Výkonný výbor Slovenského futbalového zväzu podľa článku 8 ods. 3 písm. e) a článku 52 písm. a) stanov Slovenského futbalového zväzu (ďalej len "SFZ") a na základe § 22 ods. 17 zákona č. 1/2014 Z. z. o organizovaní verejných športových podujatí a o zmene a doplnení niektorých zákonov (ďalej len "zákon") schválil túto smernicu:

I. Časť - Úvodné ustanovenia

Čl. 1
Predmet úpravy

Táto smernica upravuje podrobnosti o vytvorení, spravovaní a prevádzkovaní informačného systému o bezpečnosti na športových podujatiach (ďalej len "informačný systém"), vymedzenie a rozsah prístupových práv a rolí oprávnených subjektov, pravidlá spracúvania a sprístupňovania údajov v informačnom systéme, povinnosti správcu informačného systému, prevádzkovateľa informačného systému a ďalších oprávnených subjektov, podrobnosti o evidenciách podľa § 22 ods. 2, 6 a 7 zákona a ďalšie pravidlá súvisiace s prevádzkou a používaním informačného systému.

Čl. 2
Vymedzenie pojmov

Na účely tejto smernice sa rozumie

a) **verejným športovým podujatím** (ďalej len "podujatie) podujatie podľa § 2 písm. a) až d) zákona,
b) **informačným systémom** funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov umožňujúcich vykonávanie automatizovaných operácií s údajmi v informačnom systéme; informačný systém tvorí súbor údajov, ktoré sú spracúvané automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania v evidenciách podľa § 22 ods. 2, 6 a 7 zákona,
c) **informačnou činnosťou** získavanie, zhromažďovanie, spracúvanie, sprístupňovanie, poskytovanie, prenos, ukladanie, archivácia a likvidácia údajov,
d) **správcom informačného systému** SFZ, ktorý zodpovedá za vytváranie, správu, prevádzku, funkčnosť, údržbu a inováciu informačného systému,
e) **prevádzkovateľom informačného systému** SFZ, Slovenský zväz ľadového hokeja alebo iný športový zväz,
f) **oprávneným subjektom** subjekt, ktorý má oprávnenie používať informačný systém a vykonávať role v zákonom ustanovenom rozsahu,
g) **oprávnenou osobou** fyzická osoba, ktorej bol pridelený identifikátor prístupu do informačného systému a ktorú oprávnený subjekt poveril vykonávaním jeho rolí v informačnom systéme,
h) **identifikátorom prístupu** používateľské meno identifikujúce oprávnenú osobu v informačnom systéme a heslo viažuce sa k tomuto používateľskému menu,
i) **prístupovým právom** právo používať informačný systém a v rozsahu pridelenej role

pristupovať k údajom v informačnom systéme a vykonávať informačné činnosti v informačnom systéme,

j) **autentifikáciou** proces overovania prístupového práva, umožňuje správne pridelenie prístupových práv prihlásenej oprávnenej osobe s automatizovaným pridelením príslušných rolí,

k) **rolou** oprávnenie vykonávať určenú skupinu operácií v informačnom systéme; rola má svoje pomenovanie, ktoré je prepojené s prístupovým právom oprávneného subjektu,

l) **dotknutou osobou** fyzická osoba, ktorej sa údaje v informačnom systéme týkajú,

m) **zodpovednou osobou** osoba poverená výkonom dohľadu, ktorú prevádzkovateľ informačného systému písomne poveril dozerať na ochranu osobných údajov spracúvaných v informačnom systéme,

n) **spracúvaním údajov** vykonávanie operácií alebo súboru operácií s údajmi v informačnom systéme, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie,

o) **poskytovaním údajov** odovzdávanie údajov fyzickej osobe alebo právnickej osobe, ktorá ich ďalej spracúva,

p) **sprístupňovaním údajov** oznámenie údajov v informačnom systéme alebo umožnenie prístupu k nim právnickej osobe alebo fyzickej osobe, ktorá ich ďalej nespracúva,

q) **likvidáciou údajov** zrušenie údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich údaje nedali reprodukovať,

r) **identifikátorom fyzickej osoby** - identifikačné číslo, ktoré je fyzickej osobe pridelené pri jej evidencii v informačnom systéme,

s) **webovou aplikáciou** - verejne on-line dostupná aplikácia na internete sprístupňovaná prostredníctvom webového prehliadača a využívajúca protokol HTTPs alebo iný protokol na zabezpečenú komunikáciu.

Čl. 3
Špecifikácia informačného systému

(1) Informačný systém je webová aplikácia, ktorá po autentifikácii prístupového práva prostredníctvom identifikátora prístupu umožňuje oprávnenej osobe vykonávať svoju rolu v informačnom systéme v rozsahu pridelených prístupových práv.
(2) Technická špecifikácia prostredia informačného systému je uvedená v **prílohe č. 1** smernice.

Čl. 4
Role oprávnených osôb

(1) **Oprávnená osoba správcu informačného systému a oprávnená osoba prevádzkovateľa informačného systému** majú úplný rozsah prístupových práv do informačného systému, ktoré zahŕňajú spracúvanie údajov, poskytovanie údajov, sprístupňovanie údajov, zverejňovanie údajov, zálohovanie údajov, archiváciu údajov a likvidáciu

údajov. Prístupové práva správcu informačného systému a prevádzkovateľa informačného systému spočívajú v zisťovaní obsahu údajov, vytváraní nových údajov, zmene údajov, odstránení údajov a vytváraní výstupov v súlade so zákonom a touto smernicou.

(2) **Oprávnená osoba správcu informačného systému** spracúva údaje o fyzických osobách, ktorým bol uložený trest zákazu účasti na verejných podujatiach alebo obmedzujúce opatrenie obdobnej povahy v trestnom konaní a údaje o fyzických osobách, ktoré boli odsúdené za trestné činy spáchané v súvislosti s účasťou na verejnom podujatí, alebo ktorých trestné stíhanie za takéto trestné činy boli podmienečne zastavené alebo skončené zmierom. Tieto údaje spracúva správca informačného systému na základe rozhodnutí a informácií, ktoré sú mu zasielané orgánmi činnými v trestnom konaní a súdom.

(3) **Oprávnená osoba správcu informačného systému** okrem údajov podľa odseku 2 spracúva a aktualizuje údaje v module odbornej prípravy uchádzačov o získanie alebo overenie odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra podujatia (ďalej len "bezpečnostný manažér") a usporiadateľa.

