ nejednotné, preto je možné, že v priebehu najbližšieho obdobia bude potrebné dokumentáciu prispôbovať vydaným odporúčaniam, preto Vám odporúčame, aby ste sledovali najmä stránku Úradu na ochranu osobných údajov <https://dataprotection.gov.sk/uouu/sk> a stránku Európskeho výboru pre ochranu osobných údajov <https://edpb.europa.eu> a vykonávali pravidelný audit. Odovzdávame Vám dokumentáciu so stavom ku dňu 25.5.2018. V prípade ohlásenia kontroly zo strany Úradu na ochranu osobných údajov nás ihneď kontaktujte, aby sme zaistili prípadne nezrovnalosti od odovzdania dokumentácie a mohli zapracovať aktuálny stav osobných údajov vo Vašej spoločnosti.

Časť A VYMEDZENIE A POPIS INFORMAČNÝCH SYSTÉMOV

I. Úvod

1. Osobné údaje je možné spracúvať len na základe príslušného právneho základu a len na stanovený účel. Osobné údaje sú preto usporiadané do informačných systémov, ktoré predstavujú usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určitých kritérií.
2. Každému informačnému systému zodpovedá príslušný právny základ a príslušný účel spracúvania osobných údajov.
3. Osobné údaje uvedené v jednotlivých informačných systémoch sa spracúvajú oddelene a nie je možné ich kombinovať bez primeraného právneho odôvodnenia a bez predchádzajúceho posúdenia zodpovedného zamestnanca spoločnosti alebo právneho konzultanta.
4. Osobné údaje sa v spoločnosti spracúvajú výlučne v informačných systémoch uvedených v tomto dokumente.
5. V prípade ak dôjde k akejkoľvek zmene činností vykonávaných našou spoločnosťou, je potrebné zoznam informačných systémov upraviť tak, aby zodpovedali skutočnému stavu v spoločnosti. Tieto zmeny je možné vykonať len postupom podľa ods. 3 a 4 tejto časti smernice.
6. Informácie uvedené v tomto dokumente predstavujú jeden zo základných zdrojov informácií pre ostatné povinné dokumenty v oblasti osobných údajov. V prípade ak dôjde k akejkoľvek zmene v zozname alebo v popise jednotlivých informačných systémov, je potrebné tieto zmeny náležite zohľadniť v ostatných súvisiacich dokumentoch postupom podľa ods. 3 a 4 tejto časti smernice.
7. Ku dňu účinnosti tejto smernice spoločnosť prevádzkuje nasledovné informačné systémy:
 - a) Evidencia členov spoločnosti
 - b) Platenie členského príspevku
 - c) Mzdová agenda
 - d) Personálna agenda
 - e) Agenda bezpečnosti a ochrany zdravia pri práci
 - f) Evidencia prijatej a odoslanej pošty
 - g) Hlasovanie členov spoločnosti
 - h) Účtovné doklady
 - i) Sústavné vzdelávanie zdravotníckych pracovníkov
 - j) Usporadúvanie podujatí
 - k) Autorské a licenčné zmluvy
 - l) Hlásenie poskytnutia peňažného/nepenažného plnenia
 - m) Vyhотовovanie záznamov z podujatí
 - n) Zverejňovanie záznamov
 - o) Marketing
 - p) Zverejňovanie údajov o členoch orgánov spoločnosti
 - q) Súdne spory
 - r) Uplatňovanie práv dotknutých osôb

II. Názov informačného systému: Evidencia členov spoločnosti

1. Kategórie dotknutých osôb:

- a) Evidencia registrovaných členov spoločnosti
- b) Registrácia nových členov spoločnosti

2. Účel spracúvania osobných údajov

Identifikácia evidovaných členov spoločnosti a prihlasovanie nových členov spoločnosti.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

4. Rozsah osobných údajov

- a) meno, priezvisko a titul,
- b) rodné číslo,
- c) registračné číslo v Slovenskej lekárskej komore,
- d) adresa,
- e) e-mailová adresa,
- f) podpis.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené v listinnej podobe a niektoré sú vedené v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z.z. Civilný sporový poriadok v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v tomto informačnom systéme pre spoločnosť spracúva spoločnosť FARMÍ – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Prevádzkovanie webovej stránky je zabezpečené prostredníctvom sprostredkovateľa: Websupport, s.r.o., so sídlom: Staré Grunty 12, 841 04 Bratislava, IČO: 36 421 928 (ďalej aj ako „spoločnosť zabezpečujúca webhosting“). Spravovanie stránky pre spoločnosť zabezpečuje externá osoba ako sprostredkovateľ: obchodné meno: Ing. Marek Štefunko, s miestom podnikania: Juraja Slottu 6475/39, 917 01 Trnava, IČO: 48 303 330 (ďalej aj ako „osoba zabezpečujúca správu stránky“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v tomto informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia údajov z mailového konta. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto IS je vyjadrená dobou trvania členstva v spoločnosti.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v listinnej podobe je zabezpečená v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme evidencia členov spoločnosti pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť, externá osoba, spoločnosť zabezpečujú webhosting a osoba zabezpečujúca správu stránky, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1500. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.**

III. Názov informačného systému: Platenie členského príspevku

1. Kategórie dotknutých osôb:

- a) Členovia spoločnosti

2. Účel spracúvania osobných údajov

Prijímanie a evidencia finančných príspevkov členov na činnosť spoločnosti podľa stanov.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

Spoločnosť získava osobné údaje (rok zloženia špecializačnej skúšky) na účel zníženia príspevku člena na činnosť SSVPL v zmysle článku 6 ods. 4 GDPR.

4. Rozsah osobných údajov

- a) meno, priezvisko a titul,
- b) adresa,
- c) e-mailová adresa,
- d) rok zloženia špecializačnej skúšky

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené v listinnej podobe a niektoré sú vedené v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z.z. Civilný sporový poriadok v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme platenie členského príspevku pre spoločnosť spracúva externá spoločnosť: FARMI – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba, obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v tomto informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzický zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia údajov z mailového konta. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto IS je vyjadrená dobou trvania členstva v spoločnosti.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v listinnej podobe je zabezpečená v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Mzdovú agendu pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

Agendu platenia členského príspevku pre spoločnosť spracúva externá spoločnosť ako sprostredkovateľ, s ktorou má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1500. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

IV. Názov informačného systému: Mzdová agenda

1. Kategórie dotknutých osôb:

- b) zamestnanci
- c) vyživované deti zamestnancov
- d) bývalí zamestnanci

2. Účel spracúvania osobných údajov

Plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom alebo obdobným vzťahom (napríklad na základe dohôd o prácach vykonávaných mimo pracovného pomeru). V rámci predmetného informačného systému dochádza k plneniu hlavného účelu aj prostredníctvom:

- a) spracúvania potrebných štatistických výkazov,
- b) realizovania spracúvania miezd a vedenia príslušnej evidencie v zmysle mzdových predpisov,
- c) vykonávania zrážky zo mzdy voči štátu a iným subjektom podľa príslušných zákonov,
- d) prípravy podklady pre tvorbu rozpočtu v oblasti miezd,
- e) vedenia mzdovej agendy zamestnancov prevádzkovateľa IS pre účely pracovnoprávne, mzdové a pre účely nemocenského, zdravotného a sociálneho zabezpečenia a dane z príjmov zo závislej činnosti fyzických osôb v pracovnom pomere v zmysle Zákonníka práce a vedenia agendy pre potreby ich odmeňovania a s tým súvisiace úkony.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Zákon č. 311/2001 Z. z. zákonník práce
- b) Zákon č. 90/1996 Z. z. o minimálnej mzde

- c) Zákon č. 461/2003 Z. z. o sociálnom poistení
- d) Zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca
- e) Zákon č. 600/2003 Z. z. o prídavku na dieťa a o zmene a doplnení zákona NR SR č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov
- a) Zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- b) Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov
- c) Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- a) Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení
- b) Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení
- c) Zákon č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok)
- d) Zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- e) Zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov
- f) Zákon č. 283/2002 Z. z. o cestovných náhradách
- g) Zákon č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- h) Zákon č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní v znení neskorších predpisov

4. Rozsah osobných údajov

- a) meno, priezvisko, rodné priezvisko a titul,
- b) rodné číslo,
- c) dátum a miesto narodenia,
- d) podpis,
- e) rodinný stav,
- f) štátna príslušnosť,
- g) štátne občianstvo,
- h) trvalé bydlisko, prechodné bydlisko,
- i) údaje týkajúce sa zdravia,
- j) poberanie prídavkov na deti,
- k) mzda, plat alebo platové pomery a ďalšie finančné náležitosti,
- l) údaje o odpracovanom čase,
- m) údaje o bankovom účte fyzickej osoby,
- n) sumy postihnuté výkonom rozhodnutia nariadeným súdom alebo správnym orgánom,
- o) peňažné tresty a pokuty, ako aj náhrady uložené zamestnancovi vykonateľným rozhodnutím príslušných orgánov,
- p) neprávom prijaté sumy dávok sociálneho poistenia a dôchodkov starobného dôchodkového sporenia alebo ich preddavky, štátnych sociálnych dávok, dávok v hmotnej núdzi a príspevkov k dávke v hmotnej núdzi, peňažných príspevkov na kompenzáciu sociálnych dôsledkov ťažkého zdravotného postihnutia, ktoré je zamestnanec povinný vrátiť na základe vykonateľného rozhodnutia podľa osobitného predpis,
- q) ročný úhrn vyplateného dôchodku,
- r) údaje o pracovnej neschopnosti,
- s) údaje o dôležitých osobných prekážkach v práci,
- t) údaje o zamestnávateľoch,
- u) pracovné zaradenie a deň začiatku výkonu pracovnej činnosti,
- v) údaje o manželovi alebo manželke, deťoch, rodičoch detí v rozsahu meno, priezvisko, dátum narodenia, rodné číslo, adresa,
- w) údaje z potvrdenia o zamestnaní,
- x) údaje o vedení zamestnanca v evidencii nezamestnaných občanov,
- y) údaje o čerpaní materskej dovolenky a rodičovskej dovolenky,
- z) údaje o priznaní dôchodku, o druhu dôchodku,

- aa) údaje zo zamestnaneckej zmluvy doplnkovej dôchodkovej poisťovne,
- bb) údaje o výške príspevku zamestnanca a zamestnávateľa do doplnkovej dôchodkovej poisťovne
- cc) údaje o zmenenej pracovnej schopnosti.

5. V tomto informačnom systéme sú spracúvané osobitné kategórie osobných údajov, konkrétne údaje týkajúce sa zdravia zamestnancov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené v listinnej podobe a niektoré sú vedené v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z.z. Civilný sporový poriadok v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Daňový úrad	Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov
Sociálna poisťovňa	Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zdravotné poisťovne	Zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Doplnkové dôchodkové sporiťelne	Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Dôchodkové správcovské spoločnosti	Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Ústredie práce, sociálnych vecí a rodiny	Zákon č. 5/2004 Z. z. o službách zamestnanosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Zákon č. 53/2003 Z. z. o orgánoch štátnej správy v oblasti sociálnych vecí, rodiny a služieb zamestnanosti a o zmene a doplnení niektorých zákonov
Zástupcovia zamestnancov	Zákon č. 311/2001 Z. z. Zákonník práce
Exekútor	Zákon č. 233/1995 Z. z. o súdnych exekútoroch a exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení

	niektorých zákonov v znení neskorších predpisov
Orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce)	Zákon č. 311/2001 Z. z. Zákonník práce, Zákon 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých v znení neskorších predpisov, Zákon č. 355/2007 Z. z.
iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme mzdová agenda pre spoločnosť spracúva externá spoločnosť ako sprostredkovateľ:, IČO: (ďalej aj ako „externá účtovná spoločnosť“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“), s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v tomto informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia z mailového konta. Uchovávanie nie je realizované prostredníctvom externej firmy. Doba uloženia dokumentácie v tomto IS je: Mzdové listy 50 rokov, Výplatné listiny 10 rokov, Rodinné prídavky a materské príspevky 5 rokov, Prehlásenia k dani zo mzdy 5 rokov, Zrážky zo mzdy 10 rokov, Podklady k mzdám 5 rokov, Evidencia dochádzky 5 rokov, Evidencia dovolení 5 rokov, Popisy pracovných činností 10 rokov, Dohody o vykonaní práce 10 rokov, Dohody o hmotnej zodpovednosti 5 rokov, Evidencia o preškolení a získaní odbornej kvalifikácie 20 rokov, Nemocenské poistenie – dávky, prihlášky, odhlášky, zmeny 20 rokov, Pracovná neschopnosť – evidencia, štatistika 5 rokov, Materská dovolenka a neplatené voľno – evidencia 5 rokov, Stravovanie zamestnancov – zabezpečenie 5 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v listinnej podobe je umiestnená v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Mzdovú agendu pre spoločnosť spracúva v pozícii sprostredkovateľov externá účtovná spoločnosť a externá osoba, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá

deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

V. Názov informačného systému: Personálna agenda

1. Kategórie dotknutých osôb:

- a) zamestnanci
- b) uchádzači o zamestnanie
- c) manželia alebo manželky zamestnancov
- d) vyživované deti zamestnancov
- e) blízke osoby zamestnancov
- f) bývalí zamestnanci

2. Účel spracúvania osobných údajov

Plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom alebo obdobným vzťahom (napríklad na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane agendy pracovnej zdravotnej služby, agendy zvyšovania kvalifikácie zamestnancov a predzmluvných vzťahov. V rámci predmetného informačného systému dochádza k plneniu hlavného účelu aj prostredníctvom:

- a) vedenia osobnej agendy zamestnancov v pracovnoprávnom pomere alebo inom obdobnom právnom vzťahu,
- b) spracúvania agendy prijímania zamestnancov do pracovného pomeru a skončenia pracovného pomeru,
- c) spracúvania potrebných štatistických výkazov,
- d) komplexné zabezpečenie primárnej starostlivosti o zdravie zamestnancov na pracovisku v zmysle platnej legislatívy z dôvodu prevencie chorôb z povolania, pracovných úrazov a udržanie pracovnej a funkčnej spôsobilosti zamestnancov v priebehu ich zamestnania (práceschopnosti).

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov,
- b) Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov,
- c) Zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- d) Zákon NR SR č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov,
- e) Zákon NR SR č. 600/2003 Z. z. o prídavku na dieťa a o zmene a doplnení zákona NR SR č. 461/2003 Z. z. sociálnom poistení v znení neskorších predpisov,
- f) Zákon č. 462/2003 Z. z. o náhrade príjmu pri dočasnej pracovnej neschopnosti zamestnanca a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- g) Zákon č. 580/2004 Z. z. o zdravotnom poistení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- h) Zákon č. 650/2004 Z. z. o doplnkovom dôchodkovom sporení v znení neskorších predpisov,
- i) Zákon č. 448/2008 Z. z. o sociálnych službách v znení neskorších predpisov,
- j) Zákon č. 5/2004 Z. z. o službách zamestnanosti v znení neskorších predpisov,

- k) zákon č. 82/2005 Z. z. nelegálnej práci a nelegálnom zamestnávaní v znení neskorších predpisov,
- l) Zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona NR SR č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov,
- m) Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení,
- n) Zákon č. 355/2007 Z. z. ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- o) Zákon č. 283/2002 Z. z. o cestovných náhradách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- p) Zákon č. 233/1995 Z. z. o súdnych exekútoroch a o exekučnej činnosti (Exekučný poriadok) a o zmene a doplnení ďalších zákonov,
- q) Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- r) Vyhláška Ministerstva zdravotníctva Slovenskej republiky č. 448/2007 Z. z. podrobnostiach o faktoroch práce a pracovného prostredia vo vzťahu ku kategorizácii prác z hľadiska zdravotných rizík a o náležitostiach návrhu na zaradenie prác do kategórií.

4. Rozsah osobných údajov

- a) meno, priezvisko, rodné priezvisko a titul,
- b) rodné číslo,
- c) dátum a miesto narodenia,
- d) podpis,
- e) rodinný stav,
- f) štátna príslušnosť,
- g) štátne občianstvo,
- h) trvalé bydlisko, prechodné bydlisko,
- i) pohlavie,
- j) údaje o vzdelaní,
- k) údaje z dokladu o bezúhonnosti,
- l) údaje o pracovnej neschopnosti,
- m) údaje o predchádzajúcom zamestnaní,
- n) údaje o dôležitých osobných prekážkach v práci,
- o) osobné údaje spracúvané na potvrdeniach, osvedčenia o absolvovaných skúškach a vzdelávacích aktivitách,
- p) údaje o členstve v odborovej organizácii a platbe členského príspevku odborovej organizácii,
- q) údaje o priznaní dôchodku,
- r) údaje uvedené v životopise,
- s) fotokópie úradných dokumentov

5. V tomto informačnom systéme sú spracúvané osobitné kategórie osobných údajov, konkrétne údaje týkajúce sa zdravia zamestnancov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené v listinnej podobe a niektoré sú vedené v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov

Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce)	Zákon č. 311/2001 Z. z. Zákonník práce, Zákon 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých v znení neskorších predpisov, Zákon č. 355/2007 Z. z.
iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme mzdová agenda pre spoločnosť spracúva externá spoločnosť ako sprostredkovateľ:, IČO: (ďalej aj ako „externá účtovná spoločnosť“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“), s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia z emailového konta. Uchovávanie nie je realizované prostredníctvom externej firmy. Doba uloženia dokumentácie v tomto IS je: Mzdové listy 50 rokov, Výplatné listiny 10 rokov, Rodinné prídavky a materské príspevky 5 rokov, Prehlásenia k dani zo mzdy 5 rokov, Zrážky zo mzdy 10 rokov, Podklady k mzdám 5 rokov, Evidencia dochádzky 5 rokov, Evidencia dovolení 5 rokov, Popisy pracovných činností 10 rokov, Dohody o vykonaní práce 10 rokov, Dohody o hmotnej zodpovednosti 5 rokov, Evidencia o preškolení a získaní odbornej kvalifikácie 20 rokov, Nemocenské poistenie – dávky, prihlášky, odhlášky, zmeny 20 rokov, Pracovná neschopnosť – evidencia, štatistika 5 rokov, Materská dovolenka a neplatené voľno – evidencia 5 rokov, Stravovanie zamestnancov – zabezpečenie 5 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v listinnej podobe je umiestnená v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Personálnu agendu pre spoločnosť spracúva v pozícii sprostredkovateľov externá účtovná spoločnosť a externá osoba, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá

deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1. K informačnému systému majú prístup poverení členovia spoločnosti v čase vypracovania v celkovom počte 4.

VI. Názov informačného systému: Agenda bezpečnosti a ochrany zdravia pri práci

1. Kategórie dotknutých osôb:

- a) zamestnanci
- b) bývalí zamestnanci

2. Účel spracúvania osobných údajov

Plnenie povinností zamestnávateľa súvisiacich s pracovným pomerom alebo obdobným vzťahom (napríklad na základe dohôd o prácach vykonávaných mimo pracovného pomeru) vrátane agendy bezpečnosti a ochrany zdravia pri práci. V rámci predmetného informačného systému dochádza k plneniu hlavného účelu aj prostredníctvom komplexného zabezpečenia BOZP, pracovnej zdravotnej služby a s tým súvisiace úkony ako vedenie evidencie a registrácie pracovných úrazov, ako aj evidencia z vykonaných kontrol dodržiavania predpisov BOZP, predpisov týkajúcich sa ochrany, podpory a rozvoja verejného zdravia, školení zamestnancov a podobne.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z.z. o ochrane osobných údajov).

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z.z. o ochrane osobných údajov), najmä:

- a) Zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- b) Vyhláška č. 500/2006 Z.z. MPSVaR, ktorou sa ustanovuje vzor Záznamu o registrovanom pracovnom úraze,
- c) Zákon č. 314/2001 Z.z. o ochrane pred požiarimi v znení neskorších predpisov a jeho vykonávacie predpisy.
- d) Zákon č. 355/2007 Z.z o ochrane, podpore a rozvoji verejného zdravia a o zmene a doplnení niektorých zákonov
- e) Vyhláška č. 208/2014 Z.z. Ministerstva zdravotníctva SR o podrobnostiach o rozsahu a náplni výkonu pracovnej zdravotnej služby, o zložení tímu odborníkov, ktorí ju vykonávajú, a o požiadavkách na ich odbornú spôsobilosť

4. Rozsah osobných údajov

- a) meno, priezvisko, rodné priezvisko a titul,
- b) dátum narodenia,
- c) pracovné zaradenie,
- d) podpis.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov.

6. Spôsob spracúvania osobných údajov

Osobné údaje tohto informačného systému sa nachádzajú v spoločnosti a sú v listinnej podobe. Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ nepoužíva žiadne softvér.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z.z. Civilný sporový poriadok v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z.z. o ochrane osobných údajov
Orgány štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce)	Zákon č. 311/2001 Z. z. Zákonník práce, Zákon 125/2006 Z. z. o inšpekcii práce a o zmene a doplnení zákona č. 82/2005 Z. z. o nelegálnej práci a nelegálnom zamestnávaní a o zmene a doplnení niektorých v znení neskorších predpisov, Zákon č. 355/2007 Z. z.
Iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme agenda bezpečnosti a ochrany zdravia pri práci pre nás spracúva externá osoba ako sprostredkovateľ:, sídlo:, IČO: (ďalej aj ako „osoba zabezpečujúca BOZP“), pracovnú zdravotnú službu sprostredkovateľ:, sídlo:, IČO: (ďalej aj ako „osoba zabezpečujúca PZS“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“), s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme agenda bezpečnosti a ochrany zdravia pri práci nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z.z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná prostredníctvom skartácie. Uchovávanie nie je realizované prostredníctvom externej firmy. Doba uloženia dokumentácie v tomto IS je 5 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v listinnej podobe je umiestnená v uzamykateľnej skrini.

