

Slovenská federácia pétanque

Právna forma: Občianske združenie

IČO/SID: 36064742

Sídlo: Ilýrska 2, 85110 Bratislava - Rusovce

Bezpečnostný projekt

Bratislava, 1.1.2018

História dokumentu

Číslo verzie	Dátum verzie	Popis zmien	Zmeny označené
1.0	1.1.2018	Prvá verzia	

Obsah

1	Úvod	4
1.1	Definície	5
1.2	Základné údaje o prevádzkovateľovi	5
1.3	Zoznam informačných systémov	5
1.4	Bezpečnostný zámer	6
1.4.1	Bezpečnostné ciele	6
1.4.2	Vymedzenie okolia informačného systému	6
1.5	Analýza bezpečnosti informačného systému	8
1.5.1	Identifikácia aktív a vlastníkov	10
1.5.2	Analýza rizík	11
1.5.3	Vymedzenie hraníc určujúcich množinu zostatkových rizík	14
1.6	Bezpečnostná smernica	15
1.6.1	Popis bezpečnostných opatrení	15
1.6.2	Rozsah oprávnení	17
1.6.3	Rozsah zodpovednosti	18
1.6.4	Spôsob, forma a periodicita kontrolnej činnosti	19
1.6.5	Postupy pri haváriách, poruchách a mimoriadnych situáciách	19
1.6.6	Preventívne opatrenia na zníženie rizika vzniku mimoriadnych udalostí	19

1 Úvod

Slovenská federácia pétanque (ďalej len „SFP“) si je vedomá dôležitosť zabezpečiť ochranu svojich aktív, aktivít a spolupracujúcich subjektov. Neoddeliteľnou súčasťou týchto aktív sú nielen citlivé informácie, ale aj osobné údaje členov, hráčov a spolupracujúcich subjektov.

Pre vytvorenie základného rámca pravidiel tejto ochrany a splnenie zákonných požiadaviek dalo vedenie „SFP“ vypracovať tento dokument, ktorý je bezpečnostným projektom „SFP“. Tento bezpečnostný projekt je vypracovaný v zmysle zákona č. 122/2013 Z.z. o ochrane osobných údajov v platnom znení (ďalej len „Zákon“).

Bezpečnostný projekt určuje požiadavky na ochranu osobných údajov spracúvaných v informačných systémoch „SFP“.

Bezpečnostný projekt je udržiavaný v aktuálnom stave. Preto sa vyhodnocuje, reviduje a aktualizuje :

- v prípade významných organizačných a technických zmien,
- pri zistení nových rizík,
- ak je zaznamenaný zvýšený počet bezpečnostných incidentov.

Za pravidelné vyhodnocovanie, revízie a prípravu zmien tohto bezpečnostného projektu zodpovedá osoba poverená vedením agendy ochrany osobných údajov (ďalej len „poverená osoba“). Bezpečnostný projekt predkladá na schválenie prezídiu „SFP“.

Správa bezpečnostného projektu môže byť uskutočňovaná dodávateľským spôsobom.

Bezpečnostný projekt obsahuje dôverné informácie, preto musí byť uchovávaný na bezpečnom mieste, ktoré umožňuje jeho ochranu pred zverejnením neoprávneným osobám, zničením alebo modifikáciou obsahu.

Vybrané časti tohto dokumentu môžu byť na základe pracovnej potreby prístupné pre poverené osoby „SFP“ alebo poverené osoby tretích strán, pokiaľ je to pre ich činnosť nevyhnutné a taktiež kontrole uskutočňovanej v zmysle príslušných ustanovení „Zákona“.

1.1 Definície

Chránený priestor – priestor (oblasť) určený „SFP“ pre vykonávanie operácií s osobnými údajmi.

Poverená osoba – osoba poverená SFP dohľadom nad plnením podmienok ustanovení „Zákona“.

Mobilná pracovná stanica – prenosné zariadenie na spracovanie informácií prostredníctvom nainštalovaných aplikácií (mobilný telefón, tablet, notebook, ...).

Pri spracovávaní tohto bezpečnostného projektu boli primerane aplikované ustanovenia noriem STN ISO/IEC 27001 a STN ISO/IEC 27002.