(4) **Oprávnená osoba Policajného zboru** spracúva v informačnom systéme údaje o fyzických osobách,

a) ktoré boli postihnuté za priestupky podľa § 25 ods. 1, 3 až 6 zákona a priestupky diváckeho násilia podľa § 26 zákona,
b) ktorým bolo uložené obmedzujúce opatrenie spočívajúce v zákaze účasti na verejných podujatiach,
c) ktoré majú príslušným orgánom verejnej moci uložené predbežné opatrenie podľa § 27 ods. 2 zákona alebo primerané obmedzenie spočívajúce v zákaze účasti na podujatiach podľa osobitného predpisu,
d) ktoré sú štátnymi príslušníkmi iného štátu a bolo im uložené administratívne vyhostenie a zákaz vstupu na územie Slovenskej republiky za protiprávne konanie v súvislosti s účasťou na podujatí, ktorého sa dopustili na území Slovenskej republiky,
e) ktoré boli postihnuté alebo potrestané za protiprávne konanie v súvislosti s účasťou na podujatí v cudzine,
f) ktoré sa dopustili konania zakladajúceho podozrenie z priestupku diváckeho násilia alebo trestného činu spáchaného v súvislosti s účasťou na podujatí a ich totožnosť nebola zistená.

(5) **Oprávnená osoba Policajného zboru** spracúva v informačnom systéme okrem údajov podľa odseku 4 aj

a) údaje o priestupkoch podľa § 25 ods. 2 zákona a § 26 ods. 1 a 2 zákona, uložených sankciách a opatreniach, ak ide o hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa,
b) evidenciu textov a vyhlásení, zástav, odznakov, hesiel alebo symbolov skupín alebo hnutí a ich programov alebo ideológií, ktoré smerujú k potláčaniu základných ľudských práv a slobôd alebo obhajujúcich, podporujúcich alebo podnecujúcich nenávisť, násilie alebo neodôvodnene odlišné zaobchádzanie voči skupine osôb alebo jednotlivcovi pre ich príslušnosť k niektorej rase, národu, národnosti, farbe pleti, etnickej skupine, pôvodu rodu alebo pre ich náboženské vyznanie (ďalej len "evidencia extrémistických symbolov").

(6) **Oprávnená osoba národného športového zväzu** spracúva v informačnom systéme

údaje týkajúce sa

a) hlavného usporiadateľa a bezpečnostného manažéra v evidencii hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov v rozsahu podľa § 22 ods. 6 písm. a) až k) zákona,
b) fyzických osôb, ktoré boli postihnuté v disciplinárnom konaní za agresívne prejavy v súvislosti s účasťou na podujatí.

(7) **Oprávnená osoba športového zväzu** spracúva v informačnom systéme údaje týkajúce sa

a) usporiadateľov v evidencii hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov v rozsahu podľa § 22 ods. 6 písm. a) až k) zákona,
b) fyzických osôb, ktoré boli postihnuté v disciplinárnom konaní za agresívne prejavy v súvislosti s účasťou na podujatí.

(8) **Oprávnená osoba športového klubu** spracúva v informačnom systéme údaje o usporiadateľoch v evidencii hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov v rozsahu podľa § 22 ods. 6 písm. a) až k) zákona.

(9) **Oprávnená osoba organizátora** podujatia spracúva v informačnom systéme

a) dohody podľa § 8 ods. 3 a § 18 ods. 4 zákona,
b) údaje týkajúce sa fyzických osôb, ktoré
    1. porušili organizačný poriadok podujatia alebo návštevný poriadok podujatia,
    2. sa dopustili konania zakladajúceho podozrenie z priestupku diváckeho násilia alebo trestného činu spáchaného v súvislosti s účasťou na podujatí a ich totožnosť nebola zistená,

(10) **Oprávnená osoba organizátora podujatia** vyhotovuje výpis z evidencií informačného systému na účely plnenia povinnosti členov usporiadateľskej služby podľa § 14 ods. 2 písm. e) zákona a správu o podujatí s osobitným režimom (ďalej len “správa o podujatí”).

Čl. 5

(1) Oprávnenou osobou národného športového zväzu, športového zväzu, športového klubu a organizátora podujatia je bezpečnostný manažér. Ak národný športový zväz, športový zväz, športový klub alebo organizátor podujatia nemá bezpečnostného manažéra, oprávnenou osobou je hlavný usporiadateľ alebo iná osobitne poverená osoba.

(2) Iné oprávnené subjekty, najmä obecná polícia, Národné futbalové informačné stredisko, osoba, ktorú obec poverila vykonávať v jej mene dozor, osoba delegovaná národným športovým zväzom alebo športovým zväzom vykonávajú prístupové práva do informačného systému prostredníctvom oprávnenej osoby v rozsahu nevyhnutnom na plnenie ich povinností a úloh ustanovených právnymi predpismi.

Čl. 6

Rozsah prístupových práv a zodpovedajúcich pridelených rolí oprávnených osôb podľa článkov 4 a 5 je uvedený v **prílohe č. 2**.

Čl. 7
Pridelenie prístupového práva a identifikátora prístupu

(1) Na vytvorenie prístupu a pridelenie identifikátora prístupu do informačného systému má právo

len oprávnená osoba podľa článkov 4 a 5, ktorej to vyplýva z jej role v informačnom systéme.
(2) Prístup do informačného systému môže byť umožnený aj iným právnickým osobám alebo fyzickým osobám, ak je to nevyhnutné na plnenie ich povinností a úloh ustanovených právnymi predpismi, alebo na základe žiadosti fyzickej osoby, ak si to vyžaduje jej činnosť vo vzťahu k podujatiu.
(3) Na povolenie prístupu do informačného systému slúži registračný formulár "**Schválenie prístupu do informačného systému**", ktorého vzor je uvedený v **prílohe č. 3**. Riadne vyplnený a podpísaný registračný formulár doručí žiadateľ o pridelenie prístupu správcovi informačného systému. Registračný formulár za žiadateľa podáva ním poverená oprávnená osoba.
(4) Oprávnená osoba správcu informačného systému na základe doručeného registračného formulára prideľuje pre žiadateľa príslušné role a úroveň prístupových práv v informačnom systéme, zabezpečí zriadenie prístupových práv a pridelí oprávnenej osobe identifikátor prístupu pozostávajúci z používateľského mena a hesla.
(5) Používateľské meno a heslo je v informačnom systéme neopakovateľné. Heslo obsahuje najmenej 8 alfanumerických znakov v kombinácii, najmenej jedno veľké písmeno, jedno malé písmeno a jedno číslo.
(6) Oprávnená osoba správcu informačného systému je povinná viesť prehľad o všetkých oprávnených osobách v informačnom systéme, ich prístupových právach vrátane ich rozsahu a dĺžky platnosti a zodpovedá za archiváciu všetkých schválených registračných formulárov.

Čl. 8
Platnosť prístupového práva

Doba platnosti prístupových práv závisí od rozsahu prístupových práv a rolí, ktoré oprávnená osoba vykonáva. Prístupové právo bezpečnostného manažéra a hlavného usporiadateľa sa prideľuje na dobu určitú a končí sa dňom uplynutia obdobia platnosti osvedčenia bezpečnostného manažéra alebo osvedčenia hlavného usporiadateľa. Ak bezpečnostný manažér a hlavný usporiadateľ úspešne absolvuje opakované overenie odbornej spôsobilosti, jeho prístupové práva sa predlžujú podľa platnosti osvedčenia bezpečnostného manažéra alebo osvedčenia hlavného usporiadateľa.