Agendu bezpečnosti a ochrany zdravia pri práci pre spoločnosť spracúvajú v pozícii sprostredkovateľov osoba zabezpečujúca BOZP, osoba zabezpečujúca PZS a externá osoba, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorí deklarovali dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je 0. K informačnému systému majú prístup poverení členovia spoločnosti v čase vypracovania dokumentácie v celkovom počte 4.

VII. Názov informačného systému: Evidencia prijatej a odoslanej pošty

1. Kategórie dotknutých osôb:

Fyzické osoby – odosielatelia a prijímatelia korešpondencie

2. Účel spracúvania osobných údajov

Evidencia prijatej a odoslanej pošty

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov

4. Rozsah osobných údajov

- a) titul, meno, priezvisko,
b) adresa,
c) predmet a obsah pošty,
d) e-mailová adresa.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené ručne v papierovej podobe. Osobné údaje v tomto informačnom systéme sú spracúvané aj automatizovane (výpočtová technika). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač prostredníctvom ktorého sa prihlasuje do emailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme evidencia prijatej a odoslanej pošty sú spracúvané prostredníctvom sprostredkovateľov externej spoločnosti: FARMÍ – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externou osobou: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“), s ktorými má spoločnosť podpísanú zmluvu

o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v tomto informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzický zlikvidovaná skartáciou. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto IS je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v papierovej podobe je umiestnená v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 2 mesačne. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

VIII. Názov informačného systému: Hlasovanie členov spoločnosti

1. Kategórie dotknutých osôb:

a) Registrovaní členovia spoločnosti

2. Účel spracúvania osobných údajov

Hlasovanie členov spoločnosti s využitím komunikačných prostriedkov na účely zabezpečenia volieb do orgánov spoločnosti, prijímanie rozhodnutí orgánov spoločnosti a informovanie členov spoločnosti o výsledkoch hlasovania.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

4. Rozsah osobných údajov

- g) meno, priezvisko a titul,
- h) registračné číslo v Slovenskej lekárskej komore,
- i) adresa,
- j) e-mailová adresa,
- k) podpis.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené v listinnej podobe a niektoré sú vedené v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z.z. Civilný sporový poriadok v znení neskorších predpisov, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme hlasovanie členov spoločnosti pre spoločnosť spracúva externá spoločnosť: FARMÍ – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v tomto informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia údajov z mailového konta. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto IS je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Agendu evidencie členov pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných

údajov a ktorá deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1500. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 5.

IX. Názov informačného systému: Účtovné doklady

1. Kategórie dotknutých osôb:

- a) zamestnanci dodávateľov tovaru a služieb
- b) účastníci podujatia – fyzické osoby

2. Účel spracúvania osobných údajov

Spracovanie a evidencia účtovných dokladov.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov
- b) Zákon č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov
- c) Zákon č. 595/2003 Z. z. o daní z príjmov
- d) Zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov
- e) Zákon č. 152/1994 Z. z. o sociálnom fonde a o zmene a doplnení zákona č. 286/1992 Zb. o daniach z príjmov v znení neskorších predpisov

4. Rozsah osobných údajov

- a) titul, meno a priezvisko,
- b) adresa trvalého pobytu,
- c) telefónne číslo,
- d) e-mailová adresa,
- e) dátum narodenia,
- f) podpis,
- g) číslo bankového účtu fyzickej osoby v tvare IBAN,
- h) DIČ,
- i) IČO.

5. **V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.**

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané v listinnej podobe a niektoré údaje sú spracúvané automatizovane v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Sociálna poisťovňa	Zákon č. 461/2003 Z. z. o sociálnom poistení v znení neskorších predpisov, Zákon č. 43/2004 Z. z. o starobnom dôchodkovom sporení a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Zdravotné poisťovne	Zákon č. 580/2004 Z. z. o zdravotnom poistení o zmene a doplnení zákona č. 95/2002 Z. z. o poisťovníctve a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
Daňový úrad	Zákon č. 595/2003 Z. z. o dani z príjmov v znení neskorších predpisov
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme účtovné doklady pre spoločnosť spracúva externá spoločnosť ako sprostredkovateľ:,
IČO: (ďalej aj ako „externá účtovná spoločnosť“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“), s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v tomto informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzický zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia z programového softvéru a odstránenia zo všetkých dostupných pamäťových médií, vrátane externého zariadenia, na ktorom je zabezpečené zálohovanie. Uchovávanie nie je realizované prostredníctvom externej firmy. Doba uloženia dokumentácie v papierovej podobe a dokumentácie v elektronickej podobe, ktoré sú spracúvané v tomto informačnom systéme je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Dokumentácia v listinnej podobe je umiestnená v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Účtovné doklady pre spoločnosť spracúva v pozícii sprostredkovateľov externá účtovná spoločnosť a externá osoba, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 0. K informačnému systému majú prístup poverení členovia spoločnosti v čase vypracovania v celkovom počte 4.

X. Názov informačného systému: Sústavné vzdelávanie zdravotníckych pracovníkov

1. Kategórie dotknutých osôb:

- a) účastníci sústavného vzdelávania – zdravotnícki pracovníci, poskytovatelia zdravotnej starostlivosti

2. Účel spracúvania osobných údajov

Evidencia účasti na akreditovaných odborných podujatiach a spracovanie pridelených kreditov do elektronického kreditného systému.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov

4. Rozsah osobných údajov

- a) meno, priezvisko, titul,
b) dátum narodenia,
c) členstvo v príslušnej komore,
d) registračné číslo v komore,
e) forma účasti (aktívna/pasívna),
f) počet získaných kreditov,
g) údaje o pracovisku,
h) podpis.

- 5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.**

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané v listinnej podobe a niektoré údaje spracúvané automatizovane v elektronickej podobe (výpočtová technika – počítač).

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Akreditačná rada Slovenska pre sústavné medicínske vzdelávanie	Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme sústavné vzdelávanie zdravotníckych pracovníkov pre spoločnosť spracúva externá spoločnosť: FARMI – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná prostredníctvom výmazu zo všetkých pamäťových médií. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto informačnom systéme je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme sústavné vzdelávanie zdravotníckych pracovníkov pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1500. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

XI. Názov informačného systému: Usporiadávanie podujatí

1. Kategórie dotknutých osôb:

- a) Členovia spoločnosti
- b) účastníci podujatia, ktorí nie sú členmi spoločnosti

2. Účel spracúvania osobných údajov

Usporiadávanie odborných podujatí, ktoré súvisia so sústavným vzdelávaním zdravotníckych pracovníkov a usporiadávanie odborných podujatí, ktoré nesúvisia so sústavným vzdelávaním zdravotníckych pracovníkov.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

4. Rozsah osobných údajov

Rozsah osobných údajov v prípade usporiadávania odborných podujatí:

- a) titul, meno a priezvisko,
- b) dátum narodenia,
- c) registračné číslo SLK,
- d) názov a adresa pracoviska,
- e) telefónne číslo,
- f) emailová adresa.

Rozsah osobných údajov v prípade usporiadávania iných ako odborných podujatí:

- a) titul, meno a priezvisko,
- b) adresa,
- c) telefónne číslo,
- d) emailová adresa.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané ručne v papierovej podobe (prezenčné listiny). Osobné údaje v tomto informačnom systéme sú spracúvané aj automatizovane (výpočtová technika). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, Zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov

Subjekt poskytujúci peňažné/nepenažné plnenie	Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov
Iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme sústavné vzdelávanie zdravotníckych pracovníkov pre spoločnosť spracúva externá spoločnosť: FARMI – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako “externá osoba”). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná prostredníctvom odstránenia z programového softvéru a odstránenia zo všetkých dostupných pamäťových médií. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v papierovej podobe a dokumentácie v elektronickej podobe v tomto informačnom systéme je 5 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme usporadúvanie podujatí pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 1500. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

XII. Názov informačného systému: Autorské a licenčné zmluvy

1. Kategórie dotknutých osôb:

- a) Zmluvné strany – fyzické osoby (účastníci sústavného vzdelávania, účastníci odborného podujatia)

2. Účel spracúvania osobných údajov

Uzatváranie autorských a licenčných zmlúv na autorské dielo prezentované na podujatí a následné využívanie tohoto diela.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné na účely plnenia zmluvy, ktorej zmluvnou stranou je dotknutá osoba v zmysle článku 6 ods. 1 písm. b) GDPR (§ 13 ods. 1 písm. b) zákona č. 18/2018 Z. z. o ochrane osobných údajov).

4. Rozsah osobných údajov

- a) meno a priezvisko,
- b) adresa trvalého bydliska,
- c) číslo účtu v tvare IBAN,
- d) emailová adresa,
- e) telefónne číslo,
- f) názov pracoviska,
- g) adresa pracoviska,
- h) podpis.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané v papierovej podobe (licenčné zmluvy), aj automatizovane prostredníctvom výpočtovej techniky (počítač).

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Osobitný predpis podľa § 13 ods. 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme sústavné vzdelávanie zdravotníckych pracovníkov pre spoločnosť spracúva externá spoločnosť: FARMI – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v listinnej podobe, obsahujúca osobné údaje z tohto informačného systému je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z.z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v listinnej podobe v prípade autorských a licenčných zmlúv je určená dobou trvania majetkových autorských práv autora k dielu.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme autorské a licenčné zmluvy pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania 0. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

XIII. Názov informačného systému: Hlásenie poskytnutia peňažného/nepeňažného plnenia

1. Kategórie dotknutých osôb:

- a) poskytovatelia zdravotnej starostlivosti,
- b) zamestnanci poskytovateľov zdravotnej starostlivosti,
- c) zdravotnícki pracovníci,
- d) tretie osoby, prostredníctvom ktorých bolo poskytnuté peňažné alebo nepeňažné plnenie od držiteľa pre poskytovateľa zdravotnej starostlivosti.

2. Účel spracúvania osobných údajov

Hlásenie poskytnutia peňažných a nepeňažných plnení subjektu, ktorý peňažné/nepeňažné plnenie poskytol. Oznamovanie výšky nepeňažného plnenia správcovi dane. Oznamovanie o zrazení a odvedení dane vyberanej zrážkou z peňažného plnenia správcovi dane.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov
- b) Zákon č. 595/2003 o dani z príjmov

4. Rozsah osobných údajov

- 1) Hlásenie poskytnutia peňažných a nepeňažných plnení subjektu, ktorý peňažné/nepeňažné plnenie poskytol.
 - a) meno, priezvisko, titul,
 - b) zdravotnícke povolanie,
 - c) názov a adresa zdravotníckeho zariadenia, v ktorom zdravotnícky pracovník poskytuje zdravotnú starostlivosť, alebo adresu sídla poskytovateľa zdravotnej starostlivosti, ak ide o poskytovateľa zdravotnej starostlivosti,
 - d) výška a účel nepeňažného plnenia, poskytnutého priamo alebo nepriamo zdravotníckemu pracovníkovi alebo poskytovateľovi zdravotnej starostlivosti.

- 2) Oznamovanie výšky nepeňažného plnenia správcovi dane.
 - a) meno, priezvisko, titul,
 - b) dátum narodenia,
 - c) DIČ,
 - d) názov a adresa zdravotníckeho zariadenia,
 - e) výška poskytnutého nepeňažného plnenia,
 - f) dátum poskytnutia nepeňažného plnenia.

- 3) Oznámenie správcovi dane o zrazení a odvedení dane vyberanej zrážkou.
 - a) meno, priezvisko, titul,
 - b) dátum narodenia,
 - c) DIČ,
 - d) názov a adresa zdravotníckeho zariadenia,
 - e) výška poskytnutého peňažného plnenia,
 - f) dátum poskytnutia peňažného plnenia.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

Osobné údaje v tomto informačnom systéme sú spracúvané automatizovane (výpočtová technika).

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Subjekt poskytujúci peňažné/nepeňažné plnenie	Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov
Národné centrum zdravotníckych informácií	Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov, Zákon č. 153/2013 Z.z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov
Ministerstvo zdravotníctva	Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach a o zmene a doplnení niektorých zákonov

Daňový úrad	Zákon č. 595/2003 Z. z. o dani z príjmu
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme sústavné vzdelávanie zdravotníckych pracovníkov pre spoločnosť spracúva externá spoločnosť: FARMI – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako “externá osoba”). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje, v papierovej podobe je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná prostredníctvom skartácie. Dokumentácia, obsahujúca osobné údaje, v papierovej podobe je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná výmazom zo všetkých dostupných pamäťových médií prostredníctvom možnosti Shift+Del a rovnako sa uskutočňuje pravidelné formátovanie pamäťových médií. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto informačnom systéme je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme hlásenie poskytnutia peňažného / nepeňažného plnenia pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania 0. K informačnému systému majú prístup poverení členovia spoločnosti v celkovej počte 4.

XIV. Názov informačného systému: Vyhotovovanie záznamov z podujatí

1. Kategórie dotknutých osôb:

- a) účastníci podujatia.

2. Účel spracúvania osobných údajov

Vyhotovovanie kamerových a fotografických záznamov z organizovaných podujatí.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. f) GDPR (§ 13 ods. 1 písm. f) zákona č. 18/2018 Z. z. o ochrane osobných údajov):

- a) Oprávnený záujem prevádzkovateľa

4. Rozsah osobných údajov

- a) meno, priezvisko, titul
- b) podobizeň dotknutej osoby,
- c) dátum a čas pohybu.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

Osobné údaje v tomto informačnom systéme sú spracúvané automatizovane (výpočtová technika).

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme sústavne vzdelávanie zdravotníckych pracovníkov pre spoločnosť spracúva externá spoločnosť: FARMI – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzický zlikvidovaná

prostredníctvom výmazu zo všetkých pamäťových médií. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto informačnom systéme je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme vyhotovovanie záznamov z podujatí pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 500. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

XV. Názov informačného systému: Zverejňovanie záznamov z podujatí

1. Kategórie dotknutých osôb:

- a) účastníci podujatia, prezentujúci autorské dielo

2. Účel spracúvania osobných údajov

Zverejňovanie kamerových a fotografických záznamov s autorom diela z podujatí na internetových stránkach.

3. Právny základ spracúvania osobných údajov

Na zverejnenie kamerových a fotografických záznamov dotknutých osôb na internetových stránkach sa vyžaduje súhlas dotknutej osoby v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Súhlas so spracúvaním osobných údajov

4. Rozsah osobných údajov

- a) meno, priezvisko, titul
b) podobizeň dotknutej osoby,
c) dátum a čas pohybu.

- 5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.**

6. Spôsob spracúvania osobných údajov

Osobné údaje v tomto informačnom systéme sú spracúvané automatizovane (výpočtová technika).

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v tomto informačnom systéme pre spoločnosť spracúva spoločnosť FARMÍ – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Prevádzkovanie webovej stránky je zabezpečené prostredníctvom sprostredkovateľa: Websupport, s.r.o., so sídlom: Staré Grunty 12, 841 04 Bratislava, IČO: 36 421 928 (ďalej aj ako „spoločnosť zabezpečujúca webhosting“). Spravovanie stránky pre spoločnosť zabezpečuje externá osoba ako sprostredkovateľ: obchodné meno: Ing. Marek Štefunko, s miestom podnikania: Juraja Slottu 6475/39, 917 01 Trnava, IČO: 48 303 330 (ďalej aj ako „osoba zabezpečujúca správu stránky“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme sú zverejňované na webovej stránke spoločnosti a na webových stránkach externej spoločnosti.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzický zlikvidovaná prostredníctvom výmazu zo všetkých pamäťových médií. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto informačnom systéme je 10 rokov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme zverejňovanie záznamov z podujatí pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť, externá osoba, spoločnosť zabezpečujú webhosting a osoba zabezpečujúca správu stránky, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných

údajov a ktorá deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 50. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

XVI. Názov informačného systému: Marketing

1. Kategórie dotknutých osôb:

- b) Členovia spoločnosti
- c) Osoby, ktoré nie sú členmi spoločnosti

2. Účel spracúvania osobných údajov

Rozposielanie newsletterov propagujúcich činnosť spoločnosti, členom spoločnosti a osobám, ktoré nie sú členmi spoločnosti.

3. Právny základ spracúvania osobných údajov

Spracúvanie pre zasielanie newsletterov členom spoločnosti je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. f) GDPR (§ 13 ods. 1 písm. f) zákona č. 18/2018 Z. z. o ochrane osobných údajov):

- a) oprávnený záujem prevádzkovateľa

Na zasielanie newsletterov osobám, ktoré nie sú členmi spoločnosti sa vyžaduje súhlas dotknutej osoby v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- a) Súhlas so spracúvaním osobných údajov

4. Rozsah osobných údajov

- a) meno, priezvisko
- b) adresa
- c) emailová adresa

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané v papierovej podobe, aj automatizovane prostredníctvom výpočtovej techniky (počítač).

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov

Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
-----------------------	--

8. Sprostredkovatelia

Osobné údaje v tomto informačnom systéme pre spoločnosť spracúva spoločnosť FARMÍ – PROFÍ, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako „externá osoba“). Prevádzkovanie webovej stránky je zabezpečené prostredníctvom sprostredkovateľa: Websupport, s.r.o., so sídlom: Staré Grunty 12, 841 04 Bratislava, IČO: 36 421 928 (ďalej aj ako „spoločnosť zabezpečujúca webhosting“). Spravovanie stránky pre spoločnosť zabezpečuje externá osoba ako sprostredkovateľ: obchodné meno: Ing. Marek Štefunko, s miestom podnikania: Juraja Slottu 6475/39, 917 01 Trnava, IČO: 48 303 330 (ďalej aj ako „osoba zabezpečujúca správu stránky“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná prostredníctvom výmazu zo všetkých pamäťových médií. Uchovávanie nie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v tomto informačnom systéme je spravidla 10 rokov, maximálne však do okamihu vyjadrenia nesúhlasu spracúvať osobné údaje na marketingové účely.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v listinnej podobe sú zabezpečené v uzamykateľnej skrini. Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme marketing pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť, externá osoba, spoločnosť zabezpečujú webhosting a osoba zabezpečujúca správu stránky, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

12. Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je 0. K informačnému systému majú prístup poverení členovia spoločnosti v čase vypracovania v celkovom počte 4.

XVII. Názov informačného systému: Zverejňovanie údajov o členoch orgánov spoločnosti

1. Kategórie dotknutých osôb:

- a) Členovia orgánov spoločnosti

2. Účel spracúvania osobných údajov

Zverejňovanie fotografií, kontaktných údajov a životopisov členov orgánov spoločnosti na webovej stránke v súvislosti s propagáciou činností a zvýšením dôveryhodnosti spoločnosti.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. c) GDPR (§ 13 ods. 1 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov), najmä:

- b) Súhlas so spracúvaním osobných údajov

4. Rozsah osobných údajov

- a) meno, priezvisko, titul,
- b) pracovná pozícia,
- c) údaje o vzdelaní,
- d) emailová adresa,
- e) podobizeň dotknutej osoby,
- f) údaje uvedené v životopise.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje vedené v elektronickej podobe (výpočtová technika – počítač). Na spracúvanie osobných údajov v tomto informačnom systéme prevádzkovateľ používa softvér – internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v tomto informačnom systéme pre spoločnosť spracúva externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako "externá osoba"). Prevádzkovanie webovej stránky je zabezpečené prostredníctvom sprostredkovateľa: Websupport, s.r.o., so sídlom: Staré Grunty 12, 841 04 Bratislava, IČO: 36 421 928 (ďalej aj ako „spoločnosť zabezpečujúca webhosting“). Spravovanie stránky pre spoločnosť zabezpečuje externá osoba ako sprostredkovateľ: obchodné meno: Ing. Marek Štefunko, s miestom podnikania: Juraja Slottu 6475/39, 917 01 Trnava, IČO: 48 303 330 (ďalej aj ako „osoba zabezpečujúca

správu stránky“). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme sú zverejňované na webovej stránke spoločnosti.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia, obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná prostredníctvom výmazu zo všetkých pamäťových médií. Uchovávanie nie je realizované prostredníctvom externej firmy. Doba uloženia dokumentácie v tomto informačnom systéme je určená trvaním pôsobenia člena v orgáne spoločnosti.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v tomto informačnom systéme pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá osoba, spoločnosť zabezpečujú webhosting a osoba zabezpečujúca správu stránky, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je orientačne 20. K informačnému systému majú prístup poverení členovia spoločnosti v čase vypracovania v celkovom počte 4.

XVIII. Názov informačného systému: Súdne spory

1. Kategórie dotknutých osôb:

- a) členovia spoločnosti,
- b) bývalí členovia,
- c) účastníci podujatí organizovaných spoločnosťou, ktorý nie sú členmi spoločnosti.

2. Účel spracúvania osobných údajov

Preukazovanie, uplatňovanie, obhajovanie alebo bránenie právnych nárokov v prípade súdnych sporov.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 6 ods. 1 písm. f) GDPR (§ 13 ods. 1 písm. f) zákona č. 18/2018 Z. z. o ochrane osobných údajov):

- a) Oprávnený záujem poskytovateľa zdravotnej starostlivosti.

