



# BEZPEČNOSTNÁ SMERNICA GDPR

ZÁSADY BEZPEČNOSTI PRE POVERENÉ OSOBY-  
POUŽÍVATEĽOV IS,  
ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ IS,  
ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV V LISTINÁCH A  
DOKUMENTOCH PRI SPRACOVÁVANÍ OSOBNÝCH ÚDAJOV,  
ZÁSADY BEZPEČNOSTI PRI PREVÁDZKE INFORMAČNÝCH A  
KOMUNIKAČNÝCH TECHNOLOGIÍ NA PRACOVISKU IS,  
INFORMAČNÁ POVINNOSŤ PREVÁDZKOVATEĽA  
DOTKNUTÝM OSOBÁM,

Dokument:

Bezpečnostný projekt GDPR  
Časť: Bezpečnostná smernica  
GDPR

Prevádzkovateľ:  
KLUB SLOVENSKÝCH TURISTOV  
IČO: 00 688 312



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 2/24
------------------------------	--	--------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## OBSAH

Obsah .....	2
1.Hlavné zásady ochrany osobných údajov .....	4
2.Hlavné zásady GDPR .....	5
3. Zásady GDPR bezpečnosti pre poverene osoby .....	6
-používateľov IS.....	6
3.1 Všeobecné ustanovenia .....	6
3.2 Manipulácia s technickými prostriedkami IS.....	6
3.3 Manipulácia s dátovými nosičmi osobných údajov .....	7
(pamäťovými médiami IS) .....	7
3.4 Základné zásady pre manipuláciu s programovým .....	7
vybavením IS .....	7
3.5 Ochrana pred neoprávneným prístupom a .....	8
riadenie prístupu oprávnených osôb .....	8
3.6 Manipulácia s údajmi IS .....	9
3.7 Antivírusové opatrenia.....	10
3.8 Zaznamenávanie a hlásenie problémov.....	10
s pracovnou stanicou .....	10
3.9 Prístup do siete Internet .....	11
4.Zásady GDPR bezpečnosti pri správe databáz a aplikácií IS .....	12
4.1 Všeobecné ustanovenia .....	12
4.2 Podmienky zakladania databáz.....	12
osobných údajov v IS.....	12
4.3 Základné zásady bezpečnosti pri správe .....	13
databáz a aplikácií.....	13
5. Zásady GDPR bezpečnosti pri prevádzke informačných a .....	15
komunikačných technológií na pracovisku IS .....	15
5.1 Všeobecné ustanovenia .....	15



KLUB SLOVENSKÝCH JURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 3/24
------------------------------	--	--------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

5.2	Kľúčové komponenty IS .....	15
5.3	Základné zásady bezpečnej prevádzky IS .....	15
5.4	Zálohovanie .....	16
5.5	Zásady riešenia nepredvídaných udalostí s.....	17
	dopadom na prevádzku IS .....	17
5.6	Zásady riešenia bezpečnostných incidentov .....	17
5.7	Prevenia Zodpovedná osoba resp. štatutárom poverená oprávnená osoba v spolupráci s externým špecialistom je povinná: .....	18
6.	Informačná povinnosť prevádzkovateľa .....	19
	dotknutým osobám podľa GDPR .....	19
6.1	Informácie, ktoré sa majú poskytovať pri získavaní.....	19
	osobných údajov od dotknutej osoby .....	19
6.2	Informácie, ktoré sa majú poskytnúť, ak osobné údaje .....	19
	neboli získané od dotknutej osoby .....	19
6.3	Právo dotknutej osoby na prístup k údajom .....	20
6.4	Spôsob poskytovania žiadosti .....	21
	dotknutej osoby .....	21
6.5	Podmienky vyjadrenia súhlasu zo spracovaným osobných údajov .....	22
6.6	Osobitné kategórie osobných údajov .....	22
6.7	Kopírovanie, skenovanie a zaznamenávanie úradných dokladov všeobecne .....	23
6.8	Správnosť a aktuálnosť osobných údajov .....	24
6.9	Likvidácia osobných údajov .....	24
6.10	Čo je osobný údaj .....	24



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 4/24
------------------------------	--	--------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

## 1. HLAVNÉ ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV

1. Spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“).
2. Získavané na konkrétne určené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi; ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či štatistické účely sa v súlade s článkom 89 ods. 1 nepovažuje za nezlučiteľné s pôvodnými účelmi („obmedzenie účelu“).
3. Primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov“).
4. Správne a podľa potreby aktualizované; musia sa prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia („správnosť“).
5. Smernica európskeho parlamentu a rady (eú) 2015/1535 z 9. Septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (ú. V. Eú I 241, 17.9.2015, s. 1).
6. Uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú.
7. Osobné údaje sa môžu uchovávať dlhšie, pokiaľ sa budú spracúvať výlučne na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb („minimalizácia uchovávania“).
8. Spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení („integrita a dôvernosť“).



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 5/24
------------------------------	--	--------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## 2. HLAVNÉ ZÁSADY GDPR

- Zákonnosť, spravodlivosť a transparentnosť:** Osobné údaje môže prevádzkovateľ spracúvať len v prípade, ak disponuje primeraným právnym základom, napríklad súhlasom alebo na základe osobitného právneho predpisu či na účel plnenia zmluvy. Na transparentné spracúvanie osobných údajov sa vyžaduje, aby dotknutá osoba bola informovaná o rozsahu a spôsoboch spracúvania jej údajov.
- Obmedzenie účelu spracovania:** Získavať osobné údaje dotknutých osôb je prípustné len na výslovne uvedené a legitímne účely a môžu byť ďalej spracúvané len na účel, na ktorý boli získané. Získané osobné údaje sa nesmú ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s účelom, na ktoré boli tieto osobné údaje získané (okrem výnimiek ustanovených v GDPR, napr. v prípade kompatibilného účelu). Je neprípustné získavať osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti.
- Minimalizácia údajov (nevyhnutnosť):** Rozsah spracúvaných osobných údajov dotknutých osôb má byť primeraný (obmedzený) vzhľadom na účel, na ktorý sa spracúvajú. Tzn. na určený účel sa majú spracúvať len osobné údaje, ktoré sú na naplnenie daného účelu nevyhnutné.
- Správnosť osobných údajov:** Prevádzkovateľ má povinnosť zabezpečiť, aby sa osobné údaje dotknutých osôb, ktoré sú nesprávne bezodkladne vymazali alebo opravili.
- Minimalizácia uchovávaní osobných údajov (likvidácia):** Osobné údaje majú byť uchovávané najviac do doby potrebnej na naplnenie účelov, na ktoré sú údaje spracúvané. Uchovávanie osobných údajov na dlhšiu dobu je možné výlučne v prípadoch špecifikovaných v GDPR. Okrem toho je potrebné zabezpečiť, aby boli uchovávané len nevyhnutné údaje.
- Integrita a dôvernosť (bezpečnosť):** Osobné údaje majú byť spracúvané výlučne takým spôsobom, aby sa zabezpečila primeraná bezpečnosť pri ich spracúvaní, ako aj pred ich nezákonným spracúvaním, náhodnou stratou, zničením alebo poškodením. Zabezpečenie ochrany osobných údajov má byť realizované prostredníctvom primeraných technických alebo organizačných opatrení.
- Zodpovednosť:** Prevádzkovateľ a rovnako aj sprostredkovateľ musia vedieť preukázať, že splnil požiadavky GDPR počas celej doby spracúvania osobných údajov.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 6/24
------------------------------	--	--------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