1.2 Základné údaje o prevádzkovateľovi

Prevádzkovateľom spracúvajúcim osobné údaje je SFP

Slovenská federácia pétanque

Právna forma: Občianske združenie

IČO/SID: 36064742

Sídlo: 851 10 Bratislava - Rusovce, Ilýrska 2

1.3 Zoznam informačných systémov

Tento bezpečnostný projekt sa vzťahuje na nasledovné informačné systémy:

Informačné systémy osobných údajov pre hlavné firemné procesy

- a) IS účtovné doklady

Informačné systémy osobných údajov pre podporné firemné procesy

- b) IS účtovné doklady
- c) IS práva dotknutých osôb
- d) IS správa registratúry

Pre tieto informačné systémy osobných údajov je „SFP“ prevádzkovateľ.

Podrobnosti o každom z týchto informačných systémov sú uvedené v evidenčných formulároch, ktoré sú súčasťou tohto bezpečnostného projektu.

1.4 Bezpečnostný zámer

Tento dokument je bezpečnostným zámerom „SFP“ vypracovaný v zmysle zákona č. 122/2013 Z.z. o ochrane osobných údajov a je súčasťou bezpečnostného projektu.

1.4.1 Bezpečnostné ciele

Základnými bezpečnostnými cieľmi „SFP“ sú:

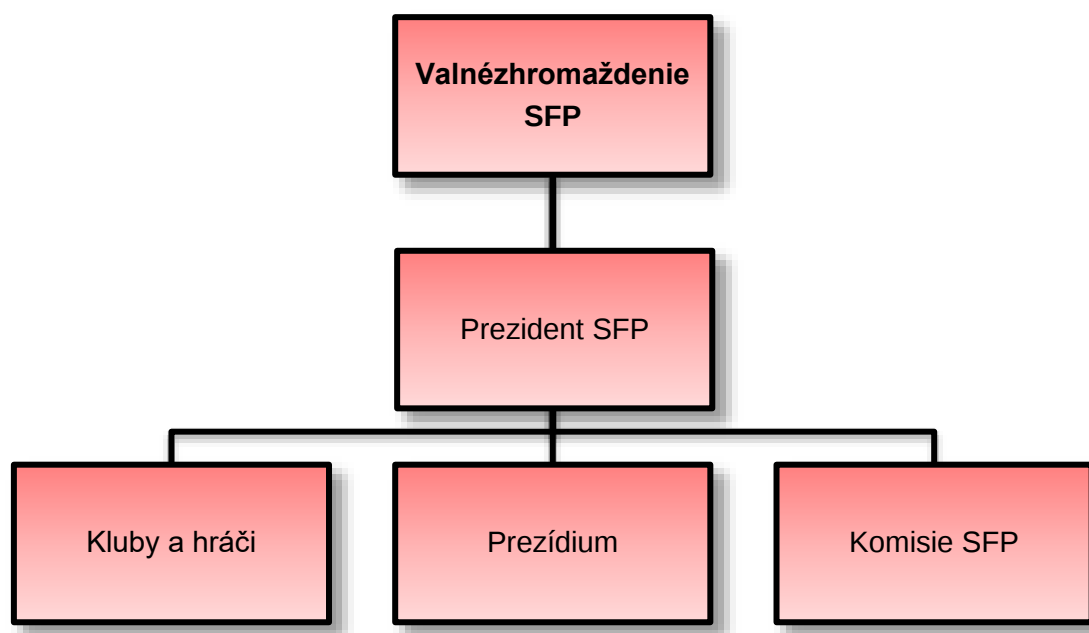
1. Deklarovať záväzok vedenia „SFP“ ochraňovať osobné údaje a neustále túto ochranu zlepšovať,
2. Zabezpečiť ochranu osobných údajov subjektov v zmysle ustanovení „Zákona“,
3. Vyvárať a neustále vylepšovať predpoklady pre také technické a organizačné opatrenia, ktoré zabezpečia ochranu osobných údajov v zmysle požiadaviek „Zákona“,
4. Udržiavať automatizované prostriedky spracúvania osobných údajov v stave neohrozujúcom bezpečnosť týchto osobných údajov,
5. Pre manuálne spracúvanie osobných údajov zaznamenaných na papierových a elektronických médiách vytvárať vhodné organizačné, technické a personálne predpoklady tak, aby nebola ohrozená bezpečnosť týchto osobných údajov,
6. Stanoviť úroveň rizika, pri ktorej budú vyčlenené potrebné zdroje na realizáciu minimálne požadovaných bezpečnostných opatrení.