4. Rozsah osobných údajov

- a) meno, priezvisko, titul,
- b) adresa bydliska,
- c) dátum narodenia.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané v papierovej podobe aj automatizovane prostredníctvom výpočtovej techniky.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme súdne spory pre spoločnosť spracúva externá osoba ako sprostredkovateľ: obchodné meno: Mgr. Silvia Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako "externá osoba"), s ktorou má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v papierovej podobe, obsahujúca osobné údaje, je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzický zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná výmazom zo všetkých dostupných pamäťových médií, prostredníctvom možnosti Shift+Del a rovnako sa uskutočňuje pravidelné formátovanie pamäťových médií. Uchovávanie je realizované prostredníctvom sprostredkovateľa. Doba uloženia dokumentácie v papierovej podobe a dokumentácie v elektronickej podobe, ktoré sú spracúvané v tomto informačnom systéme je v prípade účastníkov podujatia obdobie, počas ktorého je možné uplatňovať právne nároky zo zmluvných vzťahov.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete

internet a sú chránené antivírusovým programom. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je 0. K informačnému systému majú prístup poverení členovia spoločnosti v čase vypracovania v celkovom počte 4.

XIX. Názov informačného systému: Uplatňovanie práv dotknutých osôb

1. Kategórie dotknutých osôb:

- a) členovia spoločnosti,
- b) účastníci podujatí organizovaných spoločnosťou, ktorí nie sú členmi spoločnosti

2. Účel spracúvania osobných údajov

Vybavovanie žiadostí v súvislosti s uplatňovaním práv dotknutých osôb.

3. Právny základ spracúvania osobných údajov

Spracúvanie je nevyhnutné podľa osobitného predpisu v zmysle článku 12 ods. 1 a nasl. GDPR (§ 29 ods. 1 a nasl. zákona č. 18/2018 Z. z. o ochrane osobných údajov).

4. Rozsah osobných údajov

- a) meno, priezvisko, titul,
- b) adresa bydliska,
- c) emailová adresa,
- d) telefónne číslo.

5. V tomto informačnom systéme nie sú spracúvané osobitné kategórie osobných údajov. V tomto informačnom systéme nie sú spracúvané biometrické údaje.

6. Spôsob spracúvania osobných údajov

V tomto informačnom systéme sú osobné údaje spracúvané v papierovej podobe aj automatizovane prostredníctvom výpočtovej techniky.

7. Okruh tretích strán

Tretie strany (prípadne okruh tretích strán)	Právny základ
Súd, orgány činné v trestnom konaní	Zákon č. 160/2015 Z. z. Civilný sporový poriadok, zákon č. 301/2005 Z. z. Trestný poriadok v znení neskorších predpisov
Inšpektori Úradu na ochranu osobných údajov SR	Zákon č. 18/2018 Z. z. o ochrane osobných údajov
Iný oprávnený subjekt	Všeobecne záväzný právny predpis v zmysle § 10 ods. 2 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

8. Sprostredkovatelia

Osobné údaje v informačnom systéme uplatňovanie práv dotknutých osôb pre spoločnosť spracúva externá spoločnosť: FARMÍ – PROFI, spol. s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887 (ďalej aj ako „externá spoločnosť“) a externá osoba, obchodné meno: Mgr. Silvia

Érseková, s miestom podnikania: Bešeňov 585, 941 41 Bešeňov, IČO: 50 642 413 (ďalej aj ako "externá osoba"). Spoločnosť má so sprostredkovateľmi podpísanú zmluvu o spracúvaní osobných údajov. Spoločnosť nespracúva v tomto informačnom systéme osobné údaje pre iného prevádzkovateľa.

9. Prenos osobných údajov do zahraničia a zverejňovanie

Osobné údaje nie sú poskytované subjektom v zahraničí. Osobné údaje v informačnom systéme nie sú zverejňované.

10. Uchovávanie a likvidácia osobných údajov

Dokumentácia v papierovej podobe, obsahujúca osobné údaje, je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov fyzicky zlikvidovaná skartáciou. Dokumentácia v elektronickej podobe obsahujúca osobné údaje je po uplynutí doby uloženia alebo ak sa na nich neviaže zákon č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov zlikvidovaná výmazom zo všetkých dostupných pamäťových médií a rovnako sa uskutočňuje pravidelné formátovanie pamäťových médií. Uchovávanie je realizované prostredníctvom externej spoločnosti. Doba uloženia dokumentácie v papierovej podobe a dokumentácie v elektronickej podobe, ktoré sú spracúvané v tomto informačnom systéme je 3 roky odo dňa prijatia žiadosti.

11. Zabezpečenie osobných údajov

Prístup k osobným údajom v tomto informačnom systéme je zabezpečený uzamykateľnou miestnosťou bez možnosti prístupu iných osôb ako poverených členov spoločnosti. Priestory spoločnosti sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly. Bližšia špecifikácia zabezpečenia sa nachádza v článku XX. časti A tejto dokumentácie.

Osobné údaje v elektronickej podobe sú spracúvané prostredníctvom počítačov, priamy vstup je zabezpečený heslom, ktorým disponujú poverení členovia spoločnosti. Počítače sú pripojené do siete internet a sú chránené antivírusovým programom. Spracovanie údajov prebieha prostredníctvom softvéru internetový prehliadač, prostredníctvom ktorého sa prihlasuje do mailového konta, zabezpečeného heslom, ktorým disponujú poverení členovia spoločnosti. K počítačom, na ktorých sa nachádza informačný systém majú prístup poverení členovia spoločnosti.

Osobné údaje v informačnom systéme uplatňovanie práv dotknutých osôb pre spoločnosť spracúvajú v pozícii sprostredkovateľov externá spoločnosť a externá osoba ako sprostredkovatelia, s ktorými má spoločnosť podpísanú zmluvu o spracúvaní osobných údajov a ktorá deklarovala dodržiavanie 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.

- 12.** Spoločnosť nemá určenú zodpovednú osobu. Za vedenie tohto informačného systému zodpovedá MUDr. Peter Makara, MPH, prezident spoločnosti. Počet dotknutých osôb v tomto informačnom systéme v čase vypracovania je 0. K informačnému systému majú prístup poverení členovia spoločnosti v celkovom počte 4.

XX. Vymedzenie okolia informačného systému

- 1.** Priestory spoločnosti sú mechanicky zabezpečené uzamykateľnými dverami. Kľúčmi od priestorov spoločnosti disponujú poverení zamestnanci spoločnosti FARMI – PROFI, spol s r.o., so sídlom: Pestovateľská 2, 821 04 Bratislava – mestská časť Ružinov, IČO: 36 656 887. Priestory sú zabezpečené protipožiarnymi prostriedkami: hasiaci prístroj a vykonávajú sa pravidelné bezpečnostné kontroly.

XXI. Záverečné ustanovenia

- 1.** Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
- 2.** Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.

3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť B KVALITATÍVNA ANALÝZA RIZÍK BEZPEČNOSTI INFORMAČNÝCH SYSTÉMOV

I. Úvod

1. Analýza bezpečnosti informačného systému predstavuje posúdenie pravdepodobnosti, či spracovateľské operácie povedú k vysokému riziku pre práva a slobody fyzických osôb.
2. Kvantitatívnu analýzu rizík bezpečnosti informačných systémov spoločnosť nepovažuje za podrobný rozbor stavu bezpečnosti v podobe posúdenia rizík na ochranu údajov podľa Článku 35 GDPR.
3. Dôvodom vykonania analýzy bezpečnosti informačných systémov, ktoré obsahujú osobné údaje fyzických osôb, je včasné zistenie bezpečnostných rizík a eliminovanie ich výskytu. Súčasne výsledkom analýzy rizík je záver, či spracovateľské operácie povedú k vysokému riziku pre práva a slobody fyzických osôb.
4. V prípade, že sa výsledkom zistí, že je pravdepodobné, že spracovateľské operácie povedú k vysokému riziku pre práva a slobody fyzických osôb, spoločnosť je zodpovedná za vykonanie posúdenia vplyvu na ochranu údajov s cieľom zhodnotiť najmä pôvod, povahu, osobitosť a závažnosť tohto rizika.
5. Analýza rizík je spracovaná na základe dotazníkov vyplnených spoločnosťou a rozhovorov so zodpovednými zamestnancami spoločnosti.

II. Metodika analýzy rizík

1. Kvalitatívna analýza rizík vyhodnocuje riziko ako kombináciu pravdepodobnosti realizovania hrozby a dopadov na aktíva, ktoré môžu vyplývať zo zlyhania bezpečnosti, pričom môžu viesť k strate dôvernosti, integrity alebo dostupnosti.

Vyhodnotenie rizík pozostáva z nasledujúcich činností:

- identifikácia aktív ich vlastníkov;
 - identifikácia hrozieb pre tieto aktíva;
 - identifikácia zraniteľností zneužitelných hrozbami;
 - identifikácia dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti;
 - analýza a ohodnotenie rizík založených na určení dopadov, ktoré môžu vyplývať zo zlyhania bezpečnosti;
 - určenie reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhadom úrovne rizík vymedzujúcich, či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika;
 - identifikácia a ohodnotenie možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým a objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany;
2. Metodika analýzy rizík je založená vychádza z technickej normy STN ISO/IEC 27002 a technickej normy STN ISO/IEC 27005. Ohodnotenie bezpečnostných rizík je realizované kvalitatívnou metódou, ktoré je založené na subjektívnom hodnotení konkrétnym hodnotiteľom.
 3. Ohodnotenie dopadu je založené na hodnotení pravdepodobnosti jeho realizácie a ohodnotení dopadu, ktorý môže táto realizácia spôsobiť, pričom hodnotiteľ subjektívne ohodnotí scenár s najhoršími možnými následkami.

III. Identifikácia a ohodnotenie informačných aktív

1. Informačnými aktívami sú identifikované informačné systémy spracúvajúce osobné údaje. Každý informačný systém (aktívum) reprezentujú jeho časti, ktoré zahŕňajú služby príslušných externých dodávateľov, IT infraštruktúru (hardvér, softvér, komunikačné linky), budovu (miestnosti) a obslužný

personál. Tieto časti aktíva sa berú do úvahy pri hodnotení aktíva a identifikácii hrozieb a zraniteľností pôsobiacich na aktívum.

- Ohodnotenie aktív je vykonané pre každý z atribútov informačnej bezpečnosti – dôvernosť, dostupnosť a integrita na stupnici Nízka – Stredná – Vysoká podľa nižšie uvedenej tabuľky a vyjadruje požadovanú úroveň zaistenia daného atribútu.

Úroveň ohodnotenia aktíva	Charakteristika úrovne
Vysoká	Poškodením, zničením alebo stratou atribútu (ďalej len narušením aktíva) dôjde, alebo môže dôjsť k úplnému prerušeniu jedného alebo viacerých kľúčových procesov, k ohrozeniu zdravia alebo života; vzniknutá škoda môže byť veľmi vysoká, neohrozí však samotnú existenciu spoločnosti.
Stredná	Narušením aktíva môže dôjsť k čiastočnému narušeniu jedného kľúčového procesu, k prerušeniu jedného alebo viacerých menej významných procesov spoločnosti; vzniknutá škoda bude mať pravdepodobne vplyv na aktuálny rozpočet spoločnosti.
Nízka	Narušením aktíva môže dôjsť k narušeniu jedného alebo viacerých menej významných procesov spoločnosti; vzniknutá škoda nemá vplyv na aktuálny rozpočet spoločnosti.

IV. Identifikácia a ohodnotenie hrozieb

- Ohodnotenie pravdepodobnosti realizácie hrozieb je vykonané na stupnici Nízka – Stredná – Vysoká podľa nižšie uvedenej tabuľky.

Úroveň ohodnotenia hrozby	Charakteristika úrovne
Vysoká	Očakáva sa výskyt hrozby, v minulosti boli incidenty alebo štatistiky alebo ďalšie informácie, ktoré indikujú, že takáto hrozba sa pravdepodobne vyskytne, alebo existujú vážne dôvody alebo motivácie pre útočníka vykonať takúto hrozbu
Stredná	Hrozba sa možno vyskytne, v minulosti boli incidenty alebo štatistiky alebo ďalšie informácie, ktoré indikujú, že takáto alebo podobné hrozby sa vyskytli niekedy v minulosti, alebo existuje indikácia, že by mohli existovať pre útočníka nejaké dôvody vykonať takúto hrozbu
Nízka	Je nepravdepodobné, že sa hrozba objaví, nevyskytli sa incidenty, štatistiky, motívy, atď., ktoré by indikovali, že hrozba nastane

V. Identifikácia a ohodnotenie zraniteľnosti

- Ohodnotenie závažnosti zraniteľností je vykonané na stupnici Nízka – Stredná – Vysoká podľa nižšie uvedenej tabuľky.

Úroveň ohodnotenia zraniteľnosti	Charakteristika úrovne
Vysoká	Je jednoduché využiť zraniteľnosť, sú implementované slabé alebo žiadne ochranné opatrenia

Úroveň ohodnotenia zraniteľnosti	Charakteristika úrovne
Stredná	Zraniteľnosť by mohla byť využitá, sú implementované nejaké bezpečnostné opatrenia
Nízka	Nie je jednoduché využiť zraniteľnosť, sú implementované dobré bezpečnostné opatrenia

VI. Stanovenie rizika

1. Výška rizika je vyjadrená indexom rizika na stupnici od 1 – 10, pričom tento index je vyjadrený ako funkcia bezpečnostných faktorov dopadu a pravdepodobnosti. Bezpečnostné riziko je ohodnotený v súlade s obrázkom nižšie:

5	5	7	8	9	10	<table border="1"> <tr><td>Nízke riziko</td></tr> <tr><td>Stredné riziko</td></tr> <tr><td>Vysoké riziko</td></tr> </table>	Nízke riziko	Stredné riziko	Vysoké riziko
Nízke riziko									
Stredné riziko									
Vysoké riziko									
4	4	6	7	8	9				
3	3	5	6	7	8				
2	2	4	5	6	7				
1	1	2	3	4	5				
	1	2	3	4	5				

2. Výška rizika je hodnotená na stupnici od 1 po 7, čomu zodpovedajú nasledovné slovné kategórie rizík:
 - Vysoké – úrovne rizika 8 až 10,
 - Stredné – úrovne rizika 5 až 7,
 - Nízke – úrovne rizika 1 až 4.
3. Charakteristiky kategórií rizík z pohľadu požiadaviek na riadenie rizík sú uvedené v nasledujúcej tabuľke.

Kategórie rizika	Požiadavky na riadenie rizika
Vysoké	<p>Netolerovateľné riziko. Procesy nesmú byť spustené skôr, ako sa zníži riziko na akceptovateľnú úroveň. Ak sa riziko týka už prebiehajúcich procesov, je potrebné urýchlene podniknúť kroky na zníženie rizika. Je potrebné vytvoriť plán zvládania rizika.</p> <p>Riziká tejto kategórie majú potenciálne veľmi vážne dopady na podnikanie spoločnosti, môžu ovplyvniť spoločnosť v dlhodobej perspektíve.</p>
Stredné	<p>Väčšinou sú to významné riziká. Je potrebné vytvoriť plán zvládania rizika a implementovať opatrenia v rámci určeného časového úseku. Treba sa snažiť o zníženie rizika do kategórie Nízke. Riziká tejto kategórie majú potenciálne významné dopady na podnikanie spoločnosti, ktoré môžu ovplyvniť spoločnosť v strednodobom horizonte.</p> <p>V tejto kategórii môžu byť aj riziká, ktoré je možné akceptovať. Takéto riziká charakterizuje najmä investičná náročnosť potenciálneho opatrenia, resp. kompenzačných opatrení znižujúcich riziko. Takéto riziká taktiež charakterizuje nízka pravdepodobnosť výskytu.</p>

Kategória rizika	Požiadavky na riadenie rizika
Nízke	Menej významné riziko. Riziko je možné akceptovať, pokiaľ náklady na riadenie rizika sú neúmerne škodám, ktoré by boli spôsobené využitím zraniteľnosti hrozbou. V prípade rozhodnutia o riadení rizika sa postupuje ako v prípade rizík strednej kategórie. Riziká tejto kategórie majú len nevýznamné a krátkodobé podnikateľské dopady na spoločnosť.

VII. Analýza a vyhodnotenie rizika zlyhania bezpečnosti

- Identifikácia rizík a ich dopady na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti spojené s personálnou bezpečnosťou:

Zraniteľnosti	Zraniteľnosť by mohla byť využitá	Pravdepodobnosť výskytu	Akceptácia rizika
1. Nedostatočné bezpečnostné školenie	Chyba pri používaní - zničenie dôležitých informácií z dôvodu neznalosti bezpečnostných postupov, prípadné odcudzenie údajov z dôvodu nedostatočného uchovania dát, nedostatočných hesiel na mieste s nízkou bezpečnostnou ochranou, neuzamknutých zásuviek stola	1	Riziko akceptované
2. Chýbajúce bezpečnostné povedomie	Chyby používateľov	2	Riziko akceptované
3. Absencia monitorovacích mechanizmov	Použitie softvéru neoprávneným spôsobom	2	Riziko akceptované
4. Absencia pravidiel na správne používanie telekomunikačných médií a prenosu	Používanie telekomunikačných prostriedkov neoprávneným spôsobom	2	Riziko akceptované
5. Neodstránenie prístupových práv pri ukončení pracovného pomeru	Neoprávnený prístup	1	Riziko akceptované
6. Absencia procedúry zabezpečujúca navrátenie aktív pri ukončení pracovného pomeru	Krádež	2	Riziko akceptované
7. Nemotivovaný alebo nespokojný personál	Nesprávne použitie (zneužitie) prostriedkov spracovania informácií	2	Riziko akceptované
8. Práca externého personálu bez dozoru alebo práca personálu mimo riadnych prevádzkových hodín	Krádež	1	Riziko akceptované
9. Vstup neoprávnených osôb	Krádež - útok na dôveryhodnosť, získanie prístupových hesiel	3	Riziko akceptované
10. Nedostatočné stanovenie protipatrení pri vzniku bezpečnostného rizika	Neoprávnený prístup, krádež - má za následok opätovný únik informácií, pokiaľ sa v čo najkratšej možnej dobe nevytvorí	1	Riziko akceptované

	protiopatrenie na elimináciu tohto rizika		
11. Nedostatočná ochrana údajov pri likvidácii	Neoprávnený prístup, krádež - Veľké riziko úniku informácií pri fyzickej likvidácii, prípadne mazanie nosičov dát po splnení ich účelu	3	Riziko akceptované
12. Nedostatočné stanovenie zodpovednosti	Zneužitie práv - Spôsobuje nemožnosť disciplinárneho postihu konkrétnej osoby pri zlyhaní ľudského faktora a môže spôsobiť ďalšie zlyhanie, prípadne zneužitie oprávnenia, prípadne právomocí na vznik bezpečnostnej udalosti	2	Riziko akceptované

2. Identifikácia rizík a ich dopady na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti spojené s fyzickou a environmentálnou bezpečnosťou:

Zraniteľnosti	Zraniteľnosť by mohla byť využitá	Pravdepodobnosť výskytu	Akceptácia rizika
13. Nedostatočná alebo nepozorná kontrola fyzického prístupu do budovy, miestností a kancelárií	Úmyselné spôsobenie škody, krádež	1	Riziko akceptované
14. Absencia fyzickej ochrany budovy, dverí a okien	Krádež	1	Riziko akceptované
15. Umiestnenie v oblasti náchylnej na záplavy	Záplava	2	Riziko akceptované
16. Nechránený dátový nosič	Krádež	2	Riziko akceptované
17. Nedostatočná údržba/chybná inštalácia pamäťového média	Chyba údržby	3	Riziko akceptované
18. Absencia schémy pravidelnej obmeny zariadení (médií)	Poškodenie pamäťového média	3	Riziko akceptované
19. Citlivosť zariadení na vlhkosť, prach a znečistenie	Vzduchom sa šíriace častice/prach	3	Riziko akceptované
20. Citlivosť zariadení na zmeny teploty	Extrémne teploty	2	Riziko akceptované
21. Citlivosť zariadení na zmeny napätia	Nestabilita elektrického napätia v sieti	3	Riziko akceptované
22. Citlivosť zariadení na otrasy	Poškodenie zariadenia otrasom alebo pádom	3	Riziko akceptované

3. Identifikácia rizík a ich dopady na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti spojené s komunikáciami a riadením prevádzky:

Zraniteľnosti	Zraniteľnosť by mohla byť využitá	Pravdepodobnosť výskytu	Akceptácia rizika
23. Komplikované používateľské rozhranie	Chyba prevádzkového personálu	2	Riziko akceptované
24. Narábanie alebo znovu použitie pamäťového	Neautorizovaný prístup k informáciám	2	Riziko akceptované

Zraniteľnosti	Zraniteľnosť by mohla byť využitá	Pravdepodobnosť výskytu	Akceptácia rizika
média bez predchádzajúceho bezpečného vymazania			
25. Absencia procedúr zálohovania	Strata informácií	1	Riziko akceptované
26. Absencia aktualizácie ochranného softvéru proti škodlivému kódu	Vírusová infekcia	2	Riziko akceptované
27. Absencia oddelenia povinností	Nesprávne použitie (zneužitie) systému (náhodné alebo úmyselné)	2	Riziko akceptované
28. Nekontrolované kopírovanie	Krádež	2	Riziko akceptované
29. Nechránené pripojenie do verejných sietí	Použitie softvéru neoprávnenými používateľmi	2	Riziko akceptované

4. Identifikácia rizík a ich dopady na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti spojené s technickou, softvérovou bezpečnosťou :