### 3. ZÁSADY GDPR BEZPEČNOSTI PRE POVERENE OSOBY - POUŽÍVATEĽOV IS

#### 3.1 VŠEOBECNÉ USTANOVENIA

Táto časť smernice upravuje základné pravidlá pre zaistenie bezpečnej a spoľahlivej prevádzky pracovných staníc, na ktorých sú prevádzkované IS.

Poverenými osobami – používateľmi IS (ďalej len „používatelia IS“) sú poverené osoby, ktoré na základe pracovnej náplne a na základe oprávnenia, prostredníctvom technických prostriedkov (pracovnej stanice, počítača), využívajú služby IS, teda spracovávajú osobné údaje uložené v IS alebo majú k nim prístup za účelom plnenia svojich pracovných povinností.

V podmienkach prevádzkovateľa sa poverené osoby – používatelia IS riadia nasledovnými článkami tejto časti smernice.

#### 3.2 MANIPULÁCIA S TECHNICKÝMI PROSTRIEDKAMI IS

1. Pracovné stanice musia byť v rámci chráneného priestoru umiestnené tak, aby vplyvom okolia nedošlo k neúmyselnému poškodeniu alebo poruche zariadenia (pádmi, teplom, vodou, elektromagnetickým žiarením, priamym slnečným svetlom, ...).
2. Používateľ IS môže manipulovať s pracovnými stanicami (zapínať, používať, vypínať) len v súlade s inštrukciami výrobcu, resp. dodávateľa zariadenia alebo dodávateľa príslušného programového vybavenia.
3. Používateľ IS nesmie znižovať životnosť pracovných staníc zlým zaobchádzaním a ich znečisťovaním.
4. V blízkosti technických zariadení IS prevádzkovateľa je zakázané jesť, piť a fajčiť, ale aj vykonávať iné činnosti hroziace znečistením technických zariadení, resp. znížením ich životnosti alebo spoľahlivosti (vibrácie, vystavovanie nadmernej prašnosti, vysávanie v blízkosti zapnutého zariadenia a podobne).
5. Používateľ IS nemôže bez súhlasu zodpovednej osoby, resp. štatutára prevádzkovateľa:
  - a) robiť zásahy do pracovných staníc,
  - b) pripájať k pracovným staniciam ďalšie technické zariadenia,
  - c) odpájať technické zariadenia pracovnej stanice,
  - d) premiestňovať pracovné stanice,
  - e) manipulovať s ovládacími prvkami pracovnej stanice okrem tých, ktoré sú umiestnené na vonkajšej strane skrinky pracovnej stanice, tlačiarne a krytu monitora (zapínanie, vypínanie a „resetovanie“ počítača a tlačiarne, vkladanie a vyberanie diskiet a CD/DVD z mechanik, výmena tonera bez oboznámenia sa so spôsobom výmeny).



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 7/24
------------------------------	--	--------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

- Opravy a úpravy pracovnej stanice môže vykonávať len prizvaný kvalifikovaný externý špecialista. Externý špecialista pritom môže zasahovať do pracovnej stanice iba s preukázateľným súhlasom zodpovednej osoby, resp. štatutára prevádzkovateľa. Používateľ IS je povinný odmietnuť prístup k pracovnej stanici osobe, ktorá sa nepreukáže takýmto súhlasom.
- Čistenie povrchu technických zariadení pracovnej stanice od prachu je v kompetencii Používateľa IS. Vnútorne čistenie zariadení IS prevádzkovateľa môže vykonávať len kvalifikovaný externý špecialista pri dodržaní podmienok bodu 6.

### 3.3 MANIPULÁCIA S DÁTOVÝMI NOSIČMI OSOBNÝCH ÚDAJOV (PAMÄŤOVÝMI MÉDIAMI IS)

Na dátové nosiče osobných údajov je možné ukladať záložné kópie dát s osobnými údajmi iba šifrovaným spôsobom, čo musí zabezpečiť buď softwarový komponent IS, (aplikačný program automatizovaného alebo poloautomatizovaného spracovávanía osobných údajov v IS) alebo špeciálny zálohovací software obsahujúci šifrovaciu funkcionálnu.

- Pamäťové médiá IS prevádzkovateľa sú pevné disky, USB pamäte, diskety, magnetické pásky a ostatné médiá používané na uchovávanie dát v elektronickej forme.
- Pamäťové médiá musia byť uložené tak, aby nedošlo k poškodeniu záznamu, predovšetkým nesmú byť vystavované pôsobeniu silného elektromagnetického poľa, teplotným extrémom, vlhkosti a prašnosti.
- Do mechanik prenosných pamäťových médií (diskiet, pásov, CD/DVD) nesmú byť vkladane znečistené alebo poškodené médiá.
- Pri zapínaní pracovnej stanice (počítača) nesmie byť v disketovej mechanike založená disketa.
- Pamäťové médiá (USB pamäte, diskety, CD/DVD) obsahujúce citlivé údaje musia byť skladované na bezpečnom mieste (uzamykateľný stôl, trezor a podobne).