Čl. 9
Zrušenie prístupových práv

(1) Zrušenie prístupového práva zabezpečuje oprávnená osoba správcu informačného systému na základe
a) oznámenia oprávnenej osoby z dôvodu skončenia potreby prístupu,
b) uplynutia doby platnosti prístupových práv,
c) oznámenia skutočnosti preukazujúcej stratu spôsobilosti byť oprávnenou osobou,
d) narušenia alebo podozrenie z narušenia bezpečnosti informačného systému.

(2) Oprávnená osoba správcu informačného systému zabezpečí zrušenie všetkých prístupových práv bezodkladne.
(3) Ak oprávnená osoba správcu informačného systému zistí narušenie alebo podozrenie z narušenia bezpečnosti informačného systému, zruší príslušné prístupové práva bezodkladne a o tejto skutočnosti informuje správcu informačného systému.

(4) Oprávnená osoba správcu informačného systému zodpovedá za zrušenie všetkých prístupových práv, ktoré boli oprávnenej osobe pridelené a za vedenie evidencie zrušení prístupových práv.

Čl. 10
Záznamy v systéme prístupových práv

(1) Na dosiahnutie kontrolovaného a evidovaného prístupu k údajom v informačnom systéme zabezpečuje systém prístupových práv vytváranie auditných záznamov o týchto aktivitách

a) autentifikované prístupy do informačného systému zaznamenaním dátumu, času, identifikátora oprávnenej osoby a typu prístupu,
b) pokusy o neoprávnený prístup k údajom v informačnom systéme, zaznamenaním dátumu a času,
c) zmena konfigurácie informačného systému,
d) použitie systémových nástrojov a aplikácií,
e) aktivácia a deaktivácia ochranných systémov,
f) narušenie pravidiel prístupu,
g) zmeny alebo pokusy o zmenu bezpečnostných nastavení informačného systému,
h) informačné činnosti vykonané oprávnenou osobou v rámci každého autentifikovaného vstupu jednotlivo,
i) vytváranie výpisov z informačného systému vo forme elektronického výstupu a tlačovej zostavy.

(2) Systém prístupových práv podľa odseku 1 je dostupný výlučne oprávnenej osobe správcu informačného systému. Žiadna iná oprávnená osoba nemá prístupové práva, ktoré umožňujú zmenu alebo vymazanie auditných záznamov.
(3) Rozsah, periodicitu sledovania auditných záznamov a periodicitu ich mazania navrhuje oprávnená osoba správcu informačného systému.
(4) Auditné záznamy musia byť uchovávané najmenej po dobu 12 mesiacov.

II. Časť - Členenie a obsah informačného systému

Čl. 11
Časti informačného systému

Vnútorná štruktúra informačného systému pozostáva z týchto častí

a) evidencia fyzických osôb podľa § 22 ods. 2 zákona (ďalej len “evidencia rizikových účastníkov podujatia”) a príslušné registre,
b) evidencia hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov a príslušné registre,
c) evidencia dohôd o spolupráci organizátora podujatia s Policajným zborom alebo obecnou políciou pri zabezpečovaní činností usporiadateľskej služby (ďalej len “evidencia dohôd”) a príslušné registre,
d) evidencia extrémistických symbolov a príslušné oddiely,
e) modul odbornej prípravy uchádzačov o získanie alebo overenie odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa (ďalej len “modul

odbornej prípravy"),
f) zoznam aktívnych zákazov,
g) zoznam neaktívnych/minulých zákazov.

Čl. 12
Evidencia rizikových účastníkov podujatia

(1) V evidencii rizikových účastníkov podujatia podľa § 22 ods. 2 zákona sú vedené tieto registre:
a) **register TK** obsahujúci
   i) evidenciu fyzických osôb, ktorým bol uložený trest zákazu účasti na verejných podujatiach alebo obmedzenie obdobnej povahy v trestnom konaní; fyzické osoby, ktoré vykonávajú trest zákazu účasti na verejných podujatiach alebo sa na nich vzťahuje obmedzenie obdobnej povahy, sú evidované osobitne v **zozname zákazov** podľa druhov športu, súťaží, klubov a štadiónov, na ktoré sa tieto zákazy vzťahujú,
   ii) evidenciu fyzických osôb, ktoré boli odsúdené za trestné činy spáchané v súvislosti s účasťou na verejnom podujatí alebo ktorých trestné stíhanie za takéto trestné činy bolo podmienečne zastavené alebo skončené zmierom,
b) **register PK** obsahujúci
   i) evidenciu fyzických osôb, ktoré boli postihnuté za priestupky podľa § 25 ods. 1, 3 až 6 zákona a priestupky diváckeho násilia podľa § 26 zákona,
   ii) evidenciu fyzických osôb, ktorým bolo uložené obmedzujúce opatrenie spočívajúce v zákaze účasti na verejných podujatiach; fyzické osoby ktoré obmedzujúce opatrenie vykonávajú, sú vedené aj v **zozname zákazov** podľa druhov športu, súťaží, klubov a štadiónov, na ktoré sa tieto zákazy vzťahujú,
c) **register PO** - evidencia fyzických osôb, ktoré majú príslušným orgánom verejnej moci uložené predbežné opatrenie podľa § 27 ods. 2 zákona alebo primerané obmedzenie podľa § 86 Trestného poriadku spočívajúce v zákaze účasti na podujatiach; tieto fyzické osoby sú vedené aj v **zozname zákazov** podľa druhov športu, súťaží, klubov a štadiónov, na ktoré sa tieto zákazy vzťahujú,
d) **register V** - evidencia fyzických osôb, ktoré sú štátnymi príslušníkmi iného štátu a bolo im uložené administratívne vyhostenie a zákaz vstupu na územie Slovenskej republiky za protiprávne konanie v súvislosti s účasťou na podujatí, ktorého sa dopustili na území Slovenskej republiky,
e) **register C** - evidencia fyzických osôb, ktoré boli postihnuté alebo potrestané za protiprávne konanie v súvislosti s účasťou na podujatí v cudzine,
f) **register DK** - evidencia fyzických osôb, ktoré boli postihnuté v disciplinárnom konaní za agresívne prejavy v súvislosti s účasťou na podujatí; fyzické osoby, ktoré vykonávajú disciplinárne opatrenie zákaz vstupu na miesto konania podujatia alebo predbežné opatrenie obdobnej povahy, sú evidované aj v **zozname zákazov** podľa druhov športu, súťaží, klubov a štadiónov, na ktoré sa tieto zákazy vzťahujú,
g) **register K** - evidencia fyzických osôb, ktoré porušili organizačný poriadok podujatia alebo návštevný poriadok podujatia,
h) **register N** - evidencia fyzických osôb, ktoré sa dopustili konania zakladajúceho podozrenie z priestupku diváckeho násilia alebo trestného činu spáchaného v súvislosti s

účasťou na podujatí a ich totožnosť nebola zistená.

(2) Tá istá fyzická osoba môže byť vedená vo viacerých registroch, podľa druhu a závažnosti deliktov, ktorých sa dopustila.