Zraniteľnosti	Zraniteľnosť by mohla byť využitá	Pravdepodobnosť výskytu	Akceptácia rizika
30. Nevhodné umiestnenie zobrazovacích zariadení	Neoprávnený prístup k informáciám	2	Riziko akceptované
31. Nevhodné umiestnenie printových zariadení	Neoprávnený prístup k informáciám	1	Riziko akceptované
32. Absencia politiky čistého stola a čistej obrazovky	Strata alebo poškodenie informácie	3	Riziko akceptované
33. Absencia identifikačných a autentizačných mechanizmov ako je autentizácia používateľa	Predstieranie používateľovej identity	2	Riziko akceptované
34. Absencia ochrana počítačových zariadení	Neoprávnený prístup k informáciám	2	Riziko akceptované
35. Žiadna alebo nesprávna politika riadenia prístupu	Neoprávnený prístup k informáciám, systémom alebo softvéru	1	Riziko akceptované
36. Nevykonanie operácie odhlásenia sa pri opustení pracovnej stanice	Použitie softvéru neoprávnenými používateľmi	2	Riziko akceptované
37. Žiadne alebo nedostatočné testovanie softvéru	Použitie softvéru neoprávnenými používateľmi	1	Riziko akceptované
38. Nedostatočný manažment hesiel (ľahko uhádnuteľné heslá, ukladanie hesiel v otvorenom tvare, nedostatočná frekvencia zmien hesla)	Predstieranie používateľovej identity	2	Riziko akceptované
39. Nezablokovanie alebo nezmenenie výrobcom	Neoprávnený prístup k informáciám, systémom alebo softvéru	2	Riziko akceptované

prednastavených kont a hesiel			
40. Nekontrolované používanie systémových utilít	Obídenie systémových ochrán alebo ochrán aplikácie	2	Riziko akceptované
41. Nevhodná ochrana šifrovacích kľúčov	Zverejnenie informácií	2	Riziko akceptované
42. Neúplná politika používania kryptografie	Porušenie legislatívy alebo noriem	2	Riziko akceptované
43. Absencia ochrany vstupných a výstupných údajov	Chyba	3	Riziko akceptované
44. Absencia validácie spracovávaných údajov	Zničenie informácie	2	Riziko akceptované
45. Absencia alebo nedostatočné testovanie softvéru	Použitie softvéru neautorizovanými používateľmi	1	Riziko akceptované
46. Nedostatočne dokumentovaný softvér	Chyba prevádzkového podporného personálu	2	Riziko akceptované
47. Nejasná alebo neúplná špecifikácia pre vývojárov	Zlyhanie softvéru	3	Riziko akceptované
48. Neriadené sťahovanie a používanie softvéru	Škodlivý softvér	3	Riziko akceptované
49. Neriadené používanie shareware/freeware pre používanie vo firme	Právna zodpovednosť	1	Riziko akceptované
50. Známe slabiny v softvéri	Použitie softvéru neautorizovanými používateľmi	1	Riziko akceptované
51. Nesprávny výber testovacích údajov	Neoprávnený prístup k osobným údajom	2	Riziko akceptované

VIII. Vyhodnotenie analýzy rizík bezpečnostného systému

- Analýza rizík bola vykonaná na základe informácií získaných od oprávnených osôb prevádzkovateľa, ako aj všetkých poskytnutých podkladov spoločnosti. Výsledky analýzy rizík úzko súvisia s ich presnosťou a úplnosťou, ako aj s úrovňou poznatkov o možných hrozbách známych v čase realizácie analýzy. Vzhľadom na rýchle tempo vývoja v oblasti informačných technológií je potrebné výsledky považovať za dostatočné na obdobie maximálne 2 rokov od jej spracovania a po uplynutí tejto doby je potrebné zvážiť potrebu vykonania opakovanej analýzy rizík.
- V prípade, že finančné náklady na bezpečnostné opatrenia prevyšujú cenu možných strát, je vhodnejšie takéto riziko akceptovať. Je potrebné sa rozhodnúť medzi cenou hodnoty informácie, údajov vrátane osobných údajov a rizikom straty, ako aj s potrebnými finančnými a ľudskými zdrojmi na ich ochranu. Na základe všeobecného pravidla uvedeného v prvej vete tohto bodu, prevádzkovateľ akceptuje zvyškové riziká ochrany osobných údajov.
- Na základe vykonanej analýzy rizík prevádzkovateľ dospel k záveru, že spracovanie osobných údajov ani v jednom z informačných systémov:
 - povedie k vysokému riziku na ochranu osobných údajov (podpis)
 - nepovedie k vysokému riziku na ochranu osobných údajov(podpis)
- Osoba zodpovedná za bezpečnosť informačných systémov je povinná označiť možnosť na základe vykonanej analýzy rizík a rozhodnutie podpísať.

5. V prípade, že spracovanie osobných údajov povedie k vysokému riziku pre práva a slobody dotknutých osôb je nevyhnutné vypracovať posúdenie vplyvu na ochranu údajov podľa článku 35 GDPR pred spracúvaním osobných údajov.

IX. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť C
ŠPECIFICKY NAVRHNUTÁ A ŠTANDARDNÁ OCHRANA OSOBNÝCH ÚDAJOV

I. Technické opatrenia

1. Technické opatrenia realizované prostriedkami fyzickej povahy:

- a) Najdostupnejším opatrením na zabezpečenie informačných systémov spoločnosti je pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, gule na dverách, mreže na dverách a oknách) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarňa signalizácia).
- b) Ďalším efektívnym opatrením, ktoré sa dá vykonať je zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia).
- c) Umiestnenie informačných systémov v chránenom priestore (ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia).
- d) Bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov ako prezenčné listiny/objednávky/mzdová agenda v uzamykateľných skrinách alebo trezoroch).
- e) Je nutné zamedziť náhodnému odpozeraniu osobných údajov zo zobrazovacích jednotiek informačného systému (napr. vhodné umiestnenie zobrazovacích jednotiek).
- f) Fyzické nosiče osobných údajov (papierová dokumentácia, externý disk, USB a iné) sa nesmú vyhadzovať do koša, ale musia sa použiť zariadenia priamo určené na ničenie takýchto nosičov (napr. skartovanie zariadenia na skartovanie listín, dátových jednotiek), prípadne ich inak zlikvidovať.
- g) Ďalšími vhodnými metódami na elimináciu rizík je využívanie elektronických zabezpečovacích prostriedkov (napr. alarmy alebo elektronická požiarňa signalizácia).

2. Ochrana pred neoprávneným prístupom:

- a) Na ochranu obsahu dátových nosičov a dát premiestňovaných prostredníctvom počítačových sietí pred neoprávneným prístupom je potrebné používať šifrovacie technológie.
- b) Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.

3. Riadenie prístupu oprávnených osôb pozostáva z identifikácie, autentizácie a autorizácie oprávnených osôb v informačnom systéme, aby sme vedeli čo najrýchlejšie analyzovať narušenie bezpečnosti a odstrániť toto bezpečnostné riziko a opätovnú možnosť bezpečnostnej udalosti. Pre vstup do informačných systémov je potrebné, aby každá oprávnená osoba mala svoje vlastné identifikačné prístupové údaje. Z tohto dôvodu je potrebné:

- a) Pri výbere a používaní hesiel by používatelia mali dodržiavať vhodné bezpečnostné praktiky.
- b) Pokiaľ by mal čo i len podozrenie z toho, že jeho heslo preniklo na verejnosť, alebo sa k nemu dostala neoprávnená osoba, musí ho okamžite zmeniť, prípadne ak takúto možnosť nemá, musí o to požiadať systémového správcu.
- c) Pre každého nového užívateľa je potrebné zadať heslo, pokiaľ by v čase zadávania hesla nebol fyzicky prítomný, môže systémový správca (alebo osoba poverená) zadať bezpečné heslo a následne povedať užívateľovi, aby si ho pri prvom používaní zmenil.
- d) Vhodný môže byť zvláštny súhlas s prístupovými právami od nadriadeného používateľa.
- e) Neodporúčame používať heslo, ktoré je napr. dátum narodenia, často používanou frázou, niečo čo sa nachádza na stole, alebo niečo, čo sa spája s užívateľom.
- f) Odporúčame, aby heslo bolo tvorené reťazcom náhodných znakov vrátane malých a veľkých písmen a číslíc.
- g) Heslo by sa malo pravidelne meniť (minimálne 2x do roka).
- h) Zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému.
- i) Užívateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený správcom informačného systému.

- j) Pokiaľ užívateľ v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený, alebo prístupové práva, ktoré mu neboli pridelené, je povinný túto skutočnosť bezprostredne oznámiť správcovi informačného systému a osobe zodpovednej za dohľad nad ochranou osobných údajov.

4. **Ochrana proti škodlivému kódu** – počítače/ počítačové stanice/ iné elektronické aktíva je nevyhnutné zabezpečiť pred napadnutím neoprávnenými osobami. Je potrebné používať len legálne a prevádzkovateľom schválené softvérové programy, súčasne odporúčame inštalovať na počítače/ pracovné stanice/ iné elektronické aktíva (v rámci možnosti) programy, ktoré eliminujú možnosť napadnutia stanice a spĺňajú tieto bezpečnostné ochrany:

- a) Antivírusová ochrana – centralizované systémy ochrany pred vírusovými napadnutiami, je nevyhnutné, aby antivírusový program bol nainštalovaný v každom počítači/ pracovnej stanici/ inom elektronickom aktíve.
- b) Firewall – kombinácia softvérových a hardvérových nástrojov na zabezpečenie LAN pred útokmi z internetu,
- c) Personal firewall – softvérové nástroje na zabezpečenie pracovných staníc s vymedzením prístupových správ,
- d) Sniffer technológia – detailné sledovanie a vyhodnocovanie dátovej komunikácie,
- e) IDS a IPS – detekcia a ochrana LAN a WAN pred vnútornými a vonkajšími narušeniami bezpečnosti,
- f) Antispamová ochrana – ochrana proti nevyžiadanim spam-om, ktoré sa voľne šíria internetom,
- g) Antispamová ochrana – ochrana pred nevyžiadanou elektronickou poštou,
- h) Backdoor ochrana – backdoor – program, ktorý umožňuje tretím osobám vstup do počítača a jeho použitie na rôzne ciele (napr. internetové útoky, rozposielanie nevyžiadanej pošty – spam). Infikovaným počítačom sa zvykne hovoriť aj zombie,
- i) Ochrana proti trojským koňom – trójsky kôň je program, ktorý sa vydáva za užitočný, ale v skutočnosti má vlastnosti backdoor programu,
- j) Ochrana proti keyloggerom – keylogger je program, ktorý sa infikuje do počítača a slúži na odchyťovanie a zaznamenávanie stlačených kláves, ktoré posielajú tretím stranám,
- k) Pokiaľ je požadovaný prístup z internetu do lokálnej siete – je nutné, aby bolo toto pripojenie a aj samotný prenos údajov, zabezpečený pomocou kryptovania. Pripojenie cez RD (Remote desktop) funkciou priamo vo Windowse OS sa používať nesmie. Doporučuje sa používať VPN (Virtual Private Network). V prípade prenosu pomocou SSH (Secure Shell) sa neodporúča používať pre autorizáciu vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite.

5. **Prevenca proti škodlivému kódu:**

- a) Nevyhnutná je pravidelná aktualizácia operačného systému, za účelom zaplátania a odstránenia rizikových miest, vždy, keď sú k dispozícii dostupné bezpečnostné aktualizácie.
- b) Je zakázané užívateľom na pracovných staniciach používať privilegované administrátorské práva, ktoré majú slúžiť výhradne na zmenu systémových nastavení, prípadne inštaláciu nových programov.
- c) Odporúča sa nainštalovať v rámci možností čo najviac programov z odseku 4, minimálne však antivírusový program.
- d) Antivírusový program musí byť pravidelne aktualizovaný, vždy keď sú k dispozícii nové aktualizácie.
- e) Pravidelne (minimálne 1x mesačne) sa musí celý počítač prekontrolovať týmto antivírusovým programom.
- f) Pred využitím pamäťového média v počítači (CD, DVD, diskety, USB flash diskety...) sa musí dátový nosič skontrolovať antivírusovým programom.
- g) Nikdy sa nesmie otvárať podozrivá nevyžiadaná e-mailová príloha.
- h) Nesmú sa navštevovať dubiózne stránky (môžu obsahovať spyware).
- i) Nesmie sa sťahovať a inštalovať žiadny softvér, ktorý nebol vopred schválený systémovým správcom, a to ani z povolených stránok.

- j) Pravidelne (minimálne 1x týždenne) sa musí vykonať záloha dôležitých údajov z disku pracovnej stanice, ktorá je na tento účel vytvorená a obsahuje minimálne dátum a čas zálohy, typ záložného média a počet kópií.
- k) Pravidelne (minimálne 1x týždenne) sa musí vykonať záloha údajov zo servera na dátové médium – o tomto úkone sa urobí záznam do knihy zálohovania, ktorá je na tento účel vytvorená a obsahuje minimálne dátum a čas zálohy, typ záložného média a počet kópií.

6. Sieťová bezpečnosť:

- a) Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou.
- b) Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete.
- c) Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall).
- d) Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam).
- e) Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok).

7. Zálohovanie je jedným z najdôležitejších opatrení, nakoľko je dôležité dáta chrániť pred zničením, poškodením alebo zneužitím, je potrebné venovať zabezpečeniu dát dostatočnú pozornosť. Medzi hlavné zásady zálohovania patria:

- a) záloha sa musí robiť pravidelne a systematicky a musí sa stať rutinnou súčasťou práce,
- b) treba si uvedomiť, že obnovením dát zo zálohy vždy nenávratne stratíme tu časť práce, ktorá bola vykonaná od posledného zálohovania,
- c) zálohovanie nesmie byť ani príliš časté, aby sa neznižovala efektívnosť práce,
- d) na zálohovanie je potrebné používať pravidelný interval a rovnaký systém ukladania, záloha sa musí robiť dôsledne,
- e) záložné médium musí byť dostatočne zabezpečené pred zničením, zneužitím neoprávnenými osobami,
- f) je potrebné v pravidelných intervaloch otestovať zálohovacie médiá a skontrolovať, či sú dáta na nich nahraté korektne a nevykazujú známky chybovosti,
- g) treba zálohovať všetky dôležité súbory, dodržiavať disciplínu,
- h) údaje na pamäťovom médiu musia byť fyzicky mimo počítača, v ideálnom prípade aj v inej miestnosti prípadne inej budove.

II. Personálne opatrenia

1. **Povedomie o ochrane osobných údajov a pravidlách** – povedomie o implementácii pravidiel ochrany osobných údajov musí byť zabezpečené na všetkých úrovniach personálu spoločnosti.
2. **Pridelenie zodpovednosti v oblasti ochrany osobných údajov** - musí byť jednoznačne definovaná zodpovednosť za ochranu jednotlivých aktív a za vykonávanie určitých bezpečnostných postupov.
3. **Zodpovednosť za aktíva** - pre všetky dôležité aktíva musia byť určení vlastníci a musí byť stanovená ich zodpovednosť za dodržiavanie primeraných bezpečnostných opatrení. Zodpovednosť za realizáciu jednotlivých bezpečnostných opatrení môže byť delegovaná ale vlastná zodpovednosť sa nemusí dostať vlastníčkovi aktív. O týchto aktívach si prevádzkovateľ vedie písomný zoznam, ktorý je pri akejkoľvek zmene aktualizovaný.
4. **Dodržiavanie mlčanlivosti** - každá oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku. Tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť, ani sprístupniť, mimo situácií vymedzených zákonom. Povinnosť mlčanlivosti trvá aj po ukončení ich spracovania. Povinnosť mlčanlivosti platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi.

Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní. Povinnosť mlčanlivosti trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru alebo obdobného pracovného vzťahu.

5. **Kvalifikačné predpoklady** - spracúvať osobné údaje v informačnom systéme majú len oprávnené osoby znalé práce na počítači, vyškolené pre prácu s aplikačným programom. Ostatné oprávnené osoby smú spracovávať osobné údaje len dokumentačne.
6. **Poučenie oprávnených osôb** - pred uskutočnením prvej spracovateľskej operácie osobnými údajmi, zodpovedná osoba, alebo iná prevádzkovateľom poverená osoba, poučí oprávnenú osobu o jej právach a povinnostiach pri spracúvaní osobných údajov. Poučenie obsahuje najmä **vymedzenie rozsahu jej oprávnení, povolených činností a podmienok spracúvania osobných údajov**. Prevádzkovateľ je povinný o poučení oprávnenej osoby vyhotoviť záznam, ktorý je povinný na požiadanie úradu hodnoverne preukázať. Prevádzkovateľ je povinný **opätovne** poučiť oprávnenú osobu, ak došlo k podstatnej zmene jej pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia.
7. **Personálne oddelenie, resp. zamestnanec zodpovedný za personálne záležitosti** - vedie evidenciu osôb prichádzajúcich do styku s osobnými údajmi. Každú takúto osobu je povinný poučiť v zmysle zákona a vyhotoviť o tom záznam o tom záznam.
8. **Postupy oprávnených osôb** spojené s automatizovanými prostriedkami spracúvania a súvisiacimi právami a povinnosťami v priestoroch prevádzkovateľa a mimo týchto priestorov) — používanie technických prostriedkov pre spracúvanie osobných informácií je povolené iba osobám oprávneným oboznamovať sa s osobnými informáciami. Technické prostriedky sú využívané zásadne zamestnancami, ktorí majú tieto prostriedky pridelené. Zamestnanci, ktorí majú pridelené technické prostriedky sú zodpovední za ich správny chod a musia dodržiavať všetky zásady práce s nimi.
9. **Zodpovednosť za informačný (počítačový) systém** - za IS zodpovedá prevádzkovateľ (spoločnosť), alebo ním poverená osoba (napríklad informatik). V prípade, že túto činnosť prevádzkovateľ zabezpečuje dodávateľsky, je nutné uzavrieť zmluvu s presne formovanými cieľmi a opatreniami zabezpečujúcimi naplnenie bezpečnostného projektu.
10. **Vymedzenie osobných údajov** — každá konkrétna oprávnená osoba musí mať v poučení presne špecifikované osobné údaje, ku ktorým má prístup na účel plnenia jej povinností a úloh a konkrétne určené postupy a popis povolených činností, ktoré je povinná uplatňovať pri spracúvaní osobných údajov. Každá osoba, ktorá pristupuje k osobným údajom, je uvedená v zozname osôb oprávnených sa oboznamovať s osobnými údajmi.
11. **Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi** — zakazuje sa zhromažďovanie a rozmnožovanie zhromaždených osobných údajov mimo zákonom stanovených prípadov. Zhromažďovať, zapisovať, evidovať osobné údaje mimo k tomu určených a zabezpečených médií. Poskytovať osobné údaje telefonicky, internetom (výnimka je zabezpečené spojenie), mobilnými sieťami. Poskytovať osobné údaje bez overenia oprávnenosti osoby. Zhromažďovať iné osobné údaje ako je stanovené zákonom. Odnášať nosiče s osobnými údajmi z pracoviska bez súhlasu prevádzkovateľa.
12. **Vymedzenie zodpovednosti za porušenie zákona** — osoby oprávnené spracúvať osobné údaje sú zodpovedné za komplexné, pravdivé, aktuálne údaje a vkladanie týchto údajov do IS. Sú zodpovedné za uchovávanie, ochranu a manipuláciu s nimi. Sú zodpovedné za preukázateľnosť súhlasu na spracúvanie osobného údaju, a to tak, že možno o ňom podať dôkaz. Sú zodpovedné za poriadok na pracovisku a odloženie všetkých písomností obsahujúcich osobné údaje a iných dokumentov, ktoré by mohli viesť k slobodnému prístupu k osobným údajom, do uzamykateľných odkladacích skriniek, resp. skriň. Sú zodpovedné za dodržiavanie zásad práce v LAN a PC podľa príkazu prevádzkovateľa v zmysle pravidiel používania lokálnej počítačovej siete. Sú povinné včas informovať osobu zodpovednú (poverenú) za dohľad

nad ochranou osobných údajov o pripravovanom začatí spracúvania osobných údajov a o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu týchto údajov.

13. **Osoby oprávnené, ktoré prevádzkujú informačný systém** - sú zodpovedné za riadny chod informačného systému, zodpovedajú za archiváciu údajovej základne a aplikačného programového vybavenia, sú zodpovedné za antivírovú ochranu LAN, spolu zodpovedajú s užívateľmi pracovných staníc za antivírovú ochranu a zodpovedajú za modernizáciu hmotných a nehmotných aktív.
14. **Vzdelávanie oprávnených osôb** — prevádzkovateľ zabezpečí školenia týkajúce sa ochrany osobných údajov (napr. v legislatívnej oblasti pri zmenách zákonov), prípadne v oblasti informačných technológií.
15. **Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby** — po skončení pracovného pomeru alebo obdobného pomeru je oprávnená osoba povinná odovzdať všetky pridelené aktíva. Oprávnenej osobe budú zrušené prístupové práva do informačného systému (meno, heslo). Oprávnená osoba bude opätovne poučená o následkoch porušenia zákonnej alebo zmluvnej mlčanlivosti.

III. Likvidácia osobných údajov a dátových nosičov

1. Bezodkladne po naplnení účelu spracúvania osobných údajov a uplynutí doby uchovávanania, musí dôjsť k likvidácii osobných údajov alebo ich anonymizácii (ak nakladanie s nim nepredpisuje iný zákon, napr. zákon č. 395/2002 z. z. o archívoch a registratúrach v znení neskorších predpisov).
2. Likvidácia je samostatná operácia spracúvania osobných údajov, pri ktorej dôjde k zničeniu osobných údajov tak, že nie sú čitateľné a obnoviteľné.
3. Uchovávanie po dobu dlhšiu ako je vopred vymedzená pre každý jednotlivý informačný systém v Časti A Vymedzenie a popis informačných systémov tejto smernice tejto smernice je možné len na základe povinností vyplývajúcich z osobitných predpisov.
4. Papierová dokumentácia obsahujúca osobné údaje musí byť likvidovaná na skartovacom zariadení a iná forma likvidácie je vylúčená. Papierová dokumentácia nesmie byť odovzdaná do zberu alebo vyhodená do koša.
5. Likvidácia údajov na elektronických nosičoch musí prebehnúť viacnásobným prepísaním a vymazaním osobných údajov na elektronickom nosiči informácií.
6. Dátové nosiče musia byť zlikvidované fyzickým zničením.