### 3.4 ZÁKLADNÉ ZÁSADY PRE MANIPULÁCIU S PROGRAMOVÝM VYBAVENÍM IS

- Používateľ IS môže na pracovných stanicach používať výlučne len programové vybavenie nainštalované externým špecialistom, resp. nainštalované s preukázateľným súhlasom zodpovednej osoby, resp. štatutára prevádzkovateľa. Používateľ IS nemôže na pracovnej stanici inštalovať ani odinštalovať žiadne programové vybavenie a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými bol riadne oboznámený na školení o používaní príslušného programového vybavenia.
- Používateľ IS nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 8/24
------------------------------	--	--------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

3. Je zakázaný akýkoľvek zásah do nastavení CMOS pracovnej stanice. Povolený zásah sa netýka prípadnej odôvodnenej zmeny počiatočného štartovacieho hesla.
4. Používatelia IS pred opustením pracoviska sú povinní ukončiť prácu s programovým vybavením a pracovnú stanicu vypnúť.
5. Pri krátkodobej neprítomnosti môže používateľ IS, pokiaľ mu to používané programové vybavenie umožňuje, nahradiť vypnutie pracovnej stanice spustením šetriča obrazovky s heslom pre jeho ukončenie.
6. Používatelia IS sú povinní vykonávať základnú údržbu pracovnej stanice – okrem vyčistenia povrchu pracovnej stanice (obrazovka, klávesnica) aspoň raz mesačne čistenie (odstraňovanie nepotrebných súborov) svojich dátových adresárov a pomocných adresárov operačného systému (vrátane adresára Kôš), prípadne spusteniu profylaktických programov (podľa použitého operačného systému – napr. scandisk, defragmentácia disku a podobne). So spôsobom vykonávania základnej údržby systému sa oboznámia na školení.
7. Používatelia IS sú povinní po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť zodpovednej osobe.

### 3.5 OCHRANA PRED NEOPRÁVNENÝM PRÍSTUPOM A RIADENIE PRÍSTUPU OPRÁVNENÝCH OSÔB

Na fyzické dátové stanice osobných údajov je možné ukladať záložné kópie dát s osobnými údajmi iba šifrovaným spôsobom, čo musí zabezpečiť buď softwarový komponent IS (aplikačný program automatizovaného alebo poloautomatizovaného spracovávania osobných údajov v IS) alebo špeciálny zálohovací software obsahujúci šifrovaciu funkcionálnosť.

Prístup tretích strán k IS musí byť zamedzený v najväčšej možnej miere a pre odôvodnenú potrebu takéhoto prístupu musia byť jasne stanovené, prehľadné a kontrolovateľné pravidlá.

Oprávnené osoby pre prístup k IS, resp. k spracovávaniu osobných údajov v IS musia mať pred samotným prístupom k IS zabezpečenú:

- a) **identifikáciu** - jednoznačné identifikovanie oprávnenej osoby pomocou identifikátora (napr. identifikačného kľúča zvereniej osobe, resp. uloženého na GRID karte alebo elektronickom zariadení – „token“)
- b) **autentizáciu** – overenie identity jedinečným príznakom, osobné heslo, osobný certifikát vystavený na konkrétnu osobu
- c) **autorizáciu** – povolenie prístupu alebo iného procesu vykonávaného v IS na základe identifikácie, resp. autentizácie.

Softwarový komponent IS musí zaznamenávať všetky vstupy (log in) a ukončenia vstupov (log out) poverenej osoby do IS a do záznamu doplniť časový údaj.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 9/24
------------------------------	--	--------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

1. Používateľ IS je povinný svoje prístupové heslá meniť najmenej jeden krát za rok, prípadne aj na pokyn zodpovednej osoby, resp. štatutára prevádzkovateľa.
2. Prístupové heslá používateľa IS musia mať aspoň 8 znakov (prístupové heslo šetriča obrazovky aspoň 4 znaky). Používateľ IS nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko.
3. Používateľ IS musí svoje prístupové heslo používať tak, aby sa ho nemohla dozvedieť iná osoba (vrátane iných používateľov). Musí si byť vedomý svojej zodpovednosti za aktivity v IS, ktoré sa vykonávajú pod jeho menom a heslom.
4. V prípade podozrenia, že iná osoba pozná heslo používateľa IS, je tento povinný príslušné heslo okamžite zmeniť a svoje podozrenie ohlásiť zodpovednej osobe.
5. Používateľ IS sa prihlasuje do aplikácie pod svojím menom a svojím heslom aj v prípade, že pracuje na pracovnej stanici pridelennej inému používateľovi.

### 3.6 MANIPULÁCIA S ÚDAJMI IS

1. Súborý údajov na lokálnom disku pracovnej stanice, ktoré používateľ IS vytvára a používa pri svojej práci, je povinný si zálohovať minimálne raz mesačne, s prihliadnutím na rozsah údajov i dvakrát mesačne. So spôsobom zálohovania sa oboznámi na školení. Používateľ IS tieto údaje zálohuje na USB pamäte, diskety alebo na CD/DVD a uskladňuje v zamknutej zásuvke stole alebo v zamknutej skrinke – kľúče od zásuvky, resp. skrinky nesmú zostať voľne prístupné.
2. Používateľ IS môže vytvárať z aplikácie tlačové výstupy len v rozsahu určenom jeho pracovnou náplňou. V prípade výstupov obsahujúcich údaje dôverného charakteru (osobné údaje) musí zabezpečiť, aby k príslušnej tlačiarne nemala počas tlačenia výstupov nekontrolovaný prístup neoprávnená osoba. Vytlačené výstupy obsahujúce údaje dôverného charakteru musia byť skladované alebo zlikvidované tak, aby nedošlo k narušeniu ich dôvernosti.
3. Používateľ IS môže poskytovať údaje IS externým subjektom len v rozsahu určenom jeho pracovnou náplňou a ďalšími predpismi. Výnimku tvoria údaje už zverejnené alebo určené na zverejnenie



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 10/24
------------------------------	--	---------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

### 3.7 ANTIVÍRUSOVÉ OPATRENIA

1. V prípade, že sa na pracovnej ploche používateľa IS zobrazí varovanie, že sa na disku alebo vložennej diskete nachádza vírus, nesmie toto varovanie ignorovať. V prípade, že zavírená disketa patrí inému subjektu, viditeľne a výrazne ju označí ako zavírenú a vráti ju danému subjektu. V prípade zavírenia pevného disku alebo vlastnej diskety, používateľ túto skutočnosť bezodkladne oznámi zodpovednej osobe, prípadne po konzultácii s ňou vykoná antivírusovú „dezinfekciu“ príslušného pamäťového média. So spôsobom vykonania antivírusovej kontroly a „dezinfekcie“ sa oboznámi na školení. V prípade, že nie je možné vykonať antivírusovú „dezinfekciu“ diskety okamžite, musí byť táto disketa viditeľne označená ako zavírená. Po vykonaní antivírusovej „dezinfekcie“ diskety, ktorá je označená ako zavírená, musí byť toto označenie odstránené.
2. V prípade objavenia vírusu v prijatej elektronickej pošte používateľa IS, bezodkladne o tejto udalosti upovedomí zodpovednú osobu, ako aj odosielateľa predmetnej elektronickej pošty. V žiadnom prípade zavírenú elektronicкую poštu neposiela inému adresátovi a na svojej pracovnej stanici ju zmaže – odstráni a priečinok „Odstránená pošta“ vyprázdni.