1.4.2 Vymedzenie okolia informačného systému

1.4.2.1 Ciele „SFP“

Cieľom „SFP“ je ústretovo a včas reagovať na požiadavky v rámci dotácií ako aj činnosti SFP, kde nevyhnutnou súčasťou je identifikácia hráčov prostredníctvom osobných údajov.

1.4.2.2 Štruktúra „SFP“



1.4.2.3 Sídlo „SFP“ a jej geografické charakteristiky

„SFP“ sídli na adrese: Ilýrska 2, 85110 Bratislava - Rusovce.

Všetky priestory „SFP“ sú chráneným priestorom, v ktorom je možné spracúvať osobné údaje.

Vstup do priestorov „SFP“ je zabezpečený uzamykateľnými bezpečnostnými dverami s bezpečnostným zámkom.

„SFP“ nemá žiadne ďalšie prevádzky a objekty.

1.4.2.4 Právne a zmluvné požiadavky pre „SFP“

Zoznam legislatívnych požiadaviek určujúcich rámec pre činnosť „SFP“ a rámec požiadaviek zákonov, na základe ktorých sú osobné údaje spracúvané je uvedený v evidenčných formulároch informačných systémov.

1.4.2.5 Rozhrania výmeny informácií

„SFP“ komunikuje so svojimi členmi pri osobnom kontakte a prostredníctvom mailov.

Spôsob získavania a likvidácie osobných údajov je popísaný v bezpečnostnej smernici.

1.4.2.6 Automatizované prostriedky spracúvania a ich zabezpečenie

„SFP“ zabezpečuje funkčnosť a bezpečnosť automatizovaných prostriedkov spracúvania osobných údajov prostredníctvom poverenej osoby.

„SFP“ využíva na spracúvanie osobných údajov nasledovné prostriedky a aplikuje nasledovné organizačné opatrenia:

Údaje sa spracovávajú v dvoch zariadeniach, ktoré nie sú spoločne zdierané.

Spracovávané údaje vrátane osobných údajov je zakázané ukladať na disky osobných počítačov alebo na súkromné prenosné médiá

„SFP“ nemá vybudovanú firemnú vnútornú sieť.

Na likvidáciu záznamov sa používa skartovacie zariadenie.

1.4.2.7 Manuálne prostriedky spracúvania a ich zabezpečenie

Charakter niektorých procesov si vyžaduje spracúvanie osobných údajov zaznamenaných na papierových médiách. Tieto osobné údaje sa preto spracúvajú manuálne.

Papierové médiá obsahujúce osobné údaje sú v čase mimo pracovnú dobu uložené v šanónoch v chránenom priestore.

Na pracovnom stole smú byť **počas pracovnej doby** uložené len také papierové médiá obsahujúce osobné údaje, ktoré sú používané na plnenie aktuálnych úloh.

1.5 Analýza bezpečnosti informačného systému

Táto analýza bezpečnosti informačných systémov osobných údajov „SFP“ bola spracovaná v zmysle požiadaviek Vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení, zároveň v nej boli primerane aplikované ustanovenia normy STN ISO/IEC 27005.

Pri vyhodnocovaní úrovne rizika bol zvolený nasledovný postup. Ohodnotenie aktíva alebo skupiny aktív. Určenie pravdepodobnosti s akou sa môže vyskytnúť incident alebo udalosť, pri ktorej je využitá zraniteľnosť niektorou z hrozieb. Stanovenie úrovne rizika podľa stanovenej stupnice.

a) Ohodnotenie aktív

Hodnota aktíva:

Veľmi nízka - málo významné aktívum, ktorého strata spôsobí zanedbateľné dopady a ktoré je veľmi jednoducho a rýchlo nahraditeľné za cenu zanedbateľných nákladov vo veľmi krátkej dobe.

Nízka - hodnota aktíva, ktorého strata by mala pre „SFP“ ľahko zvládnuteľný dopad a ktorého nahradenie je možné za cenu bežných nákladov v požadovanej dobe.