IV. Kontrolná činnosť

1. Kontrolná činnosť spoločnosti je zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému).
2. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému prevádzkovateľa identifikovaných podľa bezpečnostnej politiky prevádzkovateľa s periodicitou najmenej raz ročne.

V. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.

4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť D ZÁKLADNÉ ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV

I. Úvod

1. Zmyslom tejto časti internej smernice je rámcovo vysvetliť sedem základných zásad spracúvania osobných údajov, ktoré je potrebné pri práci s osobnými údajmi dodržiavať a najmä vysvetlenie toho, čo dodržiavanie týchto základných zásad v praxi znamená. Z týchto základných zásad vyplývajú takmer všetky ďalšie povinnosti spoločnosti a zároveň všetky práva dotknutých osôb. Nižšie vysvetlené zásady, z ktorých vyplývajú povinnosti a práva majú svoje limity a existujú z nich legitímne výnimky. Takýmto výnimkám sa venujeme v tejto internej smernici a v jej prílohách a nemožno ich vykladať ako porušenie základných zásad spracúvania.
2. GDPR vyžaduje, aby prevádzkovateľ (rozumej spoločnosť) a aj sprostredkovateľ vedeli kedykoľvek preukázať súlad spracúvania osobných údajov týmito zásadami, resp. s nariadením GDPR.

II. Zákonnosť, spravodlivosť a transparentnosť

1. Každé spracúvanie osobných údajov prevádzkovateľom a jeho zamestnancami musí byť vykonávané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe.
2. Osobné údaje možno spracúvať len zákonným spôsobom a to tak, aby nedošlo k porušeniu základných práv dotknutých osôb.
3. Zákonný spôsob spracúvania znamená, že osobné údaje nemôžete spracúvať len tak, ale musíte mať na takéto spracúvanie aspoň jeden právny základ v zmysle článku 6 GDPR (napr. dotknutá osoba vyjadrila súhlas, spracúvanie je nevyhnutné na plnenie zmluvy, spracúvanie je nevyhnutné na plnenie zákonnej povinnosti, na ochrana životne dôležitých záujmov dotknutej osoby (život, zdravie, majetok), na splnenie úlohy vo verejnom záujme alebo spracúvanie je nevyhnutné na účel oprávnených záujmov prevádzkovateľa).
4. Súhlas so spracúvaním osobných údajov je len jedným z týchto právnych základov a neslúži ako univerzálny právny základ. Je potrebné najprv zistiť, či osobné údaje nespracúvate na základe plnenia zmluvy, zákonnej povinnosti, alebo inom právnom základe. Ak sú osobné údaje spracúvané v dôsledku zákonnej povinnosti, plnenia zmluvy alebo inom právnom základe, tak nie je potrebný súhlas dotknutej osoby. Z povahy súhlasu vyplýva aj jeho odvolateľnosť, ktorá by znemožňovala dosiahnutie niektorých účelov spracúvania. V niektorých prípadoch sa prevádzkovatelia na dosiahnutie sledovaného účelu spracúvania osobných údajov spoliehajú na viacero právnych základov súčasne.
5. Zásada spravodlivého a transparentného spracúvania vyžaduje, aby dotknutá osoba mala včas, pre ňu v zrozumiteľnej forme informácie o tom:
 - a) kto o nej osobné údaje spracúva?
 - b) z akého dôvodu sú osobné údaje spracúvané?
 - c) za akým účelom?
 - d) komu sa jej osobné údaje poskytujú?
 - e) či sú prenášané do iných krajín?
 - f) ako dlho sú uchovávané?
 - g) aké má práva
 - h) a ďalšie.
6. Informácie musia byť dotknutej osobe podané v ľahko dostupnej forme, zrozumiteľne, ľahko pochopiteľne, formulované jasne a jednoducho.
7. Zásada spravodlivého a transparentného spracúvania osobných údajov neznamena, že prevádzkovateľ je povinný informovať o spracúvaní osobných údajov všetky dotknuté osoby. Poskytovanie informácií

dotknutým osobám nie je absolútna povinnosť prevádzkovateľov vo vzťahu ku všetkým dotknutým osobám vo všetkých prípadoch a situáciách, a že z týchto povinností existuje rada výnimiek.

8. V súlade so zásadou transparentnosti je realizácia informačnej povinnosti bližšie upravená v prílohe č. 1A, 1B a v prílohe č. 2 tejto dokumentácie.
9. Postup pri vybavovaní žiadosti dotknutých osôb je upravený v časti E tejto dokumentácie.

III. Obmedzenie účelu

1. Pred spracúvaním osobných údajov si prevádzkovateľ musí sám vymedziť účel spracúvania osobných údajov alebo účel prevádzkovateľovi vyplýva priamo z právneho predpisu.
2. Účel má byť vymedzený dostatočne jasne a určito, aby z neho bolo jasné, aké spracovateľské operácie na základe neho budú a nebudú prebiehať, alebo aké spracovateľské operácie dotknutá osoba môže očakávať, že s jej osobnými údajmi na základe jeho vymedzenia môžu prebiehať.
3. Spracúvať osobné údaje na iný účel, než na ktorý boli získané je zakázané, ibaže by tento iný účel úzko súvisel s pôvodným účelom spracúvania, bol s ním zlučiteľný.
4. Niektoré účely sú automaticky považované za zlučiteľné s pôvodnými účelmi. Ide o účely archivácie vo verejnom záujme, účely vedeckého alebo historického výskumu a štatistické účely upravené v článku 89 GDPR.

IV. Minimalizácia údajov

1. Spracúvanie osobných údajov má byť úzko naviazané na účel spracúvania osobných údajov, a to najmä pokiaľ ide o zoznam alebo rozsah spracúvaných osobných údajov, ktorý by mal byť nevyhnutný na to, aby sa spracúvaním daných osobných údajov mohol dosiahnuť účel.
2. Nie je správne, aby sa zoznam alebo rozsah osobných údajov, ktoré spracúvate umelo alebo dodatočne rozširoval vzhľadom na účel. Ak je účel a zoznam alebo rozsah osobných údajov stanovený zákonom, je potrebné ho rešpektovať, ak si zoznam alebo rozsah spracúvaných osobných údajov určuje prevádzkovateľ, má dbať na to, aby ho zbytočne, nad rámec účelu nerozširoval.
3. Za porušenie tejto zásady sa považuje spracúvanie osobných údajov v excesívnom rozsahu, ktoré znamená spracúvanie takých osobných údajov, ktoré nie sú potrebné na dosiahnutie účelov spracúvania. Prevádzkovateľ by preto mal vedieť preukázať, že všetky spracúvané osobné údaje potrebuje na dosiahnutie sledovaných účelov spracúvania.

V. Zásada správnosti

1. Osobné údaje spracúvané na určitý účel musia byť správne, presné a podľa potreby aktualizované tak, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne sa bezodkladne vymažú alebo opravia.
2. Ak nesprávny osobný údaj odhalí prevádzkovateľ má povinnosť ho opraviť, ak je to možné, ak nie, má povinnosť ho zlikvidovať. V prípade ak nesprávny osobný údaj zistí dotknutá osoba by mala sama iniciatívne kontaktovať prevádzkovateľa a požadovať opravu nesprávneho osobného údaju alebo jeho likvidáciu podľa tohto zákona, ak sa nesprávnosť údaju potvrdí, prevádzkovateľ má požiadavke dotknutej osoby na opravu vyhovieť.
3. Zásada aktuálnosti znamená tiež to, že prevádzkovateľ má povinnosť spracúvané osobné údaje pravidelne kontrolovať a aktualizovať (pravidelnosť kontroly je potrebné nastaviť s ohľadom na ujmu, ktorá môže vzniknúť dotknutej osobe pri spracúvaní nesprávneho osobného údaju prevádzkovateľom), a to aj po obsahovej stránke, nielen gramatickej, teda by sa nemalo stať, že osoba, ktorá uhradila svoj dlh bude v systéme prevádzkovateľa stále vedená ako dlžník napriek tomu, že reálny aj právny stav tomu už

nezodpovedá. Prevádzkovateľ nesie zodpovednosť za aktuálnosť osobného údajov v jeho informačnom systéme osobných údajov.

4. V prípade, ak dotknutá osoba sama poskytne prevádzkovateľovi nesprávne osobné údaje za ich nesprávnosť v tomto prípade nenesie zodpovednosť prevádzkovateľ, iba že by mal možnosť, prípadne zákonom stanovenú povinnosť si ich správnosť preveriť.

VI. Minimalizácia uchovávaní

1. Zásada minimalizácie uchovávaní vyžaduje, aby prevádzkovateľ uchovával osobné údaje vo forme, ktorá umožňuje identifikáciu dotknutých osôb iba dovtedy, kým to je potrebné na dosiahnutie účelu spracúvania.
2. Akonáhle je tento cieľ spracúvania osobných údajov dosiahnutý je možné, aby sa osobné údaje už spracúvali iba na účely archivácie, na účely vedeckého alebo historického výskumu či na štatistické účely podľa osobitného predpisu za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto zákonom na ochranu práv dotknutých osôb.
3. Je potrebné prijať a dodržiavať interné pravidlá stanovujúce retenčné doby (doby uchovávaní) osobných údajov na jednotlivé účely. Samotné retenčné doby stanovuje prevádzkovateľ, nakoľko iba prevádzkovateľ vie posúdiť dokedy je identifikácia dotknutých osôb potrebná na účely spracúvania osobných údajov. V niektorých prípadoch môžu retenčné doby vyplývať z osobitných predpisov. Niektoré osobitné predpisy však stanovujú len minimálnu zákonnú dobu uchovávaní (napr. uchováva najmenej 5 rokov), pričom retenčné doby môžu byť v daných prípadoch dlhšie. Zásada minimalizácie uchovávaní dovoľuje pokračovať v spracúvaní osobných údajov po uplynutí retenčných dôb na niektoré ďalšie vymedzené účely. Ide o účely archivácie vo verejnom záujme, účely vedeckého alebo historického výskumu a štatistické účely.
4. Zásada minimalizácie uchovávaní je okrem iného dotvorená aj povinnosťami týkajúcimi sa štandardne navrhutej ochrany osobných údajov v článku 25 ods. 2 GDPR.

VII. Integrita a dôvernosť

1. Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila ich primeraná bezpečnosť a dôvernosť vrátane predchádzania neoprávnenému prístupu k osobným údajom a prostriedkom spracúvania osobných údajov. Prijaté bezpečnostné opatrenia musia byť adekvátne spracúvaným osobným údajom, a to tak po technickej, personálnej, ako aj po organizačnej stránke.

VIII. Zodpovednosť

1. Podľa zásady zodpovednosti sú prevádzkovatelia zodpovední za súlad so základnými zásadami spracúvania osobných údajov podľa článku 5 ods. 1 GDPR, pričom tento súlad musia prevádzkovatelia vedieť preukázať. GDPR neupravuje spôsob preukazovania súladu so základnými zásadami spracúvania, ktorý je ponechaný na uvážení prevádzkovateľa. Táto zásada však smeruje výlučne voči úlohám a právomociam Úradu na ochranu osobných údajov a neznamená, že prevádzkovatelia by boli povinní preukazovať súlad so základnými zásadami komukoľvek inému.
2. V súlade so zásadou zodpovednosti môžu prevádzkovatelia preukázať splnenie základných zásad spracúvania osobných údajov:
 - a) zavedením primeraných politík ochrany osobných údajov podľa článku 24 ods. 2 GDPR zohľadňujúc pritom prvky štandardnej a špecifickej ochrany osobných údajov podľa článku 25 GDPR;
 - b) uzatvorením zmlúv so sprostredkovateľmi alebo spoločnými prevádzkovateľmi podľa článkov 26 alebo 28 GDPR;
 - c) vedením záznamov o spracovateľských činnostiach podľa článku 30 GDPR;
 - d) spolupracovaním s Úradom na ochranu osobných údajov pri výkone jeho úloh a právomocí podľa článku 31 GDPR;

- e) prijatím primeraných bezpečnostných opatrení podľa článku 32 GDPR;
- f) vykonaním posúdenia vplyvu a prípadnej predchádzajúcej konzultácie podľa článku 35 a 36 GDPR;
- g) vzdelávaním zamestnancov v oblasti ochrany osobných údajov;
- h) vymenovania zodpovednej osoby podľa článkov 37 až 39 GDPR;
- i) dodržiavaním pravidiel a primeraných záruk pri cezhraničných prenosoch osobných údajov do tretích krajín alebo medzinárodných organizácií;
- j) dodržiavaním schválených certifikačných mechanizmov, pečatí alebo značiek podľa článku 42 a nasl. GDPR; alebo
- k) dodržiavaním tejto internej smernice.

IX. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť E PRÁVA DOTKNUTEJ OSOBY

I. Všeobecné pravidlá pre postup pri výkone práv dotknutej osoby

1. Spoločnosť je povinná prijať vhodné opatrenia, aby informácie a oznámenia boli dotknutej osobe poskytované v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho, a to obzvlášť v prípade informácií určených dieťaťu.
2. Spoločnosť poskytne informácie dotknutej osobe písomne, prípadne aj inými prostriedkami, vrátane elektronických prostriedkov. Na žiadosť dotknutej osoby sa informácie poskytnú aj ústne, avšak len za podmienky, že sa preukázala totožnosť dotknutej osoby. Ak sa nepodarí preukázať totožnosť dotknutej osoby, informácie o spracúvaní osobných údajov nie je možné poskytnúť v ústnej forme.
3. Spoločnosť je povinná konať tak, aby dotknutej osobe uľahčila výkon jej práv uvedených v tejto časti smernice.
4. Ak spoločnosť nevie identifikovať dotknutú osobu a táto osoba poskytne dodatočné informácie za účelom jej identifikácie a uplatní niektoré z práv podľa tejto časti smernice, spoločnosť musí takejto žiadosti vyhovieť. To neplatí v tých prípadoch, kedy aj po poskytnutí dodatočných informácií spoločnosť nevie dotknutú osobu identifikovať.
5. Spoločnosť poskytne dotknutej osobe všetky informácie o opatreniach, ktoré spoločnosť prijala na základe žiadosti dotknutej osoby podľa tejto časti smernice.
6. Na základe žiadosti dotknutej osoby je spoločnosť povinná poskytnúť dotknutej osobe požadované informácie bez zbytočného odkladu, najneskôr však do jedného mesiaca od doručenia žiadosti. Táto lehota sa môže v prípade potreby predĺžiť o ďalšie dva mesiace, pričom sa zohľadní komplexnosť žiadosti a počet žiadostí. Pri predĺžení lehoty je spoločnosť povinná informovať o tom dotknutú osobu do jedného mesiaca od doručenia žiadosti, a to spolu s uvedením dôvodov pre zmeškanie pôvodnej lehoty.
7. Ak bola žiadosť dotknutej osoby podaná elektronickými prostriedkami, spoločnosť poskytne informácie dotknutej osobe taktiež elektronickými prostriedkami. Výnimkou je situácia, v ktorej dotknutá osoba sama požiada o poskytnutie informácií iným spôsobom.
8. V prípade ak spoločnosť na základe žiadosti dotknutej osoby neprijme žiadne opatrenia, je spoločnosť povinná bezodkladne, avšak najneskôr do jedného mesiaca, informovať dotknutú osobu o dôvodoch nekonania, o možnosti podať sťažnosť Úradu na ochranu osobných údajov a o možnosti uplatniť súdny prostriedok nápravy.
9. Všetky informácie a oznámenie poskytované dotknutej osobe podľa tejto časti smernice sa poskytujú bezodplatne.
10. Ak sú žiadosti dotknutej osoby zjavne neopodstatnené alebo neprimerané (napr. z dôvodu ich opakovania), v takom prípade môže spoločnosť postupovať týmito spôsobmi:
 - a) spoločnosť môže požadovať primeraný poplatok zohľadňujúci administratívne náklady na poskytnutie informácií alebo na oznámenie alebo na uskutočnenie požadovaného opatrenia, alebo
 - b) spoločnosť môže odmietnuť konať na základe žiadosti.
11. Spoločnosť odmietne poskytnutie informácií alebo vykonanie požadovaných opatrení len vo výnimočných prípadoch, a to na základe vopred udeleného súhlasu zodpovedného zamestnanca spoločnosti. Spoločnosť musí v takom prípade preukázať zjavnú neopodstatnenosť alebo neprimeranosť žiadosti dotknutej osoby. V prípade akýchkoľvek nejasností ohľadom splnenia podmienok pre odmietnutie žiadosti dotknutej osoby je potrebné túto otázku konzultovať s interným alebo externým právnym poradcom.

12. Ak má naša spoločnosť po prijatí žiadosti akékoľvek oprávnené pochybnosti o totožnosti dotknutej osoby, môže spoločnosť požiadať túto osobu o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.
13. Základné informácie o spoločnosti, o spracúvaní osobných údajov a o právach dotknutej osoby je možné poskytnúť v kombinácii so štandardizovanými ikonami, a to s cieľom poskytnúť dobre viditeľný, jasný a zrozumiteľný prehľad zamýšľaného spracúvania. Ikony použité v elektronickej podobe musia byť strojovo čitateľné. Pri používaní ikon je spoločnosť povinná postupovať v súlade s právnymi predpismi EÚ.

II. Právo na prístup k údajom

1. Na žiadosť dotknutej osoby je jej potrebné vydať potvrdenie o spracúvaní jej osobných údajov a tiež umožniť jej prístup k svojim osobným údajom.
2. Dotknutej osobe je potrebné na jej žiadosť poskytnúť aj nasledujúce informácie:
 - a) o účele spracovania osobných údajov,
 - b) o kategóriách dotknutých osobných údajov,
 - c) o príjemcoch a kategóriách príjemcov osobných údajov (osobitne je potrebné informovať o príjemcoch osobných údajov so sídlom v tretích štátoch a tiež o medzinárodných organizáciách),
 - d) o dobe uchovávaní osobných údajov (ak je to možné) alebo o kritériách na jej určenie,
 - e) o práve požadovať opravu svojich osobných údajov,
 - f) o práve požadovať vymazanie svojich osobných údajov,
 - g) o práve požadovať obmedzenie spracúvania osobných údajov,
 - h) o práve namietať proti spracúvaniu osobných údajov,
 - i) o práve podať sťažnosť dozornému orgánu,
 - j) o zdroji osobných údajov (ak sa osobné údaje nezískali od dotknutej osoby),
 - k) o automatizovanom rozhodovaní a profilovaní; v týchto prípadoch je potrebné informovať o použitom postupe, o význame a dôsledkoch takéhoto spracúvania pre dotknutú osobu.
3. Na žiadosť dotknutej osoby je potrebné poskytnúť kópiu jej osobných údajov. Primeraný poplatok za poskytnutie kópie osobných údajov je možné požadovať až pri akýchkoľvek následných kópiách, najviac však vo výške zodpovedajúcej primeraným administratívnym nákladom.
4. Ak je žiadosť dotknutej osoby podaná elektronickými prostriedkami, informácie je potrebné poskytnúť v bežne používanej elektronickej podobe (s výnimkou prípadov, ak dotknutá osoba požiada o iný spôsob).
5. Kópie podľa ods. 4. a 5. sa poskytnú len v prípade, ak to nebude mať nepriaznivé dôsledky na práva a slobody iných.