### 3.8 ZAZNAMENÁVANIE A HLÁSENIE PROBLÉMOV S PRACOVNOU STANICOU

1. Používateľ IS používajúci pracovnú stanicu zaznamená a zodpovednej osobe bezodkladne ohlásí každú vnímateľnú odchýlku od bežnej činnosti pracovnej stanice, predovšetkým však nasledovné udalosti:
  - a) hlásenia chýb operačného systému a aplikácií, s ktorými používateľ pracuje (presný prepis chybového hlásenia) spolu so stručným popisom situácie (vykonávaných akcií), počas ktorej sa toto hlásenie vyskytlo, problémy s technickými zariadeniami pracovnej stanice spolu s popisom situácie, počas ktorej k problémom došlo (popis akcií, zadávaných údajov a/alebo viditeľných javov, ktoré predchádzali, resp. nasledovali výskytu problému).
2. Používateľ IS používajúci pracovnú stanicu zaznamená a svojmu nadriadenému a následne zodpovednej osobe bezodkladne ohlásí každú udalosť, ktorá by mohla indikovať porušenie bezpečnosti IS, predovšetkým však nasledovné udalosti:
  - a) výskyt vírusu (prepis varovného hlásenia),
  - b) únik údajov s informáciou, aké informácie unikli, kam a ako,
  - c) odcudzenie médií s údajmi z pracovnej stanice,
  - d) odcudzenie technických zariadení pracovnej stanice,
  - e) neoprávnený zásah do technických zariadení pracovnej stanice,
  - f) neoprávnený zásah do programového vybavenia pracovnej stanice (vrátane výskytu nových súborov alebo adresárov na disku pracovnej stanice) alebo do nastavenia jeho parametrov (napr. nastavené zdieľanie disku alebo adresárov pracovnej stanice)
3. Vyššie uvedené zásady platia aj v prípade, že používateľ IS dočasne používa pracovnú stanicu pridelenú inému používateľovi. V takom prípade navyš informuje aj používateľa, ktorému bola pracovná stanica



KLUB SLOVENSKÝCH TURISTOV	<u><i>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</i></u>	STRANA: 11/24
------------------------------	---	---------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

pridelená. V prípade podozrenia z poškodenia alebo neoprávnenej manipulácie s osobnými údajmi a nemožnosti postupu podľa tejto smernice postupuje podľa Havarijného plánu pracovísk.

4. Používateľ IS informuje zodpovednú osobu a svojho nadriadeného aj v prípade, keď má podozrenie, že súčasný stav umožňuje narušenie bezpečnosti alebo funkčnosti IS.
5. Používatelia IS sú povinní spolupracovať so zodpovednou osobou a ňou prizvaným externým špecialistom pri objasňovaní príčin výskytu bezpečnostných problémov, aby mohli byť následne vykonané opatrenia, ktoré by zabránili výskytu podobnej situácie.

### 3.9 PRÍSTUP DO SIETE INTERNET

1. Každý používateľ IS, ktorému bol umožnený prístup do siete Internet, je povinný rešpektovať nasledovné zásady:
  - a) prístup do siete Internet využívať predovšetkým v súlade so svojou pracovnou náplňou
  - b) svojou činnosťou v sieti Internet reprezentuje nielen seba, ale aj pracovisko prevádzkovateľa, ktoré mu prístup do siete umožnilo. Je preto povinný rešpektovať etické zásady platné v Internete a zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena pracoviska alebo k iným škodám,
  - c) komunikácia v Internete (napríklad elektronická pošta) spravidla nie je chránená pred „odpočúvaním“. V prípade potreby prenosu dôverných údajov sieťou Internet, je nevyhnutné tieto riadne zabezpečiť ich zašifrovaním,
  - d) Internet je bohatým zdrojom nielen informácií, ale aj rôznych programov. Pre získavanie programového vybavenia a jeho použitie na počítačových systémoch pracoviska platia rovnaké pravidlá ako pre ostatné programové vybavenie (*Základné zásady pre manipuláciu s programovým vybavením IS*).



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 12/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## 4.ZÁSADY GDPR BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ IS

### 4.1 VŠEOBECNÉ USTANOVENIA

1. Táto časť smernice upravuje základné pravidlá pre zaistenie bezpečnosti databáz IS a aplikácií informačných systémov (IS) na pracovisku prevádzkovateľa.
2. Bezpečnosť databáz IS a aplikácií IS prevádzkovateľa zabezpečujú samotní používatelia IS v spolupráci so zodpovednou osobou.

### 4.2 PODMIENKY ZAKLADANIA DATABÁZ OSOBNÝCH ÚDAJOV V IS

1. Zoznam databáz IS osobných údajov, ktoré sa pracujú u prevádzkovateľa, a vymedzenie účelu ich spracovania tvorí samostatnú časť: **Záznamy o spracovateľských činnostiach**, ktoré sú uschované u zodpovednej osoby.
2. Vznik novej databázy IS podlieha súhlasu štatutára prevádzkovateľa.
3. Databáza IS môže vzniknúť na základe splnomočujúcich ustanovení zákona alebo potreby plniť úlohy prevádzkovateľa, riadiacich aktov. V prípade, že na spracovanie osobných údajov nejestvuje splnomočujúce ustanovenie zákona, musí byť k tomuto spracovaniu zabezpečený súhlas dotknutých osôb v súlade s príslušným predpisom a v prípade ich nespôsobilosti na právne úkony, súhlas ich zákonných zástupcov.
4. Povinnosti podľa ods.3 nepodliehajú:
  - a) databázy IS pozostávajúce z titulu, mena, priezviska a adresy dotknutej osoby na účely poštového styku,
  - b) údaje na štatistické účely, ak sa zabezpečí ich anonymizovanie,
  - c) údaje na historické alebo vedecké účely spracovávané prevádzkovateľom,
  - d) už zverejnené osobné údaje, ak sú náležite označené a ich spracovateľ dokáže preukázať ich zverejnenie,
  - e) osobné údaje, ktoré sú súčasťou platnej zmluvy, kde dotknutá osoba je jednou zo zmluvných strán a jej podpis sa považuje za súhlas na spracovávanie osobných údajov.
5. O vzniku databázy IS jej používateľ informuje zodpovednú osobu, ktorá zaeviduje databázu IS do zoznamu spracovateľských činností prevádzkovateľa a preverí bezpečnosť systému, ktorý má databázu spracovávať ešte pred začatím spracovávania databázy. Zodpovedná osoba v prípade nedostatkov vykoná opatrenia na zabezpečenie informačnej bezpečnosti spracovávaných údajov. Vstupnú kontrolu systému zapíše do prevádzkového denníka príslušného IS.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 13/24
------------------------------	--	---------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