(3) Fyzické osoby v registroch je možné zobraziť v prehľadoch vytvorených podľa rôznych kritérií, najmä podľa príslušnosti k športovému odvetviu, športovému klubu, skupine priaznivcov, podľa spriatelených skupín priaznivcov iných domácich športových klubov a zahraničných športových klubov.

Čl. 13

Evidencia hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov

V evidencii hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov sú vedené tieto registre

a) **register HU** obsahujúci evidenciu fyzických osôb s platným osvedčením hlavného usporiadateľa,
b) **register BM** obsahujúci evidenciu fyzických osôb s platným osvedčením bezpečnostného manažéra,
c) **register U** obsahujúci evidenciu fyzických osôb s platným preukazom usporiadateľa.

Čl. 14

Evidencia dohôd

(1) V evidencii dohôd sú vedené tieto registre

a) **register DPZ** obsahujúci evidenciu písomných dohôd organizátora podujatia a Policajného zboru podľa § 18 ods. 4 zákona a
b) **register DOP** obsahujúci evidenciu písomných dohôd organizátora podujatia a obecnej polície podľa § 8 ods. 3 zákona.

(2) Dohody v registroch DPZ a DOP sú vedené v prehľade dohôd aj podľa rokov, športových odvetví a doby platnosti dohôd.

Čl. 15

Evidencia extrémistických symbolov

(1) V evidencii extrémistických symbolov sú vedené tieto oddiely

a) oddiel obsahujúci evidenciu extrémistických symbolov používaných v Slovenskej republike,
b) oddiel obsahujúci evidenciu extrémistických symbolov používaných v zahraničí,
c) oddiel obsahujúci evidenciu extrémistických symbolov pravicového extrémizmu,
d) oddiel obsahujúci evidenciu extrémistických symbolov ľavicového extrémizmu,
e) oddiel obsahujúci evidenciu extrémistických symbolov náboženského extrémizmu.

(2) Údaje v evidencii podľa odseku 1 je možné zobraziť aj podľa športových klubov a ich priaznivcov, podľa spriatelených skupín priaznivcov iných domácich športových klubov a zahraničných športových klubov, ktorí jednotlivé extrémistické symboly v minulosti použili v súvislosti s účasťou na podujatí konanom na Slovensku alebo v zahraničí.

Čl. 16

Modul odbornej prípravy

(1) Modul odbornej prípravy uchádzača obsahuje študijné materiály najmä právne predpisy, metodické odporúčania, smernice, odborné publikácie, prezentácie, odborný test a iné pomôcky slúžiace na odbornú prípravu uchádzačov o získanie alebo overenie odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa, ktoré budú uchádzačom sprístupnené prostredníctvom webového sídla správcu informačného systému.
(2) Odborný test na prípravu a skúšku uchádzačov o získanie alebo overenie odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa vypracuje odborná komisia v súlade s § 13 ods. 7 zákona, ktorá zároveň určí jednotné pravidlá pre používanie testov a postup pri overovaní odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa a oznámi ich správcovi informačného systému.
(3) Správca informačného systému zapracuje jednotné pravidlá pre používanie testov a postup pri overovaní odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa do modulu odbornej prípravy.
(4) Uchádzač o získanie alebo overenie odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa absolvuje prípravu a skúšku v module odbornej prípravy po pridelení identifikátora fyzickej osoby.
(5) V module odbornej prípravy sa automaticky v časovom poradí ukladajú informácie o postupe uchádzača pri získaní alebo overení odbornej spôsobilosti hlavného usporiadateľa, bezpečnostného manažéra a usporiadateľa, ktoré sú prístupné Policajnému zboru a príslušnému národnému športovému zväzu.

Čl. 17
Štruktúra údajov v evidenciách

(1) Do registrov evidencie rizikových účastníkov podujatia sa údaje o fyzických osobách a jej konaní, ktoré bolo dôvodom zápisu do príslušného registra, zaznamenávajú v štruktúre podľa § 22 ods. 3 a 4 zákona.
(2) Do informačného systému sa zaznamenávajú aj obrazové, zvukové a obrazovo-zvukové záznamy (ďalej len “záznam”) s týmito popisnými dátami:

a) dátum a čas vyhotovenia záznamu,
b) miesto vyhotovenia záznamu,
c) označenie podujatia, na ktorom bol záznam vyhotovený,
d) identifikačné údaje fyzickej osoby, ktorá sa dopustila konania, na preukázanie ktorého záznam slúži, ak sú známe,
e) identifikačné údaje fyzickej osoby, ktorá záznam vyhotovila,
f) špecifikácia zariadenia, ktorým bol záznam vyhotovený.

(3) Popisné dáta sa pripájajú k záznamu takým spôsobom, aby slúžili na vyhľadávanie a zostavovanie prehľadov a zostáv v jednotlivých registroch evidencie rizikových účastníkov podujatia podľa zadaných kritérií.
(4) Do registrov evidencie hlavných usporiadateľov, bezpečnostných manažérov a usporiadateľov sa údaje o hlavnom usporiadateľovi, bezpečnostnom manažérovi a usporiadateľovi zaznamenávajú údaje v štruktúre podľa § 22 ods. 6 zákona.

Čl. 18
Identifikátor fyzickej osoby

(1) Informačný systém automaticky vygeneruje každej fyzickej osobe uvedenej v informačnom systéme v jednotlivých evidenciách jedinečné identifikačné číslo odlišné od rodného čísla, s ktorým je v systéme previazané za účelom autentifikácie jedinečnosti fyzickej osoby v informačnom systéme.
(2) Jedinečnosť identifikátora fyzickej osoby podľa odseku 1 je zabezpečená kontrolou rodného čísla, ktoré sa uvádza pri evidovaní fyzickej osoby v príslušnom registri. Následne sa používa výhradne identifikátor fyzickej osoby.
(3) Ak ide o štátneho príslušníka iného štátu, namiesto rodného čísla sa používa číslo identifikačného dokladu s fotografiou vydaného príslušným orgánom iného štátu.

Čl. 19
Formát údajov v evidenciách

(1) Fotografia tváre fyzickej osoby sa zaznamenáva v bežne používaných štandardizovaných formátoch.
(2) Pre popisné dáta o záznamoch podľa čl. 9 sa používajú bežne používané štandardizované formáty.
(3) Pre prenos údajov a popisných dát sa použijú štandardy
a) jazyka schém XML Schema Definition minimálne vo verzii 1.0,
b) formátu Extensible Markup Language vo verzii 1.0 podľa World Wide Web Consortium
c) formát Portable Document Format (.pdf),
d) špecifikácie znakovej sady Unicode Transformation Format, kódovanie UTF-8.
(5) Lekársky posudok o spôsobilosti osoby na výkon činnosti usporiadateľskej služby a čestné vyhlásenie o bezúhonnosti sa vkladá do príslušného registra vo formáte Portable Document Format (.pdf).
(6) Dohody organizátorov podujatí a Policajného zboru podľa § 18 ods. 4 zákona a dohody organizátorov podujatí a obecnej polície sa vkladajú do príslušného registra vo formáte Portable Document Format (.pdf).
(7) Extrémistické symboly sa vkladajú do príslušného oddielu v bežne používaných štandardizovaných formátoch.