III. Právo na opravu a vymazanie

1. Na žiadosť dotknutej osoby je potrebné bezodkladne opraviť jej nesprávne osobné údaje a doplniť neúplné osobné údaje, a to aj na základe doplnkového vyhlásenia.
2. Na žiadosť dotknutej osoby je potrebné vymazať jej osobné údaje, ak je splnená niektorá z nasledujúcich podmienok:
 - a) osobné údaje už nie sú potrebné na účel, na ktorý sa spracúvali,
 - b) dotknutá osoba odvolala súhlas so spracovaním osobných údajov (za podmienky, že neexistuje iný právny základ spracovania osobných údajov),
 - c) dotknutá osoba namieta voči spracúvaniu osobných údajov a neprevažujú žiadne oprávnené dôvody na spracovanie osobných údajov,
 - d) dotknutá osoba namieta voči spracúvaniu osobných údajov na účely priameho marketingu (v tomto prípade sa neprihliada na prípadné prevažujúce oprávnené dôvody),

- e) osobné údaje boli spracúvané nezákonne,
 - f) osobné údaje musia byť vymazané, pretože to vyplýva zo všeobecne záväzného právneho predpisu,
 - g) osobné údaje sa získavali s súvislosťou s ponukou služieb informačnej spoločnosti dieťaťa.
3. Ak vznikne povinnosť vymazať osobné údaje a osobné údaje boli našou spoločnosťou zverejnené, je potrebné podniknúť primerané opatrenia (vrátane technických opatrení) na informovanie osôb spracúvajúcich takto zverejnené osobné údaje ako prevádzkovatelia, o tom, že dotknutá osoba ich žiada o vymazanie všetkých odkazov na tieto osobné údaje, ich kópie a repliky. Pri tejto informačnej povinnosti sa prihliada na dostupnú technológiu a na náklady na vykonanie uvedených opatrení.
4. Osobné údaje nie je potrebné vymazať podľa ods. 2. a nie je potrebné informovať ďalších prevádzkovateľov podľa ods. 3., ak je spracúvanie osobných údajov potrebné:
- a) na uplatnenie práva na slobodu prejavu a informácie,
 - b) na splnenie povinnosti podľa všeobecne záväzného právneho predpisu alebo na splnenie úlohy vo verejnom záujme alebo pri výkone verejnej moci,
 - c) z dôvodov verejného záujmu v oblasti verejného zdravia (*napr. na účely preventívneho alebo pracovného lekárstva, posúdenia pracovnej spôsobilosti zamestnanca, lekárskej diagnózy, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby, riadenia systémov a služieb zdravotnej alebo sociálnej starostlivosti na základe práva EÚ alebo vnútroštátneho právneho predpisu alebo podľa zmluvy so zdravotníckym pracovníkom – to všetko, ak sa osobné údaje spracúvajú odborníkom alebo v rámci jeho zodpovednosti, ktorý podlieha povinnosti zachovávať profesijné tajomstvo podľa práva EÚ alebo vnútroštátneho právneho predpisu alebo podľa pravidiel príslušných vnútroštátnych orgánov, alebo ak osobné údaje spracúva iná osoba, ktorá tiež podlieha takejto povinnosti mlčanlivosti ; taktiež ak je spracúvanie osobných údajov nevyhnutné z dôvodu ochrany proti závažným cezhraničným ohrozeniam zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti a liekov alebo zdravotníckych pomôcok, na základe práva EÚ alebo vnútroštátneho právneho predpisu, ktoré stanovujú vhodné a konkrétne opatrenia na ochranu práv a slobôd dotknutej osoby, najmä profesijného tajomstva.)*
 - d) na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely, pokiaľ je pravdepodobné, že vymazanie osobných údajov znemožní alebo závažným spôsobom sťaží dosiahnutie takéhoto spracúvania,
 - e) na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

IV. Právo na obmedzenie spracúvania

1. Dotknutá osoba môže požadovať obmedzenie spracúvania osobných údajov, ak nastane niektorý z nasledujúcich prípadov:
- a) dotknutá osoba napadne správnosť osobných údajov (počas obdobia umožňujúcom overiť správnosť osobných údajov),
 - b) spracúvanie osobných údajov je nezákonné a dotknutá osoba nesúhlasí s vymazaním osobných údajov a žiada namiesto toho o obmedzenie použitia osobných údajov,
 - c) osobné údaje už nie sú potrebné na účely spracúvania, avšak potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov,
 - d) dotknutá osoba namieta voči spracúvaniu osobných údajov (a to až do overenia, či oprávnené dôvody na strane spoločnosti prevažujú nad oprávnenými dôvodmi dotknutej osoby).
2. Ak bolo spracúvanie osobných údajov obmedzené, takéto osobné údaje je možné spracovať (s výnimkou uchovávanía) len so súhlasom dotknutej osoby alebo na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov alebo na ochranu práv inej fyzickej alebo právnickej osoby alebo z dôvodov dôležitého verejného záujmu EÚ alebo Slovenskej republiky.

3. Pred zrušením obmedzenia spracúvania osobných údajov je potrebné o tom informovať dotknutú osobu, ktorá o obmedzenie spracúvania požiadala.

V. Informačná povinnosť pri oprave, vymazaní alebo obmedzení spracúvania

1. Ak došlo k oprave, vymazaniu alebo obmedzeniu spracúvania osobných údajov, je potrebné o tom informovať každého príjemcu, ktorému boli osobné údaje poskytnuté.
2. Informačná povinnosť podľa ods. 1. sa neuplatní, ak je to nemožné alebo si to vyžaduje neprimerané úsilie.
3. Na žiadosť dotknutej osoby je potrebné jej poskytnúť informácie o príjemcoch osobných údajov.

VI. Právo na prenosnosť údajov

1. Dotknutá osoba má právo získať od spoločnosti osobné údaje, ktoré nám poskytla. Tieto svoje osobné údaje má právo získať v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte.
2. Dotknutá osoba má právo preniesť svoje osobné údaje ďalšiemu prevádzkovateľovi, a to bez toho, aby jej v tom spoločnosť bránila.
3. Právo na prenosnosť údajov má dotknutá osoba v nasledujúcich prípadoch:
 - a) ak spoločnosť spracúva osobné údaje dotknutej osoby na základe ňou udeleného súhlasu so spracovaním osobných údajov,
 - b) ak spoločnosť spracúva osobitné kategórie osobných údajov dotknutej osoby na základe ňou udeleného súhlasu so spracovaním osobných údajov,
 - c) ak spoločnosť spracúva osobné údaje dotknutej osoby na základe zmluvy uzatvorenej s dotknutou osobou (ak spracovanie osobných údajov je nevyhnutné na plnenie zmluvy),
 - d) ak spoločnosť spracúva osobné údaje dotknutej osoby z dôvodu, že sa na základe žiadosti dotknutej osoby vykonávajú opatrenia pred uzatvorením zmluvy,
 - e) ak sa spracúvanie osobných údajov dotknutej osoby vykonáva automatizovanými prostriedkami.
4. Dotknutá osoba má pri uplatňovaní svojho práva na prenosnosť údajov právo na prenos svojich osobných údajov priamo od spoločnosti inému prevádzkovateľovi, ak je to technicky možné. Takýto prenos údajov inému prevádzkovateľovi sa vykoná len na základe výslovnej a preukázateľnej žiadosti dotknutej osoby, z ktorej bude vyplývať okrem iného súhlas dotknutej osoby, aby ďalšia osoba označená ako prevádzkovateľ spracúvala jej osobné údaje.
5. Uplatnenie práva na prenosnosť údajov nemá vplyv na právo dotknutej osoby na vymazanie jej osobných údajov.
6. Prenos osobných údajov nesmie mať nepriaznivé dôsledky na práva a slobody iných.

VII. Právo namietať

1. Dotknutá osoba má právo kedykoľvek namietať z dôvodu týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov z dôvodu plnenia úloh vo verejnom záujme, pri výkone verejnej moci zverenej spoločnosti alebo z dôvodu oprávneného záujmu spoločnosti. Dotknutá osoba má tiež právo namietať proti profilovaniu založenému na uvedených dôvodoch.
2. Ak dotknutá osoba namieta spracúvanie osobných údajov, spoločnosť nesmie ďalej spracúvať jej osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie. Musí ísť o také dôvody, ktoré prevažujú nad záujmami, právami a slobodami dotknutej osoby. Rovnako môže ísť o dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

3. Ak spoločnosť spracúva osobné údaje na účely priameho marketingu, dotknutá osoba môže kedykoľvek namietať proti takémuto spracúvaniu, a to vrátane profilovania súvisiaceho s priamym marketingom. Ak dotknutá osoba namieta proti spracúvaniu na účely priameho marketingu, takéto údaje sa ďalej na tento účel spracúvať nemôžu.
4. Spoločnosť je povinná upozorniť dotknutú osobu na jej právo namietať spracúvanie osobných údajov. Musíme tak vykonať najneskôr pri našej prvej komunikácii s dotknutou osobou. Toto upozornenie musí byť jasné a musí byť oddelené od akýchkoľvek iných informácií.
5. Pri používaní prostriedkov informačnej spoločnosti môže dotknutá osoba uplatňovať svoje právo namietať automatizovanými prostriedkami s použitím technických špecifikácií.
6. Dotknutá osoba má taktiež právo namietať proti spracúvaniu osobných údajov, ak sú tieto spracúvané na účely vedeckého alebo historického výskumu, ako aj proti spracúvaniu na štatistické účely. Toto právo môže dotknutá osoba uplatniť z dôvodov jej konkrétnej situácie, s výnimkou prípadov, keď je spracúvanie nevyhnutné na plnenie úlohy z dôvodov verejného záujmu.

VIII. Automatizované rozhodovanie a profilovanie

1. Dotknutá osoba má právo od spoločnosti požadovať, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, a to vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.
2. Dotknutá osoba nemá právo uvedené vyššie v ods. 1, ak je rozhodnutie:
 - a) nevyhnutné na uzavretie alebo plnenie zmluvy medzi dotknutou osobou a našou spoločnosťou,
 - b) povolené právom EÚ alebo právom Slovenskej republiky, a ktorým sa zároveň stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby,
 - c) založené na výslovnom súhlase dotknutej osoby.
3. V prípadoch uvedených v ods. 2 písm. a) a c) musí spoločnosť vykonať vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, a to aspoň práva na ľudský zásah zo strany spoločnosti, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.
4. Rozhodnutia podľa ods. 2 sa nezakladajú na osobitných kategóriách osobných údajov, pokiaľ nejde o spracúvanie osobitných kategórií osobných údajov na základe súhlasu dotknutej osoby alebo z dôvodov významného verejného záujmu a pokiaľ nie sú zavedené vhodné opatrenia na zaručenie práv a slobôd a oprávnených záujmov dotknutej osoby.

IX. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
 MUDr. Peter Makara, MPH, prezident spoločnosti

Časť F POVINNOSTI SPOLOČNOSTI PRI PLNENÍ INFORMAČNÝCH POVINNOSTI

I. Rozsah informačnej povinnosti

1. V prípade ak sa od dotknutých osôb získavajú osobné údaje, spoločnosť je povinná poskytnúť pri získavaní nasledujúce informácie (ďalej v texte „*informačná povinnosť*“):
 - a) totožnosť a kontaktné údaje spoločnosti,
 - b) kontaktné údaje zodpovednej osoby, ak je stanovená,
 - c) účely spracovania osobných údajov a právne základy,
 - d) kategórie dotknutých osobných údajov (ak sa osobné údaje nezískali od dotknutej osoby),
 - e) oprávnené záujmy spoločnosti, ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) GDPR (*spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana*),
 - f) príjemcovia a kategórie príjemcov osobných údajov (osobitne je potrebné informovať o príjemcoch osobných údajov so sídlom v tretích štátoch a tiež o medzinárodných organizáciách),
 - g) doba uchovávanía osobných údajov (ak je to možné) alebo kritériá na jej určenie,
 - h) právo požadovať opravu svojich osobných údajov,
 - i) právo požadovať vymazanie svojich osobných údajov,
 - j) právo požadovať obmedzenie spracúvania osobných údajov,
 - k) právo namietať proti spracúvaniu osobných údajov,
 - l) právo podať sťažnosť dozornému orgánu,
 - m) právo odvolať súhlas so spracovaním osobných údajov (ak sa osobné údaje spracúvajú na právnom základe súhlasu),
 - n) z akého zdroja pochádzajú osobné údaje (ak sa osobné údaje nezískali od dotknutej osoby),
 - o) informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje a možné následky neposkytnutia údajov,
 - p) informácia o automatizovanom rozhodovaní a profilovaní; v týchto prípadoch je potrebné informovať o použitom postupe, o význame a dôsledkoch takéhoto spracúvania pre dotknutú osobu.

II. Realizácia informačnej povinnosti

1. Spoločnosť je oprávnená splniť si informačné povinnosti v rozsahu vymedzenom v predchádzajúcom bode 1. akýmkoľvek spôsobom, bez ohľadu na formu a podobu poskytnutých informácií. Tieto informácie je spoločnosť povinná poskytnúť iniciatívne, nie až na základe žiadosti alebo vyzvania dotknutej osoby.
2. Spoločnosť je povinná svoju informačnú povinnosť preukázať.
3. Za účelom ochrany spoločnosti a možnosti dodatočného preukázania splnenia tejto povinnosti vo vzťahu k účastníkom odborného podujatia je potrebné informácie v rozsahu podľa bodu 1 tejto časti umiestniť na viditeľné miesto v priestoroch spoločnosti alebo v priestoroch konania odborného podujatia, ktoré je dostupné všetkým účastníkom odborného podujatia a upozorniť ich na možnosť oboznámenia so základnými informáciami pre účastníkov odborného podujatia o spracúvaní osobných údajov. V prípade, že spoločnosť používa na svoju prezentáciu webové sídlo, odporúčame zverejnenie základných informácií pre účastníkov odborného podujatia na webovom sídle (odporúčaný postupom je zverejniť základné informácie pre účastníkov odborného podujatia zaužívaným spôsobom v spodnej lište webstránky pod označením napr. „Podmienky ochrany súkromia“, „Ochrana súkromia“ alebo „Ochrana osobných údajov“ a pod.)
4. Za účelom ochrany spoločnosti a možnosti dostatočného preukázania splnenia tejto povinnosti vo vzťahu k zamestnancom je potrebné informácie zamestnancom poskytovať v písomnej forme. Tam kde je to

možné, je potrebné zabezpečiť podpis dotknutej osoby potvrdzujúci prijatie informácie o spracúvaní osobných údajov. V prípade ak nie je možné zabezpečiť informovanie v písomnej forme alebo ak nie je možné získať písomné potvrdenie dotknutej osoby o prijatí tejto informácie, je potrebné bezodkladne informovať zodpovedného zamestnanca spoločnosti a vyžiadať si usmernenie k ďalšiemu postupu.

5. Vzorový dokument v rozsahu základných informácií vo vzťahu k účastníkom odborného podujatia sa nachádza v Prílohe č. 1A, 1B a 1C a vzorový dokument v rozsahu základných informácií vo vzťahu k zamestnancom sa nachádza v Prílohe č. 2 a slúži ako návod pre splnenie informačnej povinnosti spoločnosti podľa čl. 13 a 14 GDPR najmä vo vzťahu k dotknutým osobám – účastníkom odborného podujatia a zamestnancom.
6. Na preukázanie splnenia povinnosti informovať dotknutú osobu je rozhodujúce, či dotknutá osoba mala možnosť pri získavaní osobných údajov oboznámiť sa s týmito informáciami a nie je skutočnosť, či tak dotknutá osoba skutočne urobila, nakoľko dotknuté osoby nie sú povinné oboznamovať sa alebo čítať tieto informácie.
7. V prípade získavania osobných údajov od dotknutej osoby je potrebné, aby základne informácie v rozsahu podľa bodu 1 boli dotknutej osobe poskytnuté najneskôr pri získavaní jej osobných údajov, respektíve v dostatočnom časovom predstihu, jasne a zrozumiteľne a takým spôsobom, aby sa s týmito informáciami mohla skutočne oboznámiť a porozumela im.
8. V prípade, že spoločnosť nezíska osobné údaje o dotknutej osobe priamo od nej je povinná základné informácie poskytnúť v primeranej lehote po získaní osobných údajov od inej ako dotknutej osoby dotknutej osobe alebo je spoločnosť povinná plniť si informačnú povinnosť voči dotknutej osobe najneskôr v čase prvej komunikácie s ňou, alebo v čase, keď sa osobné údaje prvýkrát poskytnú plánujú poskytnúť ďalšiemu príjemcovi.

III. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jeho podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť G
POVINNOSTI SPOLOČNOSTI PRI UPLATŇOVANÍ PRÁV DOTKNUTÝCH OSÔB

I. Úvod

1. V tejto časti smernice je popísaný postup zodpovedného zamestnanca spoločnosti v prípade, ak si dotknutá osoba uplatní svoje právo na poskytnutie informácií, ktoré sa týkajú spracúvania jej osobných údajov.

II. Prijatie žiadosti zo strany Dotknutej osoby

1. Dotknutá osoba má právo požiadať v rámci práva na transparentnosť spracovania osobných údajov najmä informácie o:
 - a) totožnosti a kontaktných údajoch spoločnosti a v príslušných prípadoch zástupcu spoločnosti;
 - b) kontaktných údajoch prípadnej zodpovednej osoby;
 - c) účeloch spracúvania, na ktoré sú osobné údaje určené, ako aj právny základ spracúvania
 - d) kategórie dotknutých osobných údajov;
 - e) príjemcoch alebo kategóriách príjemcov osobných údajov, ak existujú;
 - f) dobe uchovávania osobných údajov, alebo ak to nie je možné, tak o kritériách na jej určenie atď.
2. V podmienkach spoločnosti, táto žiadosť môže byť postúpená na ktorúkoľvek pozíciu v akejkoľvek podobe:
 - a) e-mail,
 - b) list,
 - c) ústna požiadavka – potreba vyplnenia identifikácie a požiadavky v písomnej podobe,
 - d) telefonicky.

III. Postúpenie zodpovednému zamestnancovi na vybavenie žiadosti Dotknutej osoby

1. Zamestnanec alebo osoba pracujúca v obdobnom vzťahu pre spoločnosť po obdržaní takejto požiadavky bezodkladne, najneskôr nasledujúci pracovný deň musí zabezpečiť jej doručenie zodpovednému zamestnancovi spoločnosti (ďalej len ako „zodpovedný zamestnanec“), ktorý má na starosti vybavovanie žiadosti dotknutých osôb spolu s dátumom doručenia žiadosti.

IV. Preverenie oprávnenosti žiadosti

1. Zodpovedný zamestnanec pre zabezpečenie overenia totožnosti dotknutej osoby zistí, či je táto osoba klientom spoločnosti a či sa nachádza v informačných systémoch spoločnosti.
2. Zodpovedný zamestnanec pre zabezpečenie odpovede pre Dotknutú osobu zapíše žiadosť do registra žiadostí a priloží jej elektronickú podobu, ak je to možné, označí dátum prijatia žiadosti a osobu, ktorá obdržala daný podnet.

V. Činnosť zodpovedného zamestnanca pre zabezpečenie odpovede pre dotknutú osobu

1. Zodpovedný zamestnanec poskytne dotknutej osobe informácie, ktoré sa týkajú spracúvania jej osobných údajov v stručnej, zrozumiteľnej a ľahko dostupnej forme, ktoré sú formulované jasne.
2. Informácie poskytne v listinnej podobe alebo elektronickej podobe, spravidla v rovnakej podobe, v akej bola podaná žiadosť. Ak o to požiada dotknutá osoba, informácie môže zodpovedný zamestnanec poskytnúť aj ústne, ak dotknutá osoba preukáže svoju totožnosť iným spôsobom.
3. V prípade ak zodpovedný zamestnanec nevie identifikovať dotknutú osobu, ktorá si uplatní právo na informácie, v tom prípade je zodpovedný zamestnanec oprávnený na účely riadneho vybavenia žiadosti dotknutej osoby ju požiadať o poskytnutie dodatočných, dopĺňajúcich informácií na účely potvrdenia jej totožnosti. Teda vyzve dotknutú osobu, aby mu dodatočne poskytla identifikačné údaje. Napríklad vyzve osobu aby sa dostavila do sídla spoločnosti za účelom jej identifikácie a riadneho vybavenia jej žiadosti.

4. V prípade, ak dotknutá osoba zodpovednému zamestnancovi dodatočne poskytne osobné údaje na účely jej identifikácie, nesmie zodpovedný zamestnanec takúto jej iniciatívu odmietnuť, a to práve z dôvodu, že ide o uplatnenie si práv dotknutej osoby. Zodpovedný zamestnanec nemôže vyhovieť právu dotknutej osoby iba vtedy, ak preukáže, že dotknutú osobu napriek svojej maximálne vynaloženej snahe, nie je schopný identifikovať.
5. Zodpovedný zamestnanec poskytne informácie dotknutej osobe najneskôr do mesiaca od doručenia žiadosti.
6. V odôvodnených prípadoch môže zodpovedný zamestnanec lehotu predĺžiť, a to o dva mesiace. V takomto prípade zodpovedný zamestnanec musí takéto predĺženie lehoty oznámiť dotknutej osobe.
7. Takéto predĺženie lehoty na plnenie si tejto informačnej povinnosti by malo nastať len zo závažných dôvodov na strane spoločnosti. Napríklad s ohľadom na časovú náročnosť prijatia primeraných a účinných bezpečnostných opatrení, ktoré sú potrebné v súvislosti s uplatnením práva dotknutej osoby.
8. Pokiaľ ide o spôsob konania a informovania zo strany zodpovedného zamestnanca, ten by mal rešpektovať prostriedky, aké použila dotknutá osoba na podanie žiadosti. Teda to znamená, že ak sa dotknutá osoba obrátila na spoločnosť elektronicky, mal by jej zodpovedný zamestnanec odpovedať elektronicky, v prípade, ak si dotknutá osoba neustanovila iný spôsob, ktorý jej viac vyhovuje.
9. V prípade, že na základe žiadosti dotknutej osoby zodpovedný zamestnanec nekonal, neprijal žiadne opatrenia, informuje dotknutú osobu a taktiež musí uviesť dôvody, pre ktoré nekonal. Tiež ju informuje o tom, že môže podať návrh na začatie konania na Úrad na ochranu osobných údajov.
10. Zodpovedný zamestnanec vybaví žiadosť dotknutej osoby bezplatne. V prípade, ak sa žiadosti dotknutej osoby opakujú alebo sú neopodstatnené a dotknutá osoba ani na základe výzvy zodpovedného zamestnanca obsah žiadosti nedoplní, v takom prípade zodpovedný zamestnanec môže vybavenie takejto žiadosti spolatniť a to vo výške administratívnych nákladov, ktoré sú potrebné na jej vybavenie, prípadne zodpovedný zamestnanec môže odmietnuť na základe takejto žiadosti konať.
11. Preukázať to, že žiadosť dotknutej osoby bola neopodstatnená znáša spoločnosť.
12. V prípade ak žiadosť je veľmi všeobecná, zodpovedný zamestnanec môže požiadať dotknutú osobu o špecifikáciu svojej žiadosti s poučením, že v opačnom prípade jej žiadosti nebude vyhovené.