#### 4.3 ZÁKLADNÉ ZÁSADY BEZPEČNOSTI PRI SPRÁVE DATABÁZ A APLIKÁCIÍ

1. Používatelia vedú prevádzkový denník príslušného IS, resp. aplikácie, do ktorého zaznamenávajú podstatné udalosti súvisiace s databázou IS, resp. aplikáciou a jej bezpečnosťou. Do prevádzkového denníka sa zaznamenávajú predovšetkým nasledovné udalosti:
  - a) zistené chyby a odchýlky od správnej alebo požadovanej činnosti databázy IS alebo aplikácie
  - b) opravy a úpravy databázy IS alebo aplikácie, vrátane inštalácie novej verzie príslušného programového vybavenia
  - c) zmenu prístupového hesla používateľa
  - d) bezpečnostné incidenty
  - e) preverka (vyhodnotenie záznamov) prevádzkového denníka

Do prevádzkového denníka sa zapisujú minimálne nasledovné údaje:

- dátum a čas výskytu zaznamenávanej udalosti
  - stručný, výstižný a zrozumiteľný popis zaznamenávanej udalosti
  - popis postupu (riešenia), resp. prijatých opatrení
  - jednoznačná identifikácia osoby, ktorá vykonala záznam
2. Používatelia v spolupráci so zodpovednou osobou zabezpečujú systematické zálohovanie údajov databázy IS, resp. aplikácie. V odôvodnených prípadoch realizujú zálohovanie nad rámec obvyklého systematického zálohovania.
  3. Používatelia môžu realizovať zálohovanie údajov na lokálny disk pracovnej stanice iba ako núdzové riešenie a jedine za predpokladu dostatočného zabezpečenia predmetnej pracovnej stanice.
  4. Používatelia vedú prehľadnú evidenciu pridelených, zmenených a odňatých prístupových práv k predmetnej databáze IS, resp. aplikácie.
  5. Používatelia sú povinní pri svojej práci rešpektovať zásadu, podľa ktorej sa vyššie privilégia pre prácu s databázou IS, resp. aplikáciou využívajú iba na výkon činností, ktoré nie je možné vykonať s nižšími právami.
  6. Používateľ je povinný pri dlhodobom opustení miestnosti, v ktorej je uložená jemu pridelená pracovná stanica, odhlásiť sa zo systému. V prípade krátkodobého opustenia miestnosti musí aspoň aktivovať šetrič obrazovky s heslom na jeho odblokovanie.
  7. V prípade akokoľvek dlhého opustenia miestnosti zabezpečí uzamknutím dvere miestnosti, v prípade, že v miestnosti neostal iný pracovník. V prípade, že pracovník opúšťa miestnosť na prízemí a v miestnosti neostáva iný pracovník, zabezpečí zatvorenie okna.
  8. V prípade zistenia výskytu bezpečnostného incidentu súvisiaceho s príslušnou databázou alebo aplikáciou používatelia IS bezodkladne informujú zodpovednú osobu, s ktorou tiež konzultujú postup riešenia incidentu a taktiež spolupracujú pri zdokumentovaní incidentu a jeho riešenia.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 14/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

9. Používatelia IS sú povinní po inštalácii novej verzie programového vybavenia príslušnej databázy IS alebo aplikácie IS po dobu minimálne dvoch týždňov venovať zvýšenú pozornosť činnosti databázy IS, resp. aplikácie IS a vykonávať kontroly správnosti. Prípadné odchýlky od požadovaného stavu sú povinní čo najúplnejšie zdokumentovať a bezodkladne ohlásiť zodpovednej osobe.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 15/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## 5. ZÁSADY GDPR BEZPEČNOSTI PRI PREVÁDZKE INFORMAČNÝCH A KOMUNIKAČNÝCH TECHNOLOGIÍ NA PRACOVISKU IS

### 5.1 VŠEOBECNÉ USTANOVENIA

1. Táto časť smernice upravuje základné pravidlá pre zaistenie bezpečnej a spoľahlivej prevádzky informačných a komunikačných technológií informačných systémov (IS) na pracovisku prevádzkovateľa.
2. Prevádzku informačných a komunikačných technológií IS na pracovisku prevádzkovateľa, zabezpečuje zodpovedná osoba, resp. štatutár prevádzkovateľa prostredníctvom poverenej osoby.

### 5.2 KLÚČOVÉ KOMPONENTY IS

1. Pre účely tejto smernice kľúčové komponenty IS prevádzkovateľa sú tie technické a programové prostriedky a dokumenty, ktorých poškodenie, zlyhanie alebo neoprávnená manipulácia nimi môže mať za následok ohrozenie spoľahlivej a bezpečnej prevádzky IS. Medzi kľúčové komponenty patria systémové a aplikačné programové vybavenie používané v rámci IS prevádzkovateľa, pamäťové médiá obsahujúce záložné kópie údajov IS, inštalčné médiá pre základné a aplikačné programové vybavenie IS, zoznam prístupových hesiel pre použitie v prípade neprítomnosti príslušných používateľov IS a podobne.
2. Prístup ku kľúčovým komponentom IS prevádzkovateľa má len zodpovedná osoba, resp. štatutár prevádzkovateľa, resp. štatutárom poverená osoba.
3. Upratovanie a podobné práce v miestnostiach, kde sú uložené kľúčové komponenty IS, sa podľa možnosti vykonávajú s ohľadom na tieto komponenty. Osoby vykonávajúce zmienené práce musia byť vopred riadne poučené o zákaze akokoľvek manipulovať s elektronickými zariadeniami bez predchádzajúceho súhlasu zodpovednej osoby, resp. štatutára, resp. štatutárom poverenej oprávnenej osoby.

### 5.3 ZÁKLADNÉ ZÁSADY BEZPEČNEJ PREVÁDZKY IS

1. Opravy a úpravy a akýkoľvek zásah na všetkých komponentoch IS môžu vykonávať len kvalifikované osoby – externí špecialisti konajúci na základe platného, vopred daného poverenia. Všetky opravy a úpravy musia byť primerane zdokumentované.
2. Pri odstraňovaní porúch kľúčových komponentov IS je zodpovedná osoba, resp. štatutárom poverená oprávnená osoba na základe požiadavky externého špecialistu oprávnená vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre odstránenie poruchy.
3. Na staniciach PC s IS je zakázané inštalovať a prevádzkovať programové vybavenie získané nelegálnym spôsobom, resp. porušujúce platné licenčné podmienky.
4. Zodpovedná osoba, resp. štatutárom poverená oprávnená osoba vedie prevádzkový denník IS, do ktorého sa zaznamenávajú podstatné udalosti súvisiace so systémom, jeho prevádzkou a bezpečnosťou. Do prevádzkového denníka sa zaznamenávajú predovšetkým nasledovné udalosti:



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 16/24
------------------------------	--	---------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

- poruchy na kľúčových komponentoch IS (vrátane komunikácie v sieti a porúch v dodávke elektrickej energie na pracovisko)
- opravy, úpravy a zásahy do kľúčových komponentov IS
- zmeny prístupových hesiel privilegovaných používateľov (napr. správca systému)
- vykonanie preventívnej prehliadky a testovania systému alebo jeho komponentov (vrátane kontroly čitateľnosti médií so záložnými kópiami IS pracoviska)
- inštalovanie novej verzie základného alebo aplikačného programového vybavenia
- bezpečnostné incidenty (vrátane výskytu počítačového vírusu)
- previerka (vyhodnotenie záznamov) prevádzkového denníka.