III. Časť - Nakladanie s údajmi v informačnom systéme

Čl. 20
Spracúvanie údajov v informačnom systéme

(1) Spracúvať údaje v jednotlivých registroch a oddieloch evidencií informačného systému môžu len oprávnené osoby so zodpovedajúcim prístupovým právom a pridelenou rolou.
(2) Spracúvanie údajov musí zodpovedať štruktúre údajov v jednotlivých registroch a oddieloch evidencií informačného systému a určenému formátu spracovania údajov. Údaje o protiprávnom konaní, iných charakteristikách slúžiacich na identifikáciu fyzickej osoby alebo iných

skutočnostiach sa môžu spracúvať len v takom rozsahu a obsahu, ktorý zodpovedá účelu ich spracovania a sú nevyhnutné na jeho dosiahnutie.
(3) V informačnom systéme sa zaznamenávajú správne a úplne údaje; to neplatí ak ide o údaje podľa § 22 ods. 2 písm. j) zákona. Údaj sa považuje za správny, ak sa nepreukáže opak.
(4) Na účely správnosti a aktuálnosti údajov v informačnom systéme oprávnená osoba správcu informačného systému zabezpečí opravu alebo doplnenie tých údajov, ktoré sa v priebehu spracúvania stali neaktuálnymi, alebo sa neskôr preukázali ako nesprávne.
(5) V prípade zistenia neúplných, neaktuálnych alebo nesprávnych údajov oprávnená osoba o tejto skutočnosti bezodkladne informuje správcu informačného systému.

Čl. 21
Zálohovanie a archivácia údajov v informačnom systéme

(1) Účelom zálohovania a archivácie je zabezpečenie údajov spracúvaných v informačnom systéme spôsobom a v rozsahu, ktorý vychádza z požiadaviek na jednotlivé údaje.
(2) Zálohovanie údajov umožňuje obnovu údajov v prípade nedostupnosti informačného systému, zničenia alebo poškodenia údajov. Všetky údaje spracúvané v informačnom systéme musia byť zálohované.
(3) Archivácia slúži na zachovanie neaktívnych údajov a dlhodobé uloženie údajov v informačnom systéme.
(4) Pre všetky údaje v informačnom systéme sa vypracúvajú plány zálohovania a archivácie, ktoré vychádzajú z požiadaviek na integritu a dostupnosť týchto údajov určených správcom informačného systému.
(5) Prevádzkové zálohy sa vytvárajú najmenej raz denne. Archivačné zálohy sa vytvárajú najmenej raz za dva mesiace.
(6) Záložné média sú uchovávané tak, aby bola zabezpečená ich primeraná ochrana.
(7) Funkcionalita záložných médií a obnova informačného systému sa systematicky testujú.

Čl. 22
Ochrana osobných údajov

Ak zákon neustanovuje inak, pri spracúvaní a ochrane osobných údajov sa postupuje podľa zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len “zákon o ochrane osobných údajov”).

IV. Časť - Používanie informačného systému

Čl. 23
Vyhľadávanie v informačnom systéme a vyhotovenie výpisu

(1) V rámci prípravy a organizácie podujatia alebo na základe iných skutočností súvisiacich s podujatím bezpečnostný manažér vstupuje do informačného systému za účelom vyhľadania a získania informácií dôležitých pre zabezpečenie riadneho a pokojného priebehu podujatia a vykonania bezpečnostných opatrení s cieľom zníženia bezpečnostného rizika.
(2) Po úspešnom prihlásení sa do informačného systému, autentifikácii prístupových práv a po otvorení úvodného okna informačného systému bezpečnostný manažér zvolí príslušnú evidenciu

a podľa vopred zvolených kritérií priamo vyhľadáva v príslušnom registri alebo oddiely alebo v kombinácií registrov a oddielov požadované údaje.
(3) Na účely plnenia povinnosti organizátora podujatia neumožniť vstup na podujatie fyzickej osobe, ktorej účasť na podujatí bola zakázaná, bezpečnostný manažér vstupuje do zoznamu aktívnych zákazov. V zozname aktívnych zákazov na základe zvolených kritérií podľa označenia druhu podujatia, športového klubu alebo jeho družstva, súťaže alebo športu, na ktoré sa zákaz vzťahuje, bezpečnostný manažér vyhľadá fyzické osoby s aktívnym zákazom zodpovedajúcim organizovanému podujatiu.
(4) Zo zoznamu aktívnych zákazov vytvoreného podľa odseku 3 bezpečnostný manažér príslušnou operáciou v informačnom systéme vyhotoví výpis s údajmi o fyzických osobách s aktívnym zákazom účasti na organizovanom podujatí (ďalej len "výpis zákazov").
(5) Na výpise zákazov sú o fyzických osobách uvedené tieto údaje:

a) meno a priezvisko,
b) dátum narodenia,
c) príslušnosť alebo iné vzťahy k športovým klubom,
d) druh športu, v súvislosti s účasťou na ktorom sa fyzická osoba dopustila protiprávneho konania,
e) fotografiu tváre,
f) iné charakteristiky slúžiace na identifikáciu fyzickej osoby.

(6) Výpis zákazov vytvorený podľa odseku 3 je elektronickým výstupom, ktorý môže byť v tejto podobe dočasne elektronicky sprístupnený členom usporiadateľskej služby
(7) Výpis zákazov je možné generovať aj ako tlačovú zostavu vykonaním príslušných operácií v informačnom systéme. Tlačová zostava sa vytvorí vo formáte Portable Document Format (.pdf).

Čl. 24
Distribúcia výpisu zákazov členom usporiadateľskej služby

(1) Bezpečnostný manažér alebo hlavný usporiadateľ na zabezpečenie plnenia úloh usporiadateľskej služby sprístupní členom usporiadateľskej služby výpis zákazov.
(2) Pred konaním podujatia bezpečnostný manažér odovzdá hlavnému usporiadateľovi výpisy zákazov v potrebnom počte výtlačkov tlačovej zostavy. Hlavný usporiadateľ následne odovzdá výpisy zákazov ostatným členom usporiadateľskej služby.
(3) Hlavný usporiadateľ zodpovedá za odovzdanie výpisov zákazov členom usporiadateľskej služby a za riadne vrátenie všetkých výpisov zákazov bezodkladne po ukončení podujatia bezpečnostnému manažérovi.
(4) Hlavný usporiadateľ pri odovzdávaní výpisu zákazov členom usporiadateľskej služby vykoná aj poučenie o postupoch podľa tejto smernice.
(5) Člen usporiadateľskej služby je povinný prevziať výpis zákazov, používať ho pred podujatím a v priebehu podujatia na plnenie svojich úloh a ihneď po podujatí odovzdať výpis zákazov hlavnému usporiadateľovi.
(6) O odovzdaní výpisov zákazov členom usporiadateľskej služby a o ich vrátení hlavný usporiadateľ vyhotoví protokol. Protokol obsahuje

a) identifikáciu bezpečnostného manažéra,
b) identifikáciu hlavného usporiadateľa,

c) identifikáciu členov usporiadateľskej služby, ktorým bol odovzdaný výpis zákazov,
d) počet odovzdaných výpisov zákazov,
e) počet vrátených výpisov zákazov.