VI. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Tento postup nadobúda účinnosť dňom jeho podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť H HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV

I. Všeobecné pravidlá

1. Bezpečnostným incidentom sa na účely tejto smernice rozumie porušenie ochrany osobných údajov. Ide o také porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú alebo neoprávnený prístup k nim.
2. Spoločnosť má povinnosť oznamovať po splnení stanovených podmienok bezpečnostné incidenty príslušnému dozornému orgánu a dotknutej osobe.
3. Cieľom oznamovacej povinnosti je zvýšenie bezpečnosti spracúvania osobných údajov a súčasne získanie pomoci a podpory od dozorného orgánu pri zvládnutí bezpečnostného incidentu.
4. Spoločnosť má povinnosť:
 - a) včas identifikovať bezpečnostný incident,
 - b) posúdiť, či bezpečnostný incident (v širšom zmysle slova) je zároveň porušením bezpečnosti osobných údajov (t.j. či došlo porušeniu dôvernosti alebo integrity alebo dostupnosti osobných údajov),
 - c) posúdiť mieru rizika, ktorá z takého incidentu vyplýva pre dotknuté osoby (postačuje, ak je predpoklad existencie takéhoto rizika).
5. Povinnosť podľa predchádzajúceho ods. 4 tohto článku tejto časti smernice je spoločnosť povinná zdokumentovať. Vzorový formulár pre zdokumentovanie porušenia ochrany osobných údajov tvorí Prílohu č. 9 tejto smernice.

II. Hlásenie bezpečnostných incidentov dozornému orgánu

1. Dotknutým dozorným orgánom, ktorému je spoločnosť povinná hlásiť bezpečnostné incidenty je Úrad na ochranu osobných údajov.
2. Ak dôjde k porušeniu ochrany osobných údajov, spoločnosť je povinná bez zbytočného odkladu, najneskôr však do 72 hodín od kedy sa spoločnosť o bezpečnostnom incidente dozvedela, oznámiť túto skutočnosť oznámiť dozornému orgánu. Ak oznámenie nebude podané v tejto lehote, je k nemu potrebné pripojiť zdôvodnenie meškania.
3. Príslušnosť dozorného orgánu, t. j. určenie príslušnosti slovenského Úradu na ochranu osobných údajov alebo príslušnosti dozorného orgánu niektorého členského štátu EÚ je potrebné vopred konzultovať so zodpovedným zamestnancom.
4. Oznámenie bezpečnostného incidentu dozornému orgánu nie je potrebné jedine v prípade, ak nie je pravdepodobné, že tento incident povedie k riziku pre práva a slobody fyzických osôb.
5. Subjekt spracúvajúci osobné údaje v našom mene (sprostredkovateľ) je povinný oznámiť spoločnosti oznámenie o porušení ochrany osobných údajov, a to bez zbytočného odkladu, odkedy sa o porušení dozvedel.
6. Oznámenie spoločnosti pre dozorný orgán musí obsahovať najmenej nasledujúce skutočnosti:
 - a) opis povahy porušenia ochrany osobných údajov (zahŕňajúc kategórie a približný počet dotknutých osôb a kategórie a približný počet dotknutých záznamov o osobných údajoch),
 - b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,

- c) opis pravdepodobných následkov porušenia ochrany osobných údajov,
 - d) opis opatrení prijatých alebo navrhovaných našou spoločnosťou s cieľom napraviť porušenie ochrany osobných údajov, zahŕňajúc podľa potreby tiež opatrenia na zmiernenie potenciálnych nepriaznivých dôsledkov).
7. Tie informácie, ktoré nie je možné dozornému orgánu oznámiť súčasne, je možné oznámiť aj vo viacerých etapách, vždy však bez zbytočného odkladu.
 8. Spoločnosť je povinná zdokumentovať každý prípad porušenia ochrany osobných údajov, vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a opatrenia prijaté na nápravu. Táto dokumentácia musí umožniť dozorným orgánom overiť súlad nášho postupu so všeobecne záväznými právnymi predpismi (predovšetkým však s čl. 33 GDPR).

III. Hlásenie bezpečnostných incidentov dotknutej osobe

1. Ak došlo k porušeniu ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, je spoločnosť povinná bez zbytočného odkladu oznámiť porušenie ochrany osobných údajov dotknutej osobe.
2. Oznámenie dotknutej osobe musí obsahovať jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a aspoň informácie a opatrenia uvedené v čl. II. ods. 6 písm. b), c) a d) tejto časti smernice.
3. Oznámenie dotknutej osobe sa nevyžaduje, ak je splnená aspoň jedna z nasledujúcich podmienok:
 - a) spoločnosť prijala primerané technické a organizačné ochranné opatrenia a tieto opatrenia spoločnosť uplatnila na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie;
 - b) spoločnosť prijala následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb uvedené v ods. 1 tohto článku pravdepodobne už nebude mať dôsledky;
 - c) ak by oznámenie dotknutej osobe vyžadovalo neprimerané úsilie; v takom prípade dôjde namiesto toho k informovaniu verejnosti alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.
4. V čase kým spoločnosť oznámi dotknutej osobe porušenie ochrany osobných údajov, môže dozorný orgán po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak spoločnosť urobila, alebo môže rozhodnúť, že je splnená niektorá z podmienok uvedených v ods. 3 tohto článku smernice.
5. S výnimkou prípadov podľa ods. 4 tohto článku smernice je potrebné splnenie podmienok podľa ods. 3 tohto článku konzultovať so zodpovednou osobou.

IV. Odporúčané postupy pri haváriách, poruchách a iných mimoriadnych situáciách

Popis havárie	Návrh preventívnych opatrení	Postupy na zabezpečenie stavu obnovy
Havárie IS spôsobené technickou chybou niektorého komponentu centrálného počítača- serveru	<ul style="list-style-type: none"> • Monitorovať činnosť serverov, kontrolovať chybové hlásenia • Zabezpečiť dostatok finančných prostriedkov na obnovu IS • Podľa možnosti obmieňať server každé tri roky • Zálohovať 	<ul style="list-style-type: none"> • Obnova zo zálohy

<p>Porucha servera spôsobená vírusom neautorizovaným programom</p>	<ul style="list-style-type: none"> • Zabezpečiť antivírusovú ochranu • Inštalovať len autorizované programy oprávnenými zamestnancami • Preverovať cudzie nosiče (FD, CD ROM ...) • Nepripájať nepreverené PC bez vedomia admin do LAN • Nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN • Neotvárať nevyžiadané e-mailové prílohy • Nespúšťať programy z prostredia internetu nepodpísane certifikačnou autoritou • Nestáhovať neautorizované programy z prostredia internetu • Sledovať aktuálne dianie na LAN a v sieti internet 	<ul style="list-style-type: none"> • Odpojiť každého užívateľa • Spustiť antivírusový program s aktuálnou DB vírusov • detekovať spôsob narušenia • odstrániť príčiny • opraviť narušenú funkčnosť • opätovne skontrolovať systém antivírusovým programom • prekontrolovať všetky PC • nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie • znovu spustiť systém a pripojiť užívateľov
<p>3. Porucha napájania, strata dodávky elektrickej energie</p>	<ul style="list-style-type: none"> • Dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia 	<ul style="list-style-type: none"> • V čase výpadku sa musí záložný zdroj automaticky aktivovať • Pri dlhodobjšom výpadku sa server musí automaticky vypnúť (shutdown)
<p>4. Porucha prostriedkov demilitarizovanej zóny</p>	<ul style="list-style-type: none"> • Monitorovať činnosť zariadení • Monitorovať funkčnosť všetkých zariadení • Zabezpečiť prístup len pre pracovníkov s oprávnením • Periodicky meniť administrátorské a užívateľské prístupy s heslami • Zabezpečiť antivírusovú ochranu všetkých PC, ako aj e-mailového prístupu • Zabezpečiť programovú aktuálnosť • Zabezpečiť technickú aktuálnosť • Kontrolovať súbory zaznamenávajúce činnosť systému • Kontrolovať súbory 	<p>V prípade narušenia</p> <ul style="list-style-type: none"> • Odpojiť LAN od prostriedkov demilitarizovanej zóny • Vyhľadať príčinu nefunkčnosti • Odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku • Poveriť prostriedky firewallu, prekladu adres (DNS) a proxy • Po otestovaní funkčnosti pripojiť LAN
<p>5. Porucha aktívnych prvkov siete</p>	<ul style="list-style-type: none"> • Monitorovať činnosť • Zabezpečiť dostatočnú kapacitu • Pripájať ich prostredníctvom záložného zdroja • Zabezpečiť dostatočnú ochranu pred nepovolaným prístupom 	<ul style="list-style-type: none"> • Vymeniť nefunkčnú časť
<p>6. Porucha pasívnej časti siete</p>	<ul style="list-style-type: none"> • Premeranie kabeláže, zásuviek a konektorov 	<ul style="list-style-type: none"> • Opraviť prípadne vymeniť vadnú časť
<p>7. Havária databáz</p>	<ul style="list-style-type: none"> • Sledovať konfiguračné súbory • Monitorovať hlásenia programov a včas na ne reagovať • Denne kontrolovať chybové hlásenia aplikácie a databázy 	<ul style="list-style-type: none"> • Po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy
<p>8. Havária aplikácie</p>	<ul style="list-style-type: none"> • Sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov 	<ul style="list-style-type: none"> • Preinštalovať aplikáciu • Nainštalovať novšiu verziu

	<ul style="list-style-type: none"> • Sledovať konfiguračné súbory • Monitorovať hlásenia a včas na ne reagovať • Denne kontrolovať chybové hlásenia aplikácie a databázy 	<ul style="list-style-type: none"> • aplikácie • Konzultovať chyby s dodávateľom
9. Porucha mail servera	<ul style="list-style-type: none"> • Sledovať konfiguračné súbory • Monitorovať hlásenia a včas na ne reagovať • Denne kontrolovať chybové hlásenia • Nainštalovať antivírusovú ochranu • Zálohovať systém – obraz disku 	<ul style="list-style-type: none"> • Vymeniť nefunkčnú časť • Aktualizovať softvér • V prípade výmeny disku previesť inštaláciu zo zálohy
10. Porucha pracovných staníc	<ul style="list-style-type: none"> • Používať len autorizované programy • Inštalovať antivírusové 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 	<ul style="list-style-type: none"> • Technická chyba – zabezpečiť opravu nefunkčnej časti • Softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírusovú ochranu
11. Narušenie dverí, okien	<ul style="list-style-type: none"> • Pravidelne sledovať funkčnosť 	<ul style="list-style-type: none"> • Neodkladne zabezpečiť opravu • Hľadať príčinu a odstrániť
12. Narušenie monitorovaného objektu	<ul style="list-style-type: none"> • Pravidelne sledovať funkčnosť 	<ul style="list-style-type: none"> • Hľadať a eliminovať príčinu narušenia
13. Mimoriadne udalosti spôsobené vplyvom zvyškových rizík	<ul style="list-style-type: none"> • Vybudovať komplexný záložný systém mimo priestorov budovy v bezpečnej vzdialenosti • Zabezpečiť niekoľkonásobné záložne kópie • Vytvorenie chráneného komunikačného dátového kanálu na záložne pracovisko • Zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti • Kontrolovať, či sú splnené protipožiarne opatrenia • Inštalovať EZS, bezpečnostné mreže, dvere • Zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov 	<p>V prípade vyradenia IS z činnosti</p> <ul style="list-style-type: none"> • 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 <p>V prípade napadnutia len časti IS</p> <ul style="list-style-type: none"> • Presunúť aktíva do vyhovujúcich priestorov • Inštalovať záložne databázy a pripojenia ak sú nutné • Spustiť prevádzku • Po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou

V. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.

4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť I
Kľúčový režim spoločnosti a povinnosti držiteľov kľúčov

I. Kľúčový režim Prevádzkovateľa a povinnosti držiteľov kľúčov

1. Kľúče používané na vstup do priestorov spoločnosti a otváranie zariadení v ktorých sa uschovávajú, počítače, počítačové média a písomnosti obsahujúce osobné údaje (ďalej „evidované kľúče“) sa pridelujú osobám, ktoré určí spoločnosť.
2. Evidované kľúče prideluje zodpovedný zamestnanec spoločnosti.
3. Každý evidovaný kľúč musí byť označený jedinečným kódom (znakom), pod ktorým je zapísaný v evidencii. Prevádzkovateľ vedie o evidovaných kľúčoch evidenciu, ktorá obsahuje:
 - a) identifikačný kód kľúča;
 - b) označenie dverí, zariadenia alebo zámku, ktorý sa kľúčom otvára;
 - c) dátum zaradenia kľúča do evidencie;
 - d) identifikačné údaje osoby, ktorej bol kľúč pridelený;
 - e) dátum pridelenia (vrátenia) kľúča a podpis osoby, ktorá preberá (vracia) kľúč.
4. Osoba, ktorá nie je poverená na prácu s osobnými údajmi môže mať pridelené a samostatne používať evidované kľúče od priestorov spoločnosti iba s podmienkou, že pamäťové média, písomnosti a iné dokumenty obsahujúce osobné údaje sú uzamykané v zariadeniach na úschovu prístupných iba držiteľom evidovaných kľúčov.
5. Držiteľ evidovaných kľúčov je povinný:
 - a) zaobchádzať s kľúčmi tak, aby nedošlo k ich strate alebo krádeži;
 - b) osobne dohliadať nad prácou neoprávnených osôb (napr. pomocný a technický personál) v priestoroch prevádzkovateľa, zabrániť im prístup k osobným údajom a zabezpečiť, aby sa v priestoroch, v ktorých sa spracúvajú osobné údaje nezdržiavali neoprávnené osoby z iných ako pracovných dôvodov,
 - c) uzamykať okná, dvere a zariadenia, od ktorých má pridelené evidované kľúče vždy, keď sa vzdáľuje z priestorov prevádzkovateľa,
 - d) pred uzamknutím a opustením prevádzkovateľa uschovať všetky pamäťové média a písomnosti obsahujúce osobné údaje, ktoré sú voľne položené v priestoroch Prevádzkovateľa,
 - e) pred uzamknutím a opustením prevádzkovateľa uschovať všetky pamäťové média a písomnosti obsahujúce osobné údaje, ktoré sú voľne položené v priestoroch Prevádzkovateľa,
 - f) bez omeškania oznámiť prevádzkovateľovi stratu alebo krádež evidovaných kľúčov,
 - g) na výzvu prevádzkovateľa, v stanovenom termíne odovzdať evidované kľúče.

II. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.

4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť J

SMERNICA O ROZSAHU PRÁV, POVINNOSTÍ A ZODPOVEDNOSTI SPOLOČNOSTI A OPRÁVNENÝCH OSÔB

I. Všeobecné ustanovenia

1. Účelom tejto časti smernice je určiť rozsah práv, povinností a zodpovednosti prevádzkovateľa a oprávnených osôb.
2. Oprávnená osoba je každá fyzická osoba, ktorá spracúva osobné údaje v rámci svojho pracovnoprávneho vzťahu alebo obdobného pracovnoprávneho vzťahu alebo na základe poverenia spoločnosti.
3. Používateľ informačného systému je oprávnená osoba, ktorá spracúva osobné údaje v rámci výkonu svojho povolania v danom informačnom systéme.
4. Spracúvaním osobných údajov je spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.

II. Práva a povinnosti spoločnosti (prevádzkovateľa)

1. Za bezpečnosť osobných údajov zodpovedá spoločnosť v pozícii prevádzkovateľa.
2. Spoločnosť spracúva osobné údaje prostredníctvom poučených zamestnancov – oprávnených osôb, ktoré musia svojím podpisom potvrdiť písomné poučenie, ktoré tvorí prílohu č. 6 tejto Dokumentácie k ochrane osobných údajov.
3. Spoločnosť je povinná písomne poučiť všetky oprávnené osoby o ich právach, povinnostiach a zodpovednosti podľa predchádzajúceho ods. 2 tejto časti smernice pred vykonaním prvého spracúvania osobných údajov.
4. Osoba zodpovedná za konkrétny informačný systém vymedzený v Časti A tejto Dokumentácie k ochrane osobných údajov prideluje oprávneným osobám oprávnenia, ich rozsah, popis povolených činností, spôsob ich identifikácie (*proces, pomocou ktorého informačný systém rozpozná osobu, avšak neoverí si, či ide skutočne o ňu – prehlásenie totožnosti*) a autentizácie (*proces, ktorý nasleduje spravidla po identifikácii, a ktorý overí, že prihlásená osoba je naozaj tá, za ktorú sa vydáva - ide o overenie totožnosti*).
5. Rozsah zodpovednosti jednotlivých oprávnených osôb schvaľuje štatutárny orgán spoločnosti. Spoločnosť je povinná určiť oprávnenej osobe postupy, ktoré je povinná pri spracúvaní osobných údajov dodržiavať.
6. Spoločnosť zabezpečí kontrolu vstupu do priestorov spoločnosti, kde sa spracúvajú osobné údaje.
7. Po ukončení pracovného pomeru (obdobného pomeru) spoločnosť zabezpečí odobratie prístupu oprávnenej osoby do evidencie (odovzdanie preukazu, hesla, ktorým sa prihlasuje do informačného systému), kde sa spracúvajú osobné údaje. O tomto odovzdaní sa vyhotoví písomný protokol.

III. Práva a povinnosti oprávnených osôb

1. Oprávnenej osobe musia byť sprístupnené informačné systémy osobných údajov za účelom ich spracúvania.
2. Oprávnená osoba má právo na opätovné poučenie, v prípade podstatnej zmeny jej pracovného zaradenia (ak sa podstatne zmenil obsah náplne jej pracovných činností).

3. Oprávnená osoba môže odmietnuť vykonanie spracovateľskej operácie, ktorý je v rozpore so všeobecne záväzným predpisom.
4. Oprávnená osoba má právo pre prevádzkovateľa (spoločnosť) získavať osobné údaje výlučne len na základe príslušného právneho základu a len na stanovený účel podľa Časti A tejto dokumentácie. Je zakázané získavať osobné údaje na účel a odlišný právny základ ako je vymedzený v Časti A tejto dokumentácie alebo za účelom inej činnosti.
5. Oprávnená osoba musí vedieť preukázať súhlas zo spracovaním osobných údajov od dotknutej osoby v prípade, ak sa osobné údaje spracúvajú na základe súhlasu.
6. Oprávnená osoba má povinnosť chrániť prijaté osobné údaje pred stratou, poškodením, zneužitím, neoprávneným prístupným alebo inou neprípustnou formou spracovania.
7. Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch s ktorými a v rámci svojho pracovnoprávneho vzťahu prichádza do kontaktu, a to aj po skončení jej pracovnoprávneho vzťahu.
8. Oprávnená osoba má povinnosť prevádzkovateľovi bezodkladne oznámiť porušenie ochrany osobných údajov.
9. Oprávnená osoba zodpovedá za poriadok na pracovisku a odloženie všetkých dokumentov, ktoré obsahujú osobné údaje, tak, aby nedošlo k ich vyzradeniu.
10. Oprávnená osoba spracúva len správne, úplné a aktualizované osobné údaje. Nesprávne a neúplné osobné údaje je povinná bezodkladne vymazať.
11. Vzájomné zastupovanie oprávnených osôb je možné výlučne na základe písomného súhlasu spoločnosti.
12. Do priestorov, v ktorých sa spracúvajú osobné údaje, je vstup zabezpečený výhradne pre oprávnené osoby. Iná osoba môže do týchto priestorov vstúpiť len v sprievode oprávnenej osobe na základe písomného súhlasu spoločnosti. V takomto prípade sa nesmú zobrazovať osobné údaje osôb odlišných od sprevádzajúcej osoby.

IV. Rozsah oprávnení a popis povolených činností oprávnených osôb

1. Štatutárne orgány majú úplný prístup k osobným údajom zamestnancov, dotknutých osôb vymedzený príslušnými internými predpismi spoločnosti, prípadne pracovnou náplňou (právo spúšťať pridelené procesy a čítať údaje a informácie vrátane osobných údajov dotknutých osôb). Spôsob identifikácie a autentizácie je zabezpečený prostredníctvom užívateľského mena a hesla. Popis spracovateľských operácií/činností: získavanie, zaznamenávanie, usporadúvanie, uchovávanie, zmena, oprava, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.
2. Vedúci zamestnanci majú obmedzený prístup k osobným údajom zamestnancov, dotknutých osôb vymedzený pracovnou náplňou, osobitnými právnymi predpismi (najmä zákon č. 362/2011 Z. z.) a príslušnými internými predpismi (právo spúšťať pridelené procesy a čítať a editovať údaje a informácie vrátane osobných údajov dotknutých osôb). Spôsob identifikácie a autentizácie je zabezpečený prostredníctvom užívateľského mena a hesla. Popis spracovateľských operácií/činností: získavanie, zaznamenávanie, usporadúvanie, uchovávanie, zmena, oprava, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.
3. Spracovateľskú operáciu likvidácia osobných údajov môže vykonávať výlučne osoba, ktorá je zodpovedná za informačný systém podľa Časti A tejto smernice.

4. Používatelia informačných systémov (napr. osoby na základe pracovného pomeru alebo obdobného pracovného vzťahu) majú obmedzený prístup k osobným údajom zamestnancov, dotknutých osôb vymedzený pracovnou náplňou, osobitnými právnymi predpismi (najmä zákon č. 362/2011 Z. z.) a príslušnými internými predpismi (právo spúšťať pridelené procesy a čítať a editovať údaje a informácie vrátane osobných údajov dotknutých osôb). Spôsob identifikácie a autentizácie je zabezpečený prostredníctvom užívateľského mena a hesla. Popis spracovateľských operácií/činnosti: získavanie, zaznamenávanie, usporadúvanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami.
5. Údržbár výpočtovej techniky (napr. spoločnosť zabezpečujúca servis a údržbu výpočtovej techniky) má obmedzený prístup k osobným údajom vymedzený zmluvou medzi spoločnosťou a sprostredkovateľom (právo spúšťať pridelené procesy a čítať údaje a informácie vrátane osobných údajov dotknutých osôb). Spôsob identifikácie a autentizácie je zabezpečený prostredníctvom užívateľského mena a hesla alebo sprístupnenia na základe zdieľanej správy po zadaní hesla, ktorým disponuje výlučne len spoločnosť. Popis spracovateľských operácií/činnosti: uchovávanie, vyhľadávanie, prehliadanie, zálohovanie, archivovanie. Spracovateľské operácie sú vykonávané len vo výnimočných prípadoch výlučne na základe pokynu spoločnosti.