Do prevádzkového denníka sa zapisujú minimálne nasledovné údaje:

- dátum a čas výskytu zaznamenávanej udalosti
- stručný, výstižný a zrozumiteľný popis zaznamenávanej udalosti
- popis postupu (riešenia), resp. prijatých opatrení
- jednoznačná identifikácia osoby, ktorá vykonala záznam

- Prístupové práva používateľov IS pridáva, mení a odníma iba zodpovedná osoba, štatutár, resp. štatutárom poverená oprávnená osoba.
- Zodpovedná osoba, štatutár, resp. štatutárom poverená oprávnená osoba sú povinní pri svojej práci rešpektovať zásadu, podľa ktorej sa vyššie privilégia pre prácu so systémom využívajú iba na výkon činností, ktoré nie je možné vykonať s nižšími právami.
- Prístupové heslá, ktoré boli v oprávnených prípadoch (predvádzanie funkcií systému, servisné zásahy a podobne) dočasne prepožičané externým subjektom, je potrebné po ukončení dôvodu ich prepožičania bezodkladne zmeniť tak, aby externé subjekty neboli oboznámené s novými prístupovými heslami.
- V prípade vyradovania počítačových systémov a médií z pracoviska sú používatelia IS v spolupráci s externým špecialistom povinní zabezpečiť dôkladnú likvidáciu údajov IS na vyradovaných zariadeniach a médiách.

#### 5.4 ZÁLOHOVANIE

- Kompletný systém samostatne používaných pracovných staníc (počítačov) je potrebné zálohovať tak, aby bolo možné v prípade potreby rýchlo obnoviť základné a aplikačné programové vybavenie, konfiguračné súbory, štruktúru súborového systému a všetky podstatné parametre systému potrebné pre rutinnú prevádzku.
- Všetky médiá so záložnými kópiami údajov a programového vybavenia musia byť označené tak, aby označenie jednoznačne určovalo aktuálny obsah média a taktiež, aby bolo možné určiť dátum vytvorenia záložnej kópie na predmetnom médiu.
- Zodpovedná osoba, resp. štatutárom poverená oprávnená osoba v spolupráci s externými špecialistami je povinná aspoň dvakrát ročne overiť bezporuchovosť (schopnosť zapisovať a korektne prečítať zapísané údaje) zálohovacieho zariadenia a aspoň tretiny médií používaných pre záložné kópie údajov a v prípade



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 17/24
------------------------------	--	---------------

Dátum 1. vydania: 25.5.2018	Spracoval: PK-Systems, s. r. o.	Schválili (funkcia): Predseda klubu	Vydané dňa: 25.5.2018
--------------------------------	------------------------------------	--	--------------------------

zistenej zníženej spoľahlivosti bezodkladne overiť všetky médiá a vykonať nápravné opatrenia (kvalitná oprava alebo náhrada zálohovacieho zariadenia, náhrada médií).

4. Pokiaľ je to technicky možné, médiá so záložnými kópiami údajov a programového vybavenia sa skladujú zásadne v stave zabráňujúcom zapisovanie na médium.

### 5.5 ZÁSADY RIEŠENIA NEPREDVÍDANÝCH UDALOSTÍ S DOPADOM NA PREVÁDZKU IS

1. V prípade nepredvídanej situácie ohrozujúcej prevádzku IS alebo údaje IS prevádzkovateľa sú zodpovedná osoba, resp. štatutárom poverená oprávnená osoba a ňou poverení externí špecialisti povinní pri riešení súvisiacich problémov zaistiť primeranú ochranu všetkých komponentov systému obsahujúcich citlivé údaje IS pracoviska pred prístupom neoprávnených osôb.
2. V prípade nepredvídanej situácie je zodpovedná osoba, resp. štatutár, resp. štatutárom poverená oprávnená osoba vyhlásiť technickú prestávku na nevyhnutný čas potrebný pre riešenie udalosti.
3. Externí špecialisti na základe žiadosti zodpovednej osoby, resp. štatutárom poverenej oprávnenej osoby organizujú priebežné testovanie a aktualizáciu plánu postupu pre prípad nepredvídaných udalostí.

### 5.6 ZÁSADY RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV

1. V prípade výskytu bezpečnostného incidentu zodpovedná osoba, resp. štatutárom poverená oprávnená osoba bezodkladne informuje štatutára a kontaktuje príslušného Externého špecialistu.
2. Riešenie každého bezpečnostného incidentu musí byť primerane z dokumentové.
3. Zodpovedná osoba a privolaný externý špecialista sa pri riešení bezpečnostného incidentu riadia nasledovnými prioritami:
  - a) bezodkladné obnovenie bežnej prevádzky IS aspoň v redukovanom režime, zabezpečenie ochrany údajov IS pracoviska, zachovanie dôkazového materiálu nevyhnutného na ďalšiu analýzu príčin vzniku bezpečnostného incidentu
  - b) zistenie príčin, ktoré viedli k vzniku bezpečnostného incidentu
  - c) určenie zodpovednosti za vznik bezpečnostného incidentu a vyvodenie dôsledkov
  - d) zovšeobecnenie zistených skutočností a návrh opatrení na zabránenie opakovanému výskytu bezpečnostného incidentu



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 18/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

### 5.7 PREVENCIA ZODPOVEDNÁ OSOBA RESP. ŠTATUTÁROM POVERENÁ OPRÁVNENÁ OSOBA V SPOLUPRÁCI S EXTERNÝM ŠPECIALISTOM JE POVINNÁ:

1. Minimálne raz ročne vykonať základnú preventívnu kontrolu kľúčových komponentov IS (testovanie systému, odstránenie nepotrebných súborov, posúdenie rýchlosti zapíňania pamätevej kapacity, množstvo a vek životnosti médií používaných na zálohovanie, preverka na výskyt nových programov v systéme, vyčistenie komponentov systému a podobne).
2. Pravidelne, minimálne raz za pol roka, vykonať základnú preventívnu kontrolu zameranú na preverenie funkčnosti komponentov nevyhnutných pre riešenie nepredvídaných situácií (zariadenie pre zálohovanie a obnovu údajov, médiá so záložnými kópiami údajov a programov, aktuálnosť zálohovaných prístupových hesiel).
3. Pomáhať používateľom IS riešiť problémy, ktoré sa objavia pri práci so systémom. V prípade opakovaného výskytu problémov z dôvodu nedostatočnej kvalifikácie alebo schopnosti používateľa pracovať s IS, upozorniť priamo nadriadeného príslušného používateľa na zistené nedostatky a potrebu nápravy.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 19/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## 6. INFORMAČNÁ POVINNOSŤ PREVÁDZKOVATEĽA DOTKNUTÝM OSOBÁM PODĽA GDPR

### 6.1 INFORMÁCIE, KTORÉ SA MAJÚ POSKYTOVAŤ PRI ZÍSKAVANÍ OSOBNÝCH ÚDAJOV OD DOTKNUTEJ OSOBY

1. V prípadoch, keď sa od dotknutej osoby získavajú osobné údaje, ktoré sa jej týkajú, poskytnie prevádzkovateľ pri získavaní osobných údajov dotknutej osobe všetky tieto informácie:
  - a) kontaktné údaje prípadnej zodpovednej osoby;
  - b) právny základ spracúvania, a ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany;
  - c) o dobe uchovávaní osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
  - d) konkretizácia práv dotknutej osoby, a to:
    - a. práva na ich opravu
    - b. práva na vymazanie
    - c. právo na obmedzenie spracovania
    - d. právo na prenos osobných údajov
    - e. právo namietať proti spracovaniu
    - f. existencia automatizovaného rozhodovania vrátane profilovania
  - e) ak je spracúvanie založené na súhlase, existencia práva kedykoľvek svoj súhlas odvolať;
  - f) právo podať sťažnosť na úrad;
  - g) informácia o tom, či je poskytovanie osobných údajov zákonnou alebo zmluvnou požiadavkou, alebo požiadavkou, ktorá je potrebná na uzavretie zmluvy, či je dotknutá osoba povinná poskytnúť osobné údaje, ako aj možné následky neposkytnutia takýchto údajov;
2. Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli získané, poskytnie dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a ďalšie relevantné informácie uvedené v odseku 1.

### 6.2 INFORMÁCIE, KTORÉ SA MAJÚ POSKYTNÚŤ, AK OSOBNÉ ÚDAJE NEBOLI ZÍSKANÉ OD DOTKNUTEJ OSOBY

1. Ak osobné údaje neboli získané od dotknutej osoby, prevádzkovateľ poskytnie dotknutej osobe tieto informácie:
  - a) kategórie dotknutých osobných údajov;
  - b) kontaktné údaje prípadnej zodpovednej osoby;
  - c) právny základ spracúvania; a ak sa spracúvanie zakladá na článku 6 ods. 1 písm. f) nariadenia aj oprávnené záujmy prevádzkovateľa alebo tretej strany;
  - d) doba uchovávaní osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
  - e) konkretizácia práv dotknutej osoby, a to:
    - a. práva na ich opravu
    - b. práva na vymazanie
    - c. právo na obmedzenie spracovania



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 20/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

- d. právo na prenos osobných údajov
- e. právo namietať proti spracovaniu
- f. existencia automatizovaného rozhodovania vrátane profilovania
- f) ak je spracúvanie založené na súhlase, existencia práva kedykoľvek svoj súhlas odvolať;
- g) právo podať sťažnosť na úrad;
- h) z akého zdroja pochádzajú osobné údaje, prípadne informácie o tom, či údaje pochádzajú z verejne prístupných zdrojov;

2. Ak má prevádzkovateľ v úmysle ďalej spracúvať osobné údaje na iný účel ako ten, na ktorý boli osobné údaje získané, poskytne dotknutej osobe pred takýmto ďalším spracúvaním informácie o tomto inom účele a akékoľvek ďalšie relevantné informácie uvedené v odseku 1.

### 6.3 PRÁVO DOTKNUTEJ OSOBY NA PRÍSTUP K ÚDAJOM

1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:
  - a) účely spracúvania;
  - b) kategórie dotknutých osobných údajov;
  - c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie
  - d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
  - e) existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu;
  - f) právo podať sťažnosť dozornému orgánu;
  - g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj;
  - h) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použítom postupe, ako aj význam a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.
2. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.
3. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.
4. Právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 21/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## 6.4 SPÔSOB POSKYTOVANIA ŽIADOSTI DOTKNUTEJ OSOBY

Prevádzkovateľ poskytovania informácií dotknutej osobe:

1. Musí byť stručne, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho.
2. Písomne, elektronicky alebo inými prostriedkami alebo na požiadanie ústne (*ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa podľa možnosti poskytnú elektronickými prostriedkami, pokiaľ dotknutá osoba nepožiadala o iný spôsob*);
3. Poskytnutie oznámení o prijatých opatreniach bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti (*v obzvlášť zložitých prípadoch možnosť predĺžiť o ďalšie dva mesiace, kedy sa informácia poskytne ešte za plynutia pôvodnej lehoty*);
4. Ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť na úrad a uplatniť súdny prostriedok nápravy;
5. Bezplatné poskytovanie informácií a oznámení, v osobitných prípadoch možnosť účtovať primeraný poplatok;
6. Oprávnenie prevádzkovateľa žiadať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby;
7. Prevádzkovateľ nemôže odmietnuť konať na základe žiadosti dotknutej osoby pri výkone jej práva, pokiaľ nepreukáže, že dotknutú osobu nie je schopný identifikovať;
8. Poskytnutie dotknutej osobe informácie o opatreniach bez zbytočného odkladu, nie neskôr ako do jedného mesiaca od doručenia žiadosti (*v rámci lehoty je potrebné oznámiť prípadné predĺženie lehoty o ďalšie dva mesiace v prípade obzvlášť zložitých prípadov*), ak prevádzkovateľ neprijme opatrenia na základe žiadosti dotknutej osoby, bezodkladne a najneskôr do jedného mesiaca od doručenia žiadosti informuje dotknutú osobu o dôvodoch nekonania a o možnosti podať sťažnosť úradu a uplatniť súdny prostriedok nápravy;
9. Bezodplatné poskytnutie oznámení, s výnimkou neopodstatnených alebo neprímeraných, najmä opakujúcich žiadostí (*právo požadovať náhradu administratívnych nákladov; prípadne nekonať*);
10. Právo prevádzkovateľa požadovať o poskytnutie dodatočných informácií potrebných na potvrdenie totožnosti dotknutej osoby.