Stredná - hodnota aktíva, ktorého strata by mala pre „SFP“ akceptovateľný dopad a ktorého nahradenie je možné za cenu ešte akceptovateľných nákladov v ešte akceptovateľnej dobe.

Vysoká - veľká hodnota aktíva, ktorého strata by mala pre „SFP“ veľké dopady a ktorého nahradenie je veľmi obtiažne, za cenu veľmi veľkých nákladov po veľmi dlhej dobe.

Veľmi vysoká - veľmi veľká hodnota aktíva, ktorého strata by mala pre „SFP“ existenčné dopady a ktorého obnovenie je takmer nemožné alebo je možné len za cenu neakceptovateľných nákladov investície a po neakceptovateľnej dlhej dobe.

Určenie pravdepodobnosti výskytu incidentu alebo udalosti

Pravdepodobnosť udalosti:

Veľmi nízka - predpokladá sa, že mimoriadna udalosť sa v priemere nevyskytne častejšie ako raz za 10 rokov

Nízka – predpokladá sa, že mimoriadna udalosť sa vyskytne v priemere raz za 10 rokov.

Stredná - predpokladá sa, že mimoriadna udalosť sa nevyskytne nikdy.

Vysoká – predpokladá sa, že mimoriadna udalosť sa nevyskytne nikdy.

Veľmi vysoká - predpokladá sa, že mimoriadna udalosť sa nevyskytne nikdy.

b) Stanovenie úrovne rizika:

		Pravdepodobnosť incidentu alebo udalosti (využitia zraniteľnosti príslušnou hrozbou)				
		veľmi nízka	nízka	stredná	vysoká	veľmi vysoká
aktíva	veľmi nízka	riziko nízke	riziko nízke	žiadne	žiadne	žiadne
	nízka	riziko nízke	riziko nízke	žiadne	žiadne	žiadne

	stredná	žiadne	žiadne	žiadne	žiadne	žiadne
	vysoká	žiadne	žiadne	žiadne	žiadne	žiadne
	veľmi vysoká	žiadne	žiadne	žiadne	žiadne	žiadne

Riziká sa ošetrí bezpečnostnými opatreniami v závislosti od úrovne bezpečnostného rizika a v závislosti od zdrojov vyčlenených na tento účel. Riziká sa ošetrujú v poradí: vysoké, stredné a nízke.

Nízke riziko – takáto úroveň rizika je akceptovateľná. Nie je nutné ho ošetriť bezpečnostnými opatreniami.

1.5.1 Identifikácia aktív a vlastníkov

Primárnymi aktívami „SFP“, ktoré majú priamy súvis s ochranou osobných údajov sú nasledovné aktíva.

a) Získavanie dotácií:

- preberanie a spracúvanie osobných údajov registrovaných hráčov,
- odovzdávanie spracovaných osobných údajov poskytovateľom dotácií,
- zálohovanie a archivovanie elektronickej formy osobných údajov,

b) informácie:

- osobné údaje zaznamenané na papierových médiách,
- osobné údaje v elektronickej forme uložené na záznamových médiách,

Zoznam konkrétnych osobných údajov spracúvaných v jednotlivých informačných systémoch osobných údajov je uvedený v príslušných evidenčných formulároch týchto informačných systémov.

Vlastník: osoba, ktorej agenda obsahuje osobné údaje.

Podpornými aktívami „SFP“ sú

c) hardvér

- prenosné dátové médi
- tlačiareň

Vlastník: osoba, ktorej je hardvér pridelený

d) softvér

- operačný systém windows
- MS OFIS

Vlastník: osoba, ktorej je pridelený

e) Sieť

- Verejná telefónna sieť
- Verejne prístupná Wi-Fi

Vlastník: SFP

f) osoby

- osoby zúčastňujúce sa hlavných procesov, spojených so získavaním osobných údajov.

Vlastník: SFP

g) priestory „SFP“

Priestory SFP.