V. Rozsah zodpovedností oprávnených osôb

1. Štatutárny orgán spoločnosti zodpovedá za dodržiavanie Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov ďalej ako „GDPR“) a v častiach kde sa neuplatňuje GDPR podľa zákona č. 18/2018 Z.z. o ochrane osobných údajov v každodennej praxi spoločnosti, zodpovedá za prijatie vhodných technických a organizačných opatrení, aby zabezpečil a bol schopný preukázať súlad spracúvania osobných údajov s GDPR a osobitnými právnymi predpismi. Zodpovedá za prijatie primeraných politík ochrany osobných údajov, za implementáciu bezpečnostných opatrení a dodržiavanie pravidiel ochrany osobných údajov v spoločnosti.
2. Štatutárny orgán podporuje multidisciplinárny prístup k ochrane osobných údajov v informačných systémoch a koordinuje spoluprácu vedúcich pracovníkov, zamestnancov ako používateľov informačných systémov a iným externých dodávateľov (právnici, bezpečnostní technici, ...).
3. Vedúci zamestnanci zodpovedajú za dodržiavanie GDPR a v častiach kde sa neuplatňuje GDPR podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov v každodennej praxi spoločnosti v rámci svojej pôsobnosti vymedzenej pracovnou zmluvou a Dokumentáciu k ochrane osobných údajov. Zodpovedajú za udržiavanie kontaktov s orgánmi dohliadajúcimi nad dodržiavaním zákonnosti s cieľom zabezpečiť v prípade bezpečnostného incidentu vykonanie potrebných krokov, udržiava primeranú ochranu aktív spoločnosti.
4. Používatelia informačného systému zodpovedajú za dodržiavanie GDPR a v častiach kde sa neuplatňuje GDPR podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov v každodennej praxi spoločnosti v rámci svojej pôsobnosti vymedzenej pracovnou zmluvou a Dokumentáciu k ochrane osobných údajov, najmä každodennú bezpečnosť im pridelených aktív, dodržiavanie zásad správneho spracúvania osobných údajov, dodržiavanie práv dotknutých osôb, dodržiavanie bezpečnostných procesov vyplývajúcich z pracovných zmlúv, interných predpisov spoločnosti.
5. Údržbár výpočtovej techniky zodpovedá v rozsahu vymedzenom v pracovnej zmluve, prípadne v zmluve medzi spoločnosťou a sprostredkovateľom, ktorú so spoločnosťou uzavrel.

VI. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.

3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti

Časť K

PRAVIDLÁ POUŽÍVANIA ZÁKLADNÝCH DOKUMENTOV V OBLASTI OCHRANY OSOBNÝCH ÚDAJOV

I. Všeobecné pravidlá pre používanie dokumentov

1. Prílohou tejto smernice je súbor základných dokumentov vyplývajúcich z právnej úpravy ochrany osobných údajov, ktorý zahŕňa:
 - a) Informácie pre účastníkov podujatí o spracovaní osobných údajov,
 - b) Informácie pre zamestnancov o spracúvaní osobných údajov,
 - c) Záznam o spracovateľských činnostiach,
 - d) Poučenie o mlčanlivosti zamestnancov,
 - e) Záznam o poučení oprávnených osôb,
 - f) Zmluva o spracovaní osobných údajov medzi našou spoločnosťou a sprostredkovateľom,
 - g) Záznam o nutnosti vypracovať posúdenie vplyvu na ochranu osobných údajov,
 - h) Záznam o nutnosti stanoviť zodpovednú osobu,
 - i) Súhlas dotknutej osoby so spracovaním osobných údajov.
2. V tejto časti smernice sú popísané základné pravidlá pre používanie dokumentov uvedených v ods. 1. V prípade ak táto smernica neupravuje akúkoľvek otázku alebo postup súvisiaci s používaním týchto dokumentov, je potrebné sa obrátiť na určeného zodpovedného zamestnanca spoločnosti.
3. Na akúkoľvek zmenu, úpravu alebo doplnenie dokumentov podľa ods. 1 je potrebný súhlas zodpovedného zamestnanca spoločnosti.
4. Otázky, ktoré nespádajú do kompetencie určenej zodpovednej osoby spoločnosti je potrebné adresovať internému alebo externému právnenému poradcovi. Uvedené platí aj pre tie prípady, v ktorých sa ukáže potreba vypracovania dodatočných dokumentov, ktoré nie sú prílohou tejto smernice.

II. Informácie pre účastníkov odborného podujatia o spracovaní osobných údajov

1. Spoločnosť má povinnosť informovať všetky dotknuté osoby o spracúvaní ich osobných údajov, a to bez ohľadu na právny základ spracovania osobných údajov. Tento dokument je preto potrebné poskytnúť dotknutej osobe aj v prípade, ak spracúvanie osobných údajov nie je založené na súhlase dotknutej osoby, ale vychádza napr. z uzatvorenej zmluvy, zo zákona alebo z iného právneho základu.
2. Plnenie informačnej povinnosti spoločnosti vo vzťahu k účastníkom odborného podujatia je bližšie upravené v Časti F tejto smernice.
3. Spoločnosť je povinná preukázať splnenie povinnosti podľa ods. 1. Za účelom ochrany spoločnosti a možnosti dostatočného preukázania splnenia tejto povinnosti je potrebné informácie dotknutým osobám poskytovať v písomnej forme, a to nasledovným spôsobom:
 - a) Informácie pre účastníkov odborného podujatia o spracovaní osobných údajov umiestniť na viditeľnom mieste v priestoroch spoločnosti, respektíve na mieste konania podujatia, ktoré je dostupné všetkým účastníkom odborného podujatia a upozorniť ich na povinnosť oboznámenia sa s nimi. V prípade, že spoločnosť používa na svoju prezentáciu webové sídlo, odporúčame zverejnenie základných informácií pre účastníkov odborného podujatia na webovom sídle (odporúčaný postupom je zverejniť základné informácie pre účastníkov odborného podujatia zaužívaným spôsobom v spodnej lište webstránky pod označením napr. „Podmienky ochrany súkromia“, „Ochrana súkromia“ alebo „Ochrana osobných údajov“ a pod.)
4. Podpis dotknutej osoby potvrdzujúci prijatie informácie o spracúvaní osobných údajov nie je možné zamieňať so súhlasom na spracovanie osobných údajov. Ide o dva odlišné dokumenty, ktoré sa dotknutej osobe (podľa okolností konkrétnej situácie) môžu poskytnúť súčasne alebo aj nezávisle na sebe. Prevzatie informácie preto nenahrádza súhlas so spracovaním osobných údajov.

5. Pred poskytnutím tohto dokumentu dotknutej osobe je potrebné sa uistiť, že uvádzané informácie sú dostatočne presné a úplné. Ak by sa akákoľvek časť tohto dokumentu ukázala ako nepresná, nepravdivá, neúplná alebo iným spôsobom nedostatočná, je potrebné použiť postup podľa čl. I ods. 3 a 4 tejto časti smernice.
6. Vzor sa nachádza v prílohe č. 1A, 1B, 1C a 1D tejto dokumentácie.

III. Informácie pre zamestnancov o spracovaní osobných údajov

1. Spoločnosť má povinnosť informovať všetky dotknuté osoby o spracúvaní ich osobných údajov, a to bez ohľadu na právny základ spracovania osobných údajov. Tento dokument je preto potrebné poskytnúť dotknutej osobe aj v prípade, ak spracúvanie osobných údajov nie je založené na súhlase dotknutej osoby, ale vychádza napr. z uzatvorenej zmluvy, zo zákona alebo z iného právneho základu.
2. Plnenie informačnej povinnosti spoločnosti vo vzťahu k účastníkom odborného podujatia je bližšie upravené v Časti F tejto smernice.
3. Spoločnosť je povinná preukázať splnenie povinnosti podľa ods. 1. Za účelom ochrany spoločnosti a možnosti dostatočného preukázania splnenia tejto povinnosti je potrebné informácie dotknutým osobám poskytovať v písomnej forme, a to nasledovným spôsobom:
 - a) kde je to možné, je potrebné zabezpečiť podpis dotknutej osoby – zamestnanca potvrdzujúci prijatie informácie o spracúvaní osobných údajov. V prípade ak nie je možné zabezpečiť informovanie v písomnej forme alebo ak nie je možné získať písomné potvrdenie dotknutej osoby o prijatí tejto informácie, je potrebné bezodkladne informovať zodpovedného zamestnanca spoločnosti a vyžiadať si usmernenie k ďalšiemu postupu.
4. Podpis dotknutej osoby potvrdzujúci prijatie informácie o spracúvaní osobných údajov nie je možné zamieňať so súhlasom na spracovanie osobných údajov. Ide o dva odlišné dokumenty, ktoré sa dotknutej osobe (podľa okolností konkrétnej situácie) môžu poskytnúť súčasne alebo aj nezávisle na sebe. Prevzatie informácie preto nenahrádza súhlas so spracovaním osobných údajov.
5. Pred poskytnutím tohto dokumentu dotknutej osobe je potrebné sa uistiť, že uvádzané informácie sú dostatočne presné a úplné. Ak by sa akákoľvek časť tohto dokumentu ukázala ako nepresná, nepravdivá, neúplná alebo iným spôsobom nedostatočná, je potrebné použiť postup podľa čl. I ods. 3 a 4 tejto časti smernice.
6. Vzor sa nachádza v prílohe č. 2 tejto dokumentácie.

IV. Záznam o spracovateľských činnostiach

1. Pri jednotlivých spracovateľských činnostiach je povinnosť viesť osobitné záznamy. Spracovateľská činnosť je súborom spracovateľských operácií (ako napr. získavanie osobných údajov, ich poskytovanie, zverejňovanie, uchovávanie a pod.), ktoré sú vykonávané na konkrétny účel spracúvania osobných údajov, na právnom základe a určenými prostriedkami spracúvania.
2. Obsah, štruktúra a forma záznamu o spracovateľských činnostiach je pevne stanovená a je potrebné ju rešpektovať. Vzor záznamu o spracovateľských činnostiach je prílohou tejto smernice.
3. V nasledujúcich výnimočných prípadoch vypracovanie záznamov o spracovateľských činnostiach nie je potrebné:
 - a) ak spoločnosť zamestnáva menej ako 250 osôb,
 - b) ak nie je pravdepodobné, že spracúvanie osobných údajov povedie k riziku pre práva a slobody dotknutej osoby,

- c) ak je spracúvanie osobných údajov príležitostné alebo nezahŕňa osobitné kategórie osobných údajov (ako napr. informácie odhaľujúce rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby),
 - d) ak spracúvanie osobných údajov nezahŕňa údaje o uznaní viny za trestné činy a priestupky.
4. Posúdenie uplatnenia výnimiek podľa ods. 3 a teda rozhodnutie, že spoločnosť nebude vyhotovovať záznamy o spracovateľských činnostiach patrí do výlučnej kompetencie zodpovedného zamestnanca pre ochranu osobných údajov.
 5. V prípade akýchkoľvek nejasností ohľadom uplatňovania tohto článku smernice platí, že spoločnosť je povinná vyhotovovať záznamy o spracovateľských činnostiach.
 6. Príloha č. 3 tejto dokumentácie.

V. Poučenie o povinnosti zachovávať mlčanlivosť a ochranu osobných údajov pre zamestnanca spoločnosti

1. Spoločnosť ako prevádzkovateľ a jej sprostredkovatelia (ďalej ako „spoločnosť“) sú povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.
2. Povinnosť zachovávať mlčanlivosť obdobne platí aj pre zamestnancov spoločnosti, ktorí z titulu svojej práce alebo vzhľadom na svoje povinnosti prídu do styku s osobnými údajmi. Povinnosť mlčanlivosti podľa prvej vety musí trvať aj po skončení pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu tejto fyzickej osoby.
3. Povinnosť mlčanlivosti podľa predchádzajúcich odsekov neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov.
4. Vzor sa nachádza v prílohe č. 4 tejto dokumentácie.

VI. Záznam o poučení oprávnených osôb

1. Spoločnosť nesie zodpovednosť za zákonné spracúvanie osobných údajov vrátane spracúvania osobných údajov oprávnenými osobami.
2. Oprávnenou osobou sa na účely tejto smernice rozumie každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu alebo obdobného pracovnoprávneho vzťahu so spoločnosťou.
3. Spoločnosť je povinná prijať primerané a účinné opatrenia na zaistenie bezpečnosti spracúvania osobných údajov. Rovnako je povinná na prijatie svojej zodpovednosti a deklarovania plnenia opatrení prijať adekvátne politiky ochrany osobných údajov do vnútra alebo aj navonok. Jedným z bezpečnostným opatrením po stránke organizačnej a personálne je poučenie oprávnených osôb.
4. Na účely preukázania povinnosti podľa predchádzajúceho ods. 3 tejto časti smernice spoločnosť písomne poučí oprávnené osoby o jej právach a povinnostiach a zodpovednosti, ktoré vyplývajú z ich porušenia.
5. Spoločnosť je povinná vykonať nové poučenie, ak došlo k podstatnej zmene pracovného alebo funkčného zaradenia oprávnenej osoby, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného alebo funkčného zaradenia. Rovnako je spoločnosť povinná poučiť každú ďalšiu oprávnenú osobu pri nástupe do zamestnania pred začatím spracúvania osobných údajov.

6. Vzor sa nachádza v prílohe č. 5 tejto dokumentácie.

VII. Zmluva o spracovaní osobných údajov

1. Zmluvu o spracúvaní osobných údajov uzatvára spoločnosť v tých prípadoch, v ktorých vystupujeme ako tzv. prevádzkovateľ, pričom túto zmluvu uzatvárame s tzv. sprostredkovateľom.
2. Spoločnosť vystupuje v postavení tzv. prevádzkovateľa v tých prípadoch, v ktorých spoločnosť sama alebo spoločne s inými subjektami určí účely a prostriedky spracúvania osobných údajov.
3. Tretí subjekt je považovaný za sprostredkovateľa v tom prípade, ak spracúva osobné údaje v mene prevádzkovateľa (napr. v mene spoločnosti).
4. Ak je spoločnosť prevádzkovateľom a poskytuje osobné údaje fyzických osôb (napr. osobné údaje našich zamestnancov, našich účastníkov odborného podujatia a pod.) inému subjektu, ktorý tieto osobné údaje ďalej spracúva v mene spoločnosti, potom je spoločnosť povinná zaslať tomuto subjektu samostatnú zmluvu o spracúvaní osobných údajov. Vzor tejto zmluvy tvorí prílohu tejto smernice.
5. Bez uzatvorenia zmluvy o spracúvaní osobných údajov spoločnosť nemôže poskytnúť osobné údaje inému subjektu.
6. Zmluvu o spracúvaní osobných údajov je spoločnosť povinná uzatvoriť s iným subjektom (ktorý je v postavení sprostredkovateľa) bez ohľadu na prípadnú existenciu iného zmluvného vzťahu.
7. Zmluva sa nachádza v prílohe č. 9, v prílohe č. 10, v prílohe č. 11, v prílohe č. 12, v prílohe č. 13, v prílohe č. 14, v prílohe č. 15, v prílohe č. 16, v prílohe č. 17 a v prílohe č. 18 tejto dokumentácie.

VIII. Záznam o nutnosti vypracovať posúdenie vplyvu na ochranu osobných údajov

1. Spoločnosť je povinná vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov v prípade, ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne **povedie k vysokému riziku pre práva a slobody fyzických osôb**.
2. Spoločnosť vypracovala analýzu bezpečnosti, ktorá sa nachádza v Časti B tejto smernice. V prípade, že záverom analýzy rizík je skutočnosť, že spracúvanie osobných údajov povedie k vysokému riziku pre práva a slobody fyzických osôb je nevyhnutné vykonať posúdenie vplyvu.
3. Posúdenie vplyvu na ochranu údajov sa vyžaduje, najmä v prípadoch ak by spoločnosť:
 - a) systematicky a rozsiahlo hodnotila osobné aspekty týkajúce sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu;
 - b) spracúvala vo veľkom rozsahu osobitné kategórie údajov podľa článku 9 ods. 1 alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky podľa článku 10, alebo
 - c) systematicky monitorovala verejne prístupné miesta vo veľkom rozsahu.
4. Ak nie sú splnené podmienky podľa ods. 2 a 3 tejto časti smernice je potrebné spísať záznam s odôvodnením prečo nie je potrebné vykonať posúdenie vplyvu na ochranu osobných údajov. V opačnom prípade je potrebné vykonať samotné posúdenie vplyvu.
5. Záznam sa nachádza v prílohe č. 6 tejto dokumentácie.

IX. Záznam o nutnosti určiť zodpovednú osobu

1. Prevádzkovateľ si musí určiť zodpovednú osobu v každom prípade, ak:

- a) spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci;
 - b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo
 - c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky.
2. V prípade, že spoločnosť ako prevádzkovateľ vyhodnotí, že nespadá do žiadnej z kategórií podľa ods. 1 tejto časti smernice nie je potrebné, aby bola spoločnosťou určená zodpovedná osoba. O tejto skutočnosti je potrebné spísať záznam s odôvodnením.
 3. Spoločnosť má možnosť určiť si zodpovednú osobu aj dobrovoľne.
 4. V prípade určenia zodpovednej osoby bez ohľadu na dobrovoľnosť, spoločnosť je povinná oznámiť úradu túto skutočnosť a identifikačné údaje zodpovednej osoby, a to za účelom riadneho plnenia úloh úradu, aby mohol vhodne a personalizovane zodpovednú osobu osloviť a kontaktovať, keď s ňou bude komunikovať. Úrad takto získané osobné údaje využíva a bude využívať výlučne na účely kontaktovania zodpovednej osoby pri komunikácii s ňou.
 5. Postavenie zodpovednej osoby je nezávislé a nestranné, zodpovedná osoba je povinná zachovávať mlčanlivosť v súvislosti s výkonom úloh zodpovednej osoby. Spoločnosť môže zasahovať do plnenia úloh zodpovednej osoby len ak sú princípy nestrannosti a nezávislosti zodpovednej osoby zachované.
 6. Záznam sa nachádza v prílohe č. 7 tejto dokumentácie.

X. Súhlas so spracovaním osobných údajov

1. Súhlas so spracovaním osobných údajov je jedným z právnych základov (t.j. právnych dôvodov), ktoré umožňujú spracovanie osobných údajov dotknutej osoby.
2. Súhlas so spracovaním osobných údajov je možné použiť až potom, ak nie je možné určiť iný právny základ na spracúvanie osobných údajov.
3. Súhlas so spracovaním osobných údajov musí byť formulovaný ľahko a jednoducho a musí byť odlišiteľný od iného súvisiaceho textu. Súhlas preto nemôže byť súčasťou všeobecných obchodných podmienok alebo iných obdobných dokumentov.
4. Pri udeľovaní súhlasu so spracovaním osobných údajov sa vyžaduje aktivita dotknutej osoby, ktorá má mať dostatočnú možnosť slobodne sa rozhodnúť o udelení súhlasu.
5. Dotknutá osoba môže kedykoľvek svoj súhlas so spracovaním osobných údajov odvolať, to však nesmie byť prekážkou ďalšieho pokračovania právneho vzťahu medzi dotknutou osobou a našou spoločnosťou.
6. Pred poskytnutím súhlasu na podpis dotknutej osobe je potrebné ho skontrolovať, aby v ňom boli uvedené presné a pravdivé informácie o zamýšľanom účele spracovania osobných údajov, o dotknutej osobe, o rozsahu spracúvaných osobných údajov, o účele spracovania a o dobe spracovania osobných údajov. Ak by sa akákoľvek časť súhlasu ukázala ako nepresná, nepravdivá, neúplná alebo iným spôsobom nedostatočná, je potrebné použiť postup podľa čl. 1 ods. 3 a 4 tejto časti smernice.
7. V prípade ak do 25.05.2018 boli na spracúvanie osobných údajov požívané súhlasy dotknutých osôb ako právne základy, tieto súhlasy je potrebné skontrolovať podľa nových požiadaviek GDPR. Ak tieto staré súhlasy nespĺňajú náležitosti novej právnej úpravy, nie je podľa nich možné pokračovať v spracúvaní osobných údajov. O tejto skutočnosti je potrebné bezodkladne informovať zodpovedného zamestnanca

v oblasti ochrany osobných údajov a prijať nevyhnutné opatrenie na zabezpečenie súladu s právnou úpravou.

8. Vzor sa nachádza v prílohe č. 19 tejto dokumentácie.

XI. Vzorový formulár pre zdokumentovanie porušenia ochrany osobných údajov

1. V prípade, že dôjde k bezpečnostnému incidentu spoločnosť je povinná postupovať podľa Časti H Hlásenie bezpečnostných incidentov, pričom spoločnosť má povinnosť zdokumentovať porušenie ochrany osobných údajov.
2. Vzor sa nachádza v prílohe č. 8 tejto dokumentácie.

XII. Záverečné ustanovenia

1. Táto časť dokumentácie je záväzná pre všetky oprávnené osoby spoločnosti.
2. Za dodržiavanie tejto časti dokumentácie zodpovedá štatutárny orgán spoločnosti.
3. Porušenie ustanovení tejto dokumentácie je závažným porušením stanov spoločnosti.
4. Táto časť dokumentácie nadobúda účinnosť dňom jej podpisu.

V, dňa

.....
Slovenská spoločnosť všeobecného praktického lekárstva
MUDr. Peter Makara, MPH, prezident spoločnosti