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 22/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

## 6.5 PODMIENKY VYJADRENIA SÚHLASU ZO SPRACOVANÝM OSOBNÝCH ÚDAJOV

1. Ak je spracúvanie založené na súhlase, prevádzkovateľ musí vedieť preukázať, že dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov.
  - a) súhlas by sa mal poskytnúť jasným prejavom vôle, ktorý je slobodným, konkrétnym, informovaným a jednoznačným vyjadrením súhlasu dotknutej osoby so spracúvaním osobných údajov, ktoré sa jej týkajú (napríklad prostredníctvom elektronických prostriedkov alebo ústnym vyhlásením alebo označením políčka pri návšteve internetového webového sídla; v tejto súvislosti dávame do pozornosti, že políčko nesmie byť vopred označené);
  - b) súhlas sa má vzťahovať na všetky spracovateľské činnosti vykonávané na ten istý účel alebo účely;
  - c) ak sa spracúvanie vykonáva na viaceré účely, súhlas sa má udeliť/má byť oddelený/uvedený oddelene na všetky tieto účely;
  - d) udelenie súhlasu musí byť jasne odlišiteľné od iných skutočností, so súhlasom na spracúvanie osobných údajov nesúvisiacich;
  - e) súhlas má byť formulovaný v zrozumiteľnej a ľahko dostupnej forme, jasne a jednoducho;
  - f) informovanie o možnosti súhlas odvolať musí byť také jednoduché, ako poskytnutie súhlasu;
  - g) zákaz podmieňovať súhlas so spracúvaním osobných údajov, ktorý nie je na plnenie zmluvy, vrátane poskytnutia služby, nevyhnutný;

## 6.6 OSOBITNÉ KATEGÓRIE OSOBNÝCH ÚDAJOV

1. Zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a 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.
2. Odsek 1 sa neuplatňuje, ak platí niektorá z týchto podmienok:
  - a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov
  - b) spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby;
  - c) spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas;
  - d) spracúvanie vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu;



KLUB SLOVENSKÝCH TURISTOV	<u>Smernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov</u>	STRANA: 23/24
------------------------------	--	---------------

Dátum 1. vydania:	Spracoval:	Schválili (funkcia):	Vydané dňa:
25.5.2018	PK-Systems, s. r. o.	Predseda klubu	25.5.2018

- e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;
- f) spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc;
3. Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor (*rodne číslo – „nepatri do osobitnej kategórie OU,“*) ustanovený osobitným zákonom len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania a zároveň dotknutá osoba dala písomný alebo inak hodnoverne preukázateľný súhlas na jeho spracúvanie; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný zákon, alebo ak spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa. **Zverejňovať všeobecne použiteľný identifikátor (rodne číslo) sa zakazuje.**

## 6.7 KOPÍROVANIE, SKENOVANIE A ZAZNAMENÁVANIE ÚRADNÝCH DOKLADOV VŠEOBECNE

- Poverené osoby prevádzkovateľa získavajú osobné údaje kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov len v nevyhnutnom rozsahu.
- Jedná sa najmä o nasledovné úradné doklady:
  - cestovný pas,
  - vodičský preukaz,
  - rodný list,
  - sobášny list,
  - preukaz ZŤP občana,
  - rozhodnutie o priznaní dôchodku a pod.
- Je zakázané** kopírovať, skenovať občiansky preukaz a kartičku poistenca dotknutej osoby.
- Poskytnutím takéhoto dokladu sa prevádzkovateľovi môžu dostať do informačného systému aj osobné údaje, ktoré spravidla svojim rozsahom aj obsahom idú nad rámec daného účelu spracovania. Preto je oprávnená osoba povinná kopírovať iba tie údaje, resp. tie časti osobného dokladu, ktoré nevyhnutne potrebuje na dosiahnutie daného účelu spracúvania (napr. **prekrytím nepotrebných údajov, alebo začiaŕkať takéto údaje , aby neboli čitateľne** ).
- Ak poverené osoby spracúvajú uvedené kópie úradných dokladov v informačnom systéme je k tomu nevyhnutný písomný súhlas dotknutej osoby. Iba v prípadoch kedy tento spôsob získavania osobných údajov oprávnenej osobe prevádzkovateľa vyslovene umožňuje osobitný zákon smie oprávnená osoba postupovať bez súhlasu dotknutej osoby.
- Poverená osoba si súhlas nesmie vynucovať. V prípade ak dotknutá osoba nesúhlasí s vyhotovením kópie jej úradného dokladu, oprávnená osoba vyhotoví odpis.



KLUB SLOVENSKÝCH  
TURISTOVSmernica podľa Všeobecného nariadenia o ochrane osobných údajov (GDPR) a Zákona o ochrane osobných údajov

STRANA: 24/24

Dátum 1. vydania:

25.5.2018

Spracoval:

PK-Systems, s. r. o.

Schválili (funkcia):

Predseda klubu

Vydané dňa:

25.5.2018

**6.8 SPRÁVNOSŤ A AKTUÁLNOŠŤ OSOBNÝCH ÚDAJOV**

1. Osobný údaj sa považuje za správny, kým sa nepreukáže opak.
2. Správnosť a aktuálnosť osobných údajov zabezpečuje prevádzkovateľ a to:
  - a) zmluvným záväzkom osôb, ktoré osobné údaje do informačného systému poskytujú, že sú povinné v prípade akejkoľvek zmeny túto zmenu prevádzkovateľovi v primeranej lehote oznámiť.

**6.9 LIKVIDÁCIA OSOBNÝCH ÚDAJOV**

1. Oprávnená osoba po splnení účelu spracovávania osobných údajov, zabezpečí bezodkladne likvidáciu tých osobných údajov, u ktorých bol účel ich spracovávania splnený.
2. Poverené osoby, sú povinné pri likvidácii osobných údajov vykonať ich likvidáciu tak, aby tieto údaje sa stali nečitateľnými a nemohli byť zneužitú inou neoprávnenou osobou. Pri automatizovanom spracovaní ich vymazaním z dát súboru informačného systému (subsystému), pri manuálnej podobe ich skartovaním.
3. Dokumenty s osobnými údajmi ktoré nie sú zaradené do registratúry, alebo po uplynutí doby uloženia (zákon č. 395/2002 Z.z.) sa likvidujú fyzickou likvidáciou.

**6.10 ČO JE OSOBNÝ ÚDAJ**

1. Akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby.
2. Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.
3. Online identifikátory - IP adresa, cookies, MAC adresa, geolokalizačné údaje, logy a iné informácie získavané zo serverov.
4. Anonymizované údaje - ak sa nedá spätne určiť dotknutá osoba, nespádajú pod GDPR.
5. Pseudonymizované údaje - považujeme za osobný údaj, pretože umožňujú identifikáciu osoby, hoci s použitím kľúča = bezpečnostné opatrenie.