1.5.2 Analýza rizík

1.5.2.1 Aktívum: Procesy a informácie (osobné údaje)

Hodnota aktíva: Veľmi nízka

a) Hrozby:

- neoprávnené získanie, zaznamenávanie, prehliadanie, uchovávanie osobných údajov,
- neoprávnené poskytovanie, sprístupňovanie, zverejňovanie a prenos osobných údajov,
- nesplnenie legislatívnych podmienok pri získavaní osobných údajov,
- zmeny legislatívy týkajúcej sa ochrany osobných údajov,
- neoprávnené oboznámenie sa s osobnými údajmi

Zraniteľnosti:

- poučenie oprávnených osôb sa neuskutočnilo, bolo len formálne alebo v nedostatočnom rozsahu,
- nedostatky v kontrolných procedúrach,
- chyby zamestnancov,
- zodpovednosť za dodržiavanie legislatívy v oblasti ochrany osobných údajov nie je stanovená,
- neznalosť požiadaviek legislatívy,
- sledovanie zmien legislatívy nemá vlastníka.

Pravdepodobnosť udalosti, incidentu: nízka

Dopady:

- sankcie za nedodržanie legislatívy,

- sťažnosti na neoprávnené získanie osobných údajov,

Riziko: Nízke

Možnosť minimalizovať riziko:

- ustanoviť „Poverenú osobu/y“ ako osoby zodpovednej za dodržiavanie legislatívy v oblasti ochrany osobných údajov najmä za:
 - o sledovanie zmien v tejto oblasti,
 - o poučovanie oprávnených osôb,
 - o kontrolu dodržiavania legislatívy pre proces získavania osobných údajov ale aj ďalšieho ich spracúvania,
 - o zaobstaranie alebo uskutočnenie aktualizácie analýzy bezpečnosti.
- vytvoriť možnosť získať právne poradenstvo pre osobu zodpovednú za dodržiavanie legislatívy v oblasti ochrany osobných údajov,

1.5.2.2 Hardvér

Hodnota aktíva: nízka

b) Hrozby:

- zlyhanie hardvéru,
- chyby a poruchy spôsobené neodborným zásahom,

Zraniteľnosti:

- absencia alebo nedostatočná podpora dodávateľov,
- nedostatočná alebo žiadna údržba,
- absencia kontrolných mechanizmov,
- zastaralý a dlho prevádzkovaný HW,
- neodborný alebo málo skúsený personál,
- nepozornosť,

Pravdepodobnosť udalosti, incidentu: stredná

Dopady:

- strata dostupnosti osobných údajov,

Riziko: nízke

Možnosť minimalizovať riziko:

- vyčleniť zdroje na :
 - o pravidelnú kontrolu prevádzkovaného hardvéru,

- identifikáciu a pravidelnú obmenu hardvéru, ktorý je dlhodobo prevádzkovaný,

1.5.2.3 Siete

Hodnota aktíva: nízka

c) Hrozby:

- odchytenie osobných údajov počas prenosu,
- neoprávnený vzdialený prístup k osobným údajom,

Zraniteľnosti:

- absencia technológií zamedzujúcich neoprávnené vzdialené pripojenie do vnútornej siete,
- zdieľanie prístupových údajov,
- absencia regulácie prístupových práv,
- absencia politiky hesiel,
- nedostatočná alebo žiadna údržba,
- neoprávnená inštalácia softvéru z neoverených zdrojov,

Pravdepodobnosť udalosti, incidentu: nízka

Dopady:

- strata dôvernosti a integrity osobných údajov,

Riziko: nízke

Možnosť minimalizovať riziko:

- zavedenie technických opatrení, ktoré zamedzia neoprávnené vzdialené pripojenie do vnútornej siete,

1.5.2.4 Osoby

Hodnota aktíva: nízka

d) Hrozby:

- sociálne inžinierstvo, neoprávnené poskytnutie prihlasovacích údajov,
- zverejnenie alebo poskytnutie osobných údajov neoprávneným osobám,

Zraniteľnosti:

- neodborný alebo málo skúsený personál, nepozornosť,

Pravdepodobnosť udalosti, incidentu: nízka

Dopady:

- strata dôvernosti a integrity osobných údajov,

Riziko: nízke

Možnosť minimalizovať riziko:

- poučiť osoby o spôsoboch a praktikách sociálneho inžinierstva, s cieľom získať prihlasovacie údaje,

1.5.2.5 Priestory

Hodnota aktíva: nízka

e) Hrozby:

- vstup neoprávnených osôb do chránených priestorov,

Zraniteľnosti:

- nepozornosť osôb, ktoré majú oprávnenie umožniť vstupu cudzích osôb do chránených priestorov,

Pravdepodobnosť udalosti, incidentu: nízka

Dopady:

- strata dôvernosti, integrity a dostupnosti osobných údajov,

Riziko: nízke

Možnosť minimalizovať riziko:

- poučenie osôb o sprevádzaní cudzích osôb a osôb, ktoré nie sú oprávnenými osobami v chránených priestoroch.