(7) Hlavný usporiadateľ bezodkladne po skončení podujatia odovzdá protokol a výpisy zákazov bezpečnostnému manažérovi, ktorí zabezpečí ich bezpečné uschovanie alebo likvidáciu.
(8) Bezpečnostný manažér môže sprístupniť členom usporiadateľskej služby s priamym prístupom do informačného systému výpis zákazov v elektronickej forme na čas nevyhnutný na dosiahnutie účelu zákona.
(9) Elektronický prístup pre každého člena usporiadateľskej služby sa poskytuje na časovo obmedzené obdobie určené bezpečnostným manažérom, po uplynutí ktorého tento elektronický prístup automaticky zaniká.

Čl. 25
Zápis do evidencií a registrov

(1) Ak v priebehu podujatia dôjde ku konaniu, ktoré je dôvodom zápisu do evidencie rizikových účastníkov (bezpečnostný incident), hlavný usporiadateľ vyhotoví ku každému bezpečnostnému incidentu záznam v písomnej forme alebo elektronickej forme (záznam o bezpečnostnom incidente), ktorý obsahuje popis deliktuálneho konania účastníka podujatia, ako aj údaje o dotknutej osobe, na účely zápisu do príslušného registra evidencie rizikových účastníkov podujatia.
(2) K záznamu o bezpečnostnom incidente podľa odseku 1 hlavný usporiadateľ pripojí aj príslušný záznam z kamerového zabezpečovacieho systému a iné záznamy preukazujúce identitu fyzickej osoby a okolnosti jej protiprávneho konania.
(3) Hlavný usporiadateľ bezodkladne odovzdá písomný záznam alebo elektronický záznam o bezpečnostnom incidente bezpečnostnému manažérovi. Záznamy o bezpečnostných incidentoch sú súčasťou správy o podujatí.
(4) Ak ide o konanie, ktoré je dôvodom zápisu do evidencie rizikových účastníkov podujatia a na zápis fyzickej osoby je oprávnený bezpečnostný manažér, bezpečnostný manažér zapíše bezodkladne údaje v ustanovenej štruktúre do príslušného registra evidencie rizikových účastníkov podujatia.
(5) Ak je predmetom zápisu konanie fyzickej osoby na základe rozhodnutí orgánov činných v trestnom konaní a súdu, údaje v rozsahu zaslanej informácie zapíše oprávnená osoba správcu informačného systému bezodkladne po doručení informácie.
(6) Údaje do jednotlivých evidencií informačného systému zapisuje oprávnená osoba bezodkladne.

Čl. 26

(1) Ak ide o podujatie, pri ktorom nie je zákonom ustanovená povinnosť určiť bezpečnostného manažéra, plní úlohy bezpečnostného manažéra podľa tejto smernice hlavný usporiadateľ alebo iná organizátorom podujatia osobitne poverená osoba.
(2) Ak športový zväz alebo športový klub nemá bezpečnostného manažéra, plní úlohy bezpečnostného manažéra podľa tejto smernice hlavný usporiadateľ alebo iná športovým zväzom alebo športovým klubom osobitne poverená osoba.

Čl. 27
Výmena informácií

(1) Údaje z informačného systému môžu byť na základe žiadosti sprístupnené aj inej osobe podieľajúcej sa na organizovaní podujatia alebo na kontrole dodržiavania zákona, v rozsahu zodpovedajúcom potrebám činnosti vykonávanej touto osobou.
(2) Žiadosť o sprístupnenie údajov v informačnom systéme obsahuje
a) identifikačné údaje žiadateľa,
b) činnosť, ktorú žiadateľ vykonáva,
c) odôvodnenie žiadosti,
d) účel sprístupnenia údajov,
e) rozsah požadovaných údajov.
(3) O sprístupnení údajov z informačného systému na základe žiadosti a o rozsahu sprístupnených údajov rozhoduje prevádzkovateľ informačného systému.
(4) Údaje z informačného systému sa poskytujú alebo sprístupňujú Policajnému zboru, prokuratúre, súdom, obciam, okresným úradom, Slovenskej informačnej službe, športovým zväzom a organizátorom podujatí, ak je to nevyhnutné na plnenie ich úloh.
(5) Údaje z informačného systému orgánom podľa odseku 4 poskytuje prevádzkovateľ informačného systému.
(6) Ak je to účelné, môže prevádzkovateľ informačného systému žiadateľovi podľa odseku 1 a orgánom podľa odseku 4 sprístupniť údaje v informačnom systéme pridelením prístupového práva.
(7) Cezhraničná výmena príslušných údajov v informačnom systéme podľa § 22 ods. 14 zákona sa uskutočňuje cez Národné futbalové informačné stredisko [1]).

V. Časť - Správa a prevádzka informačného systému

Čl. 28
Povinnosti správcu informačného systému

Správca informačného systému je povinný najmä
a) chrániť vlastné prístupové práva a autentifikačné prostriedky,
b) používať bezpečné heslá na správu informačného systému,
c) udržiavať dokumentáciu spravovaného informačného systému v súlade s jeho skutočným stavom,
d) informovať včas zodpovednú osobu o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu osobných údajov,
e) zabezpečovať plynulú, bezpečnú a spoľahlivú prevádzku informačného systému vrátane organizačného, odborného a technického zabezpečenia,
f) spravovať registre a oddiely príslušných evidencií,
g) zabezpečiť vytváranie a rušenie prístupových práv v ustanovenom rozsahu,

[1]) *článok 1 a nasl. rozhodnutia Rady z 25. apríla 2002 týkajúce sa bezpečnosti v súvislosti s futbalovými zápasmi s medzinárodným rozmerom (2002/348/SVV)*

h) zabezpečiť pravidelnú správu a údržbu prevádzkového systému,
i) spracovať prevádzkovú dokumentáciu o architektúre informačného systému a konfiguráciách,
j) riadiť zmeny vo funkcionalitách a konfiguráciách informačného systému,
k) chrániť údaje pred poškodením, zničením, stratou, nedovoleným prístupom a sprístupnením, ako aj pred akýmikoľvek inými neprípustnými formami spracúvania,
l) bezpečne v súlade so zákonom zálohovať a archivovať údaje v informačnom systéme,
m) oznámiť zistené porušenie zákona alebo tejto smernice orgánu príslušnému na vyvodenie disciplinárnej zodpovednosti alebo právnej zodpovednosti podľa právnych predpisov. [2])