1.5.3 Vymedzenie hraníc určujúcich množinu zostatkových rizík

Bezpečnostnými opatreniami nie sú alebo sú len čiastočne pokryté nasledovné udalosti:

a) Zaslanie médií s osobnými údajmi neoprávnenému príjemcovi.

Dopad: strata dôvernosti osobných údajov a možnosť sťažnosti dotknutých osôb s následkom udelenia pokuty v zmysle „Zákona“.

b) Chybné zaznamenanie osobných údajov do automatizovaných prostriedkov spracúvania.

Dopad: strata dôvery spolupracujúcich subjektov, nedodržanie legislatívy.

c) Strata/krádež záznamov z pracovných staníc zamestnancov.

d) - zlyhanie softvéru,

e) - zlyhanie softvéru určeného na spracovanie osobných údajov,

f) - chyby a poruchy spôsobené neodborným zásahom,

- g) - zlyhanie vytvorenia zálohy elektronickej formy osobných údajov,
- h) Odchytenie osobných údajov počas prenosu.

Dopad: strata dôveryhodnosti, integrity a dostupnosti osobných údajov a možnosť sťažnosti dotknutých osôb s následkom udelenia pokuty v zmysle „Zákona“.

- i) Preťaženie siete, spomalenie alebo zamedzenie komunikácie.

Dopad: strata dostupnosti osobných údajov

- j) Neoprávnené oboznámenie sa s osobnými údajmi z nepotrebných/vyhodených záznamových médií (papier, elektronické záznamové médiá).
- k) Neoprávnený export alebo kopírovanie osobných údajov.

Dopad: strata dôveryhodnosti osobných údajov a pri zverejnení prípadu strata dôvery spolupracujúcich subjektov.

1.6 Bezpečnostná smernica

Táto bezpečnostná smernica je spracovaná v zmysle ustanovení zákona č. 122/2013 Z.z. o ochrane osobných údajov (ďalej len „Zákon“) a je súčasťou bezpečnostného projektu SFP (ďalej len „SFP“).

Stanovuje pravidlá „SFP“ pri spracúvaní a zabezpečovaní ochrany osobných údajov. Táto smernica sa týka informačných systémov osobných údajov uvedených v úvode bezpečnostného projektu.

Smernica záväzne stanovuje povinnosti pre „SFP“, všetky oprávnené osoby, ktoré spracúvajú osobné údaje a prípadne aj pre zodpovednú osobu, ak je v zmysle zákona poverená.

1.6.1 Popis bezpečnostných opatrení

Všeobecné bezpečnostné opatrenia

1. Prezident „SFP“ musí pri vytváraní zmluvných vzťahov posudzovať zapracovanie a do novo uzatváraných zmluvných vzťahov v prípade potreby zapracovávať ustanovenia zabezpečujúce ochranu osobných údajov a ochrany dôverných informácií.
2. Osobné údaje môžu spracúvať len oprávnené osoby až po uskutočnení poučenia a podpísaní písomného „Záznamu o poučení“.
3. O zaradení medzi oprávnené osoby a rozsahu jeho oprávnení rozhoduje prezident „SFP“.

Organizačné opatrenia

4. Spracúvanie osobných údajov je povolené len pre oprávnené osoby.

5. Prístup cudzích alebo neoprávnených osôb do priestorov, kde sú umiestnené prostriedky automatizovaného spracúvania osobných údajov alebo médiá obsahujúce osobné údaje musí byť kontrolovaný a umožnený len v sprievode oprávnených „SFP“.
6. Záznamové médiá obsahujúce osobné údaje v papierovej alebo elektronickej forme musia byť odkladané, skladované alebo archivované len v chránených priestoroch.
7. Osobné údaje v písomnej forme uložené na papierových médiách sa môžu prepravovať mimo chránených priestorov len v zalepených obálkach. Tieto obálky musia byť pod neustálou kontrolou oprávneného zamestnanca, ktorý prepravu zabezpečuje.
8. Prepravu osobných údajov v písomnej forme uložených na papierových médiách je možné zabezpečovať formou doporučenej zásielky poštou alebo kuriérom.
9. Zmluvy s externými subjektmi, na základe ktorých sa uskutočňuje údržba automatizovaných prostriedkov spracúvania musia obsahovať dohody o zachovaní dôvernosti.
10. Príčiny incidentov ohrozujúcich bezpečnosť osobných údajov musia byť náležite prešetrené a musia byť prijaté príslušné opatrenia.
11. Musia byť stanovené postupy a spôsob likvidácie osobných údajov po skončení účelu ich spracúvania a musia byť určené osoby zodpovedné za túto likvidáciu.

Personálne opatrenia

12. Spracúvať osobné údaje môžu len osoby, ktoré boli poučení v zmysle §21 „Zákona“ a podpísali o poučení záznam.
13. Za bezproblémovú prevádzku automatizovaných prostriedkov musí byť poverená jedna alebo viacero osôb v zmysle „Zákona“.

Technické opatrenia

14. Automatizované prostriedky spracúvania osobných údajov musia mať:
 - a. zriadené potrebné počty prihlasovacích účtov,
 - b. nastavené politiky riadenia hesiel,
 - c. implementovanú detekciu a ochranu proti škodlivému kódu,
 - d. synchronizovaný systémový čas,
 - e. nastavené uzamknutie pri dlhšej neaktivite,
 - f. zamedzený prístup do OS a do BIOS-u
15. Dôležité udalosti spracúvania osobných údajov automatizovanými prostriedkami ako aj chyby a poruchy musia byť zaznamenávané, záznamy zálohované a bezpečne ukladané.
16. Osobné údaje v elektronickej forme musia byť v pravidelných intervaloch zálohované a čitateľnosť záloh pravidelne kontrolovaná.

1.6.2 Rozsah oprávnení

Spracúvať osobné údaje môže len oprávnená osoba.

Oprávnená osoba môže spracúvať osobné údaje len na taký účel a len na takom právnom základe, ktorý je uvedený v príslušnom evidenčnom formulári informačného systému osobných údajov.

Oprávnená osoba môže za dodržania podmienok „Zákona“ a tejto smernice vykonávať s osobnými údajmi spracúvanými v jednotlivých informačných systémoch „SFP“ nasledovné operácie:

- a) získavanie,
- b) zhromažďovanie,
- c) zaznamenávanie,
- d) usporadúvanie,
- e) prepracúvanie alebo zmena,
- f) vyhľadávanie,
- g) prehliadanie,
- h) preskupovanie,
- i) kombinovanie,
- j) premiestňovanie,
- k) využívanie,
- l) uchovávanie,
- m) blokovanie,
- n) likvidácia,

Oprávnená osoba môže nasledovné spracovateľské operácie

- o) poskytovanie,
- p) sprístupňovanie,
- q) zverejňovanie
- r) prenos,

uskutočňovať len v súlade s podmienkami, ktoré sú uvedené v príslušných evidenčných formulároch informačného systému osobných údajov.

1.6.3 Rozsah zodpovednosti

1.6.3.1 Vedenie „SFP“

Prezident „SFP“ zodpovedá za dodržiavanie ustanovení „Zákona“.

1.6.3.2 Zamestnanci „SFP“ – oprávnené osoby

Oprávnené osoby zodpovedajú za:

- a) ochranu osobných údajov pred oboznámením sa nepovolanými osobami,
- b) dodržiavanie ustanovení tejto smernice a ustanovení „Zákona“,
- c) dôsledné zničenie nepotrebných médií, na ktorých sú zaznamenané osobné údaje,

Oprávnené osoby sú povinné:

- a) zachovávať mlčanlivosť o osobných údajoch, s ktorými prišli do styku,
- b) v prípade úniku alebo podozrenia z úniku osobných údajov, oznámiť túto skutočnosť zodpovednej osobe,

Je zakázané:

- c) osobné údaje v elektronickej alebo papierovej forme:
 - a. bez povolenia kopírovať,
 - b. bez povolenia zaznamenávať.