Čl. 29
Povinnosti prevádzkovateľa informačného systému

Prevádzkovateľ informačného systému je povinný najmä
a) zabezpečiť, aby sa spracúvali len také údaje, ktoré určuje štruktúra údajov v jednotlivých evidenciách informačného systému,
b) zabezpečiť, aby údaje, ktoré boli získané na rozdielne účely, neboli združované,
c) zabezpečiť, aby zhromaždené osobné údaje boli spracované vo forme umožňujúcej identifikáciu dotknutej osoby počas doby nie dlhšej ako je ustanovená,
d) zlikvidovať údaje v súlade so zákonom a zákonom o ochrane osobných údajov,
e) spracúvať len správne, úplné a podľa potreby aktualizované údaje vo vzťahu k účelu spracúvania; nesprávne a neúplné údaje je prevádzkovateľ povinný blokovať a bez zbytočného odkladu opraviť alebo doplniť; nesprávne a neúplné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, prevádzkovateľ zreteľne označí a bez zbytočného odkladu zlikviduje,
f) spracúvať údaje v informačnom systéme v súlade so zákonom, zákonom o ochrane osobných údajov a inými právnymi predpismi a spôsobom, ktorý im neodporuje,
g) zabezpečiť výkon dohľadu nad ochranou osobných údajov písomným poverením zodpovednej osoby a umožniť jej nezávislý výkon dohľadu nad ochranou osobných údajov,
h) poučiť oprávnené osoby o právach a povinnostiach pri používaní informačného systému.

Čl. 30
Povinnosti oprávnenej osoby

Oprávnená osoba je povinná
a) dodržiavať zásady spracovania údajov ustanovené zákonom, zákonom o ochrane osobných údajov a touto smernicou,
b) dodržiavať bezpečnostné opatrenia na ochranu osobných údajov,

[2]) Podľa § 3 ods. 2 Trestného poriadku:
"*(2) Štátne orgány, vyššie územné celky, obce a* ***iné právnické osoby sú povinné bez meškania oznamovať orgánom činným v trestnom konaní skutočnosti nasvedčujúce tomu, že bol spáchaný trestný čin*** *a včas vybavovať dožiadania orgánov činných v trestnom konaní a súdov."*

c) informovať včas zodpovednú osobu o všetkých skutočnostiach, ktoré by mohli viesť k zneužitiu údajov,
d) podrobiť sa kontrole zo strany zodpovednej osoby,
e) dodržiavať pravidlá vytvárania elektronických výpisov a tlačových zostáv ustanovené touto smernicou,
f) zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; povinnosť mlčanlivosti trvá aj po zániku výkonu funkcie oprávnenej osoby,
g) oznámiť narušenie alebo podozrenie z narušenia bezpečnosti informačného systému správcovi informačného systému.

Čl. 31
Obmedzenia a zákazy

(1) Oprávnená osoba sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva, ktoré jej neboli pridelené.
(2) Oprávnená osoba nesmie napomáhať iným osobám pri získavaní prístupových práv, ktoré im neboli pridelené.
(3) Ak oprávnená osoba zistí, že má prístupové práva, ktoré jej neprináležia, nesmie ich používať a bezodkladne o tom informuje oprávnenú osobu správcu informačného systému.
(4) Oprávnená osoba nesmie údaje v informačnom systéme a výpis zákazov využívať pre osobnú potrebu alebo na iný než ustanovený účel.
(5) Oprávnená osoba nesmie vyhotovovať tlačenú, elektronickú alebo inú kópiu výpisu zákazov alebo sprístupniť výpis zákazov osobe, ktorá nie je oprávnená na jeho sprístupnenie.

Čl. 32
Príprava oprávnenej osoby

(1) Oprávnená osoba v rámci odbornej prípravy na získanie odbornej spôsobilosti na výkon svojej činnosti absolvuje poučenie o právach a povinnostiach ustanovených zákonom o ochrane osobných údajov a touto smernicou.
(2) Na používanie informačného systému správca sprístupní pre oprávnenú osobu používateľskú príručku vo forme video-návodu.

Čl. 33
Zodpovedná osoba

(1) Zodpovedná osoba má postavenie oprávnenej osoby s právom prístupu do informačného systému v rozsahu potrebnom na plnenie jej úloh. Zodpovedná osoba musí spĺňať podmienky ustanovené zákonom o ochrane osobných údajov.
(2) Zodpovedná osoba je povinná pri zistení narušenia práv a slobôd dotknutých osôb alebo porušenia zákonných ustanovení v priebehu spracovávania osobných údajov bezodkladne tieto skutočnosti písomne oznámiť oprávnenej osobe správcu informačného systému a vyzvať ju na prijatie príslušných opatrení.
(3) Zodpovedná osoba
a) vykonáva dohľad nad plnením základných povinností prevádzkovateľa informačného systému pri spracovávaní a ochrane osobných údajov,

b) zabezpečuje potrebnú súčinnosť s Úradom na ochranu osobných údajov SR,
c) zabezpečuje vybavovanie žiadostí dotknutých osôb,
d) zabezpečuje prijatie bezpečnostných opatrení, dohliada na ich aplikáciu v praxi a zabezpečuje ich aktualizáciu,
e) zabezpečuje dohľad nad cezhraničným prenosom osobných údajov,
f) zabezpečuje vedenie zoznamu oprávnených osôb v informačnom systéme,
g) zabezpečuje vedenie evidencie informačného systému v súlade so zákonom o ochrane osobných údajov.

VI. Časť - Spoločné ustanovenia

Čl. 34
Údržba informačného systému

(1) Aplikačné vybavenie, operačné systémy a iné softvérové vybavenie informačného systému musia byť chránené adekvátnymi a účinnými opatreniami na ochranu pred škodlivým softvérom. Bezpečnostné mechanizmy na ochranu pred škodlivým softvérom musia byť pravidelne aktualizované.
(2) Všetky hardverové a softvérové prostriedky informačného systému musia byť udržiavané zaškoleným personálom, ich opravu a servis môžu vykonávať len autorizovaní zamestnanci správcu informačného systému alebo tretích strán.
(3) Systém správy porúch musí byť navrhnutý a implementovaný takým spôsobom, aby bola zabezpečená detekcia, izolovanie, oprava a dokumentácia porúch prostriedkov informačného systému.
(4) Kontrola prevádzky informačného systému sa uskutočňuje nepretržite technickými prostriedkami a programovými prostriedkami.
(5) O každej vykonanej údržbe informačného systému sa vedú záznamy.

Čl. 35

Správca informačného systému môže na základe zmluvného vzťahu poveriť výkonom svojich činností v informačnom systéme tretiu osobu; tým nie sú dotknuté ustanovenia osobitných predpisov.

Čl. 36
Kontrolná činnosť

(1) Zodpovedná osoba vykoná najmenej raz ročne kontrolu zameranú na dodržiavanie ochrany osobných údajov v informačnom systéme.
(2) Zodpovedná osoba vykoná
a) kontrolu archivovania,
b) v súčinnosti s oprávnenou osobou správcu informačného systému kontrolu funkčnosti a úplnosti záloh.
(3) O výsledkoch kontrol vyhotoví zodpovedná osoba písomnú správu a predloží ju prevádzkovateľovi informačného systému. Písomná správa o kontrole obsahuje
a) zhodnotenie celkového stavu ochrany osobných údajov,

b) popis zistených nedostatkov, popis opatrení na odstránenie nedostatkov a informácia o stave ich implementácie.