1.6.3.3 „Poverená osoba“

Zabezpečuje dohľad nad plnením požiadaviek „Zákona“ v obdobnom rozsahu povinností, ktoré vyplývajú zo „Zákona“ pre zodpovednú osobu smerom k Prevádzkovateľovi a zodpovedá za dohľad nad plnením ustanovení tejto smernice.

Sleduje zmeny v legislatíve týkajúcej sa ochrany osobných údajov a zaobstaráva alebo uskutočňuje aktualizáciu bezpečnostného projektu.

Vedie agendu vyplývajúcu z požiadaviek „Zákona“.

Riadi oboznamovanie sa oprávnených osôb s ustanoveniami „Zákona“ a ich poučenie.

Vykonáva alebo riadi vykonávanie kontrolnej činnosti pre oblasť ochrany osobných údajov a navrhuje opatrenia na odstránenie zistených nedostatkov.

1.6.3.4 Zamestnanci alebo iné osoby spolupracujúcich subjektov

Zamestnanci spolupracujúcich subjektov:

- a) sú povinný sa v primeranom rozsahu oboznámiť s ustanoveniami tejto smernice,
- b) musia pred začatím spracúvania osobných údajov, ktorých prevádzkovateľom je „SFP“ byť primerane poučení a musia podpísať „Záznam o poučení“.

1.6.4 Spôsob, forma a periodicita kontrolnej činnosti

Poverená osoba vykonáva pri nahlásených a/alebo iným spôsobom zistených porušení ochrany osobných údajov alebo minimálne 1 x ročne kontrolu zameranú na dodržiavanie ustanovení tejto smernice a „Zákona“.

Kontrolnú činnosť môže vykonať aj iný zamestnanec, ktorého na tento úkon poverí vedenie „SFP“.

1.6.5 Postupy pri haváriách, poruchách a mimoriadnych situáciách

- a) Havária alebo porucha automatizovaných prostriedkov spracúvania osobných údajov (poruchy hardvéru, softvéru) a poruchy siete.

Poruchu nahlási prezidentovi „SFP“ a zabezpečí opravu.

- b) Výpadok dodávky elektrického prúdu

Ukončí prácu, korektne vypne všetky aplikácie.

1.6.6 Preventívne opatrenia na zníženie rizika vzniku mimoriadnych udalostí

- a) pravidelná kontrola technického stavu automatizovaných prostriedkov spracúvania osobných údajov, záložných zdrojov elektrickej energie,
- b) ukladanie médií, ktoré obsahujú osobné údaje do uzamykateľných zásuviek,
- c) uskutočňovanie pravidelných školení oprávnených osôb a ich oboznamovanie so zmenami v „Zákone“ a bezpečnostnom projekte.

PRÍLOHA č. 1 EVIDENCIA INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

podľa § 43 ods. 1 zákona č. 122/2013 Z. z.

o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

I. NÁZOV INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

--

II. ÚDAJE O PREVÁDZKOVATEĽOVI

Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa	
Počet oprávnených osôb	

III. ÚDAJE O INFORMAČNOM SYSTÉME OSOBNÝCH ÚDAJOV

Účel spracúvania osobných údajov	
Právny základ spracúvania osobných údajov	
Okruh dotknutých osôb	
Zoznam osobných údajov (alebo rozsah)	
Označenie bezpečnostných opatrení	

IV. SPRACOVATELSKÉ OPERÁCIE S OSOBNÝMI ÚDAJMI	
Poskytovanie osobných údajov	
Tretie strany (prípadne okruh tr. strán)	Právny základ
Ministerstvo vnútra Slovenskej republiky	
iný oprávnený subjekt	
Sprístupňovanie osobných údajov	
Okruh príjemcov	Právny základ
Zverejňovanie osobných údajov	
Spôsob zverejnenia	Právny základ
Cezhraničný prenos osobných údajov	
Tretia krajina	Právny základ

V. ZAČIATOK SPRACÚVANIA OSOBNÝCH ÚDAJOV

Odtlačok pečiatky prevádzkovateľa

Dátum, meno a podpis

štatutárneho orgánu prevádzkovateľa