(4) O vykonaní kontroly nie je zodpovedná osoba povinná oprávnenú osobu, ktorej sa kontrola týka, vopred informovať.

Čl. 37
Zodpovednosť

(1) Každý kto zistí konanie, ktoré môže byť v rozpore so zákonom alebo s touto smernicou je povinný oznámiť to správcovi informačného systému zaslaním oznámenia v písomnej forme alebo v elektronickej forme.

(2) Oprávnená osoba správcu informačného systému je povinná vykonať potrebné opatrenia na zamedzenie ďalšieho porušovania zákona, zákona o ochrane osobných údajov alebo tejto smernice.

(3) Za porušenie povinností pri nakladaní s výpisom zákazov a vyhotovení protokolu zodpovedá organizátor podujatia, ktorý môže byť postihnutý v disciplinárnom konaní.[3]) Možnosť vyvodenia zodpovednosti voči fyzickej osobe, ktorá sa dopustila protiprávneho konania, tým nie je dotknutá.

(4) Oprávnená osoba správcu informačného systému je povinná oznámiť zistené porušenie zákona alebo tejto smernice orgánom príslušným na vyvodenie zodpovednosti voči právnickej osobe, aj voči konkrétnej fyzickej osobe v konaní orgánov verejnej moci (trestné konanie, priestupkové konanie, správne konanie) a v disciplinárnom konaní.

Čl. 38
Prevádzkový účet

(1) Správca informačného systému zriadi samostatný účet v peňažnom ústave, ktorý bude používaný výhradne na príjem a úhradu prostriedkov v súvislosti so zabezpečením správy, prevádzky a rozvoja informačného systému a na iné zákonom ustanovené účely (§ 23 ods. 1 zákona).

(2) Dispozičné právo k prevádzkovému účtu vykonáva štatutárny orgán správcu informačného systému alebo ním poverená osoba. Platby z prevádzkového účtu je možné vykonať iba v súlade s ustanoveným účelom. Úhrady za plnenia a služby uvedené v odsekoch 3 až 5 sa uhrádzajú po ich schválení štatutárnym orgánom správcu informačného systému alebo ním poverenej osoby.

(3) Výdavky na správu a prevádzku informačného systému uhrádza správca informačného systému spravidla na základe dlhodobého zmluvného vzťahu s dodávateľom príslušných služieb za ceny na trhu obvyklé. Zmluvy o dodaní príslušných služieb budú po ich uzavretí bezodkladne zverejnené na webovom sídle správcu informačného systému.

(4) Výdavky na rozvoj informačného systému sa uhrádzajú na základe rozhodnutia príslušného orgánu správcu informačného systému, ktoré musí obsahovať popis, dôvody, prínos a predpokladané náklady (obvyklá trhová cena) schváleného rozvoja informačného systému. Rozhodnutia o rozvoji informačného systému a zmluvy o dodaní diela uzatvorené na základe tohto rozhodnutia budú bezodkladne zverejnené na webovom sídle správcu.

[3]) Čl. 64 Disciplinárneho poriadku SFZ (Porušenie povinnosti vyplývajúcej z predpisu alebo rozhodnutia orgánu SFZ alebo jeho člena)

(5) O vykonaní rozhodnutia o rozvoji informačného systému vyhotoví dodávateľ správu, ktorú schváli orgán správcu informačného systému, ktorý rozhodnutie vydal. Správa bude po jej schválení bezodkladne zverejnená na webovom sídle správcu informačného systému ako príloha k príslušnému rozhodnutiu správcu informačného systému o schválení rozvoja informačného systému.
(6) Výdavky, ktorých cieľom je zabezpečenie verejného poriadku a ochrany bezpečnosti, zdravia, mravnosti, majetku a životného prostredia na podujatiach a výdavky na vzdelávacie aktivity v tejto oblasti, schvaľuje príslušný orgán správcu informačného systému.
(7) Správa o príjmoch, výdavkoch a stave prevádzkového účtu informačného systému je osobitnou časťou správy o hospodárení správcu informačného systému za príslušné účtovné obdobie a je zverejnená na jeho webovom sídle.
(8) Kontrola použitia prostriedkov z prevádzkového účtu sa vykonáva

a) prostredníctvom riadneho vykonávania oprávnení a povinností správcu informačného systému,
b) prostredníctvom príslušného revízneho orgánu správcu informačného systému na základe podnetu na preskúmanie postupu alebo aj bez podnetu,
c) verejnou kontrolou príjmov, výdavkov a zodpovedajúcich zmlúv, faktúr, rozhodnutí a správ zverejnených na webovom sídle správcu informačného systému.

(9) Každý kto zistí možné pochybenie pri postupe podľa tejto smernice, oznámi ho správcovi informačného systému alebo jeho revíznemu orgánu. Správca informačného systému zriadi za tým účelom osobitnú elektronickú adresu. Podnety na preskúmanie postupu a ich vybavenie budú zverejnené na webovom sídle správcu informačného systému. Opakované podnety, ktoré neobsahujú nové skutočnosti sa nevybavujú, iba sa pripoja k predchádzajúcemu podnetu a jeho vybaveniu.
(10) Všetky príjmy a výdavky prevádzkového účtu sú podľa § 23 ods. 5 zákona priebežne zverejňované na webovom sídle správcu informačného systému.
(11) Zverejňovanie všetkých informácií súvisiacich s príjmami a výdavkami prevádzkového účtu sa uskutočňuje tak, aby umožňovalo efektívnu vecnú kontrolu jednotlivých príjmov a výdajov vrátane k nim náležiacich zmlúv a ich príloh a dodatkov, faktúr, rozhodnutí a správ.
(12) Kontrolu zasielania prostriedkov z pokút uložených za priestupky na prevádzkový účet podľa § 27 ods. 9 zákona vykonáva správca informačného systému prostredníctvom svojho revízneho orgánu alebo inej poverenej osoby.
(13) Disciplinárne orgány príslušného športového zväzu vedú evidenciu pokút uložených a uhradených organizátormi podujatí, ktorí sú jeho členmi, za porušenie povinností organizátora podujatia. Polovicu z uhradenej pokuty príslušný športový zväz bezodkladne prevedie na prevádzkový účet.
(14) Správca informačného systému najmenej raz ročne vyžiada od príslušných športových zväzov správu o uložených pokutách, ktorú zverejní na svojom webovom sídle.

Čl. 39
Zrušovacie ustanovenie

Zrušuje sa smernica o vytvorení a prevádzkovaní informačného systému o bezpečnosti pri športových podujatiach schválená výkonným výborom SFZ dňa 15. januára 2013.

Čl. 40
Záverečné ustanovenia

(1) Táto smernica nadobúda platnosť dňom jej schválenia výkonným výborom SFZ.
(2) Táto smernica nadobúda účinnosť 12. marca 2014.