

<b>MARATÓNSKY KLUB KOŠICE (MKK)</b>
Pri jazdiarni 1, 043 04 Košice
IČO: 00595209; DIČ: 2020 777 682; IČ DPH: SK2020 777 682
<p><b>SMERNICA č. MKK / 02 – 2019</b>  o riešení bezpečnostných incidentov  Táto smernica stanovuje postupy pri riešení bezpečnostných incidentov v oblasti ochrany osobných údajov spracúvaných MKK.</p>

Spracoval/a	G & Partners	Podpísal	Ing. Ján Sudzina, prezident MKK
Počet strán	4	Počet príloh	0
Účinnosť od	30.4.2019	Dátum schválenia Správnou radou MKK	30.4.2019

## Čl. 1

### Pôsobnosť a účel

Smernica upravuje pravidlá, postupy riešenia a ohlasovania bezpečnostných incidentov prevádzkovateľa, vymedzuje základné pojmy súvisiace s ohlasovaním bezpečnostných incidentov v zmysle čl. 33 a nasl. Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „Nariadenie“) a zákona NR SR č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“).

**Táto Smernica svojim obsahom nadväzuje na Smernicu o ochrane osobných údajov, ktorú prijal prevádzkovateľ v rámci implementácie bezpečnostnej dokumentácie o ochrane osobných údajov.**

Prevádzkovateľ musí mať prijaté personálne, organizačné a technické opatrenia pre zachovanie integrity, dôvernosti a dostupnosti spracúvaných osobných údajov. Len tak možno minimalizovať riziko vzniku bezpečnostného incidentu.

## Čl. 2

### Vymedzenie základných pojmov

- a) **Osobné údaje** – sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (dotknutej osoby). 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.
- b) **Osobitná kategória osobných údajov** – sú osobné údaje, 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 sexuálneho života či sexuálnej orientácie fyzickej osoby.
- c) **Prevádzkovateľ** - prevádzkovateľom informačného systému, resp. spracovateľom osobných údajov v rámci rôznych účelov spracúvania je Maratónsky klub Košice, Pri Jazdiarni 1, 04304 Košice, IČO: 00595209.
- d) **Oprávnená osoba** – zamestnanci určení štatutárnym zástupcom Maratónskeho klubu Košice, Pri Jazdiarni 1, 043 04 Košice, IČO: 00595209 na základe preukázateľného písomného poverenia.
- e) **Spracúvanie osobných údajov** – je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami.
- f) **Porušenie ochrany osobných údajov - bezpečnostný incident** – porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú alebo neoprávnený prístup k nim.
- g) **Informačný systém** – je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe.

## Čl. 3

### Postup pri ohlasovaní bezpečnostných incidentov na Úrad na ochranu osobných údajov SR

1) Všetky bezpečnostné incidenty je potrebné bezodkladne, najneskôr však do 3 hodín od momentu, od ktorého sa o ňom dozvedel zamestnanec prevádzkovateľa (nie len oprávnená osoba) alebo akákoľvek iná tretia osoba oznámiť osobe poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, a to Miriam Kopcsayová, sekretariát Maratónskeho klubu Košice – viď Príloha č. 1 – Oznámenie bezpečnostného incidentu.

2) Sprostredkovateľ je povinný oznámiť porušenie ochrany osobných údajov bez zbytočného odkladu prevádzkovateľovi po tom, ako sa o ňom dozvedel!

3) Osoba poverená na riešenie porušenia ochrany osobných údajov – bezpečnostných incidentov – po jeho nahlásení posúdi, či došlo k narušeniu dôvernosti, integrity a dostupnosti osobných údajov a súčasne či sa jedná o porušenie ochrany osobných údajov s poukazom na porušenie práv a slobôd fyzických osôb.

Príklad č. 1: Zamestnanec spoločnosti, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov, klientov, žiakov, pacientov a podobne) stratí USB kľúč, na ktorom sa nachádzajú všetky ním spracúvané databázy obsahujúce osobné údaje:

- a) pokiaľ by bol USB kľúč zabezpečený šifrovaním, teda ten, kto ho nájde by sa bez špeciálneho šifrovacieho kľúča nemohol dostať k jeho obsahu a zároveň má zamestnanec uloženú celú túto databázu aj vo svojom firemnom počítači, teda stratou USB kľúča by o ňu neprišiel – porušenie ochrany osobných údajov pravdepodobne nepovedie k riziku pre práva a slobody fyzických osôb – nie je potrebné hlásiť na Úrad na ochranu osobných údajov,
- b) pokiaľ by nebol USB kľúč zabezpečený šifrovaním, teda ten, kto ho nájde by sa bez väčších problémov dostal k jeho obsahu a ak aj zároveň má zamestnanec uloženú celú túto databázu aj vo svojom firemnom počítači, teda stratou USB kľúča by o ňu neprišiel – porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzických osôb – je potrebné hlásiť na Úrad na ochranu osobných údajov a oznámiť túto skutočnosť dotknutým osobám v zmysle Čl. 5 tejto Smernice.

Príklad č. 2: Zamestnanec spoločnosti, ktorý je oprávnenou osobou a teda spracúva osobné údaje dotknutých fyzických osôb (ostatných zamestnancov, klientov, žiakov, pacientov a podobne) si vezme prácu na doma. Cestou však stratí spisovú dokumentáciu, ktorú následne nájde náhodný okoloidúci. Spisová dokumentácia obsahuje osobné údaje fyzických osôb a jej stratou zamestnanec o túto prišiel – porušenie ochrany osobných údajov pravdepodobne povedie k riziku pre práva a slobody fyzických osôb – je potrebné hlásiť na Úrad na ochranu osobných údajov a oznámiť túto skutočnosť dotknutým osobám v zmysle Čl. 5 tejto Smernice.

4) Ak dôjde k naplneniu oboch podmienok súčasne, osoba poverená na riešenie porušenia ochrany osobných údajov – bezpečnostných incidentov – respektíve prevádzkovateľ, je povinný oznámiť túto skutočnosť Úradu na ochranu osobných údajov SR tak, aby lehota oznámenia, odkedy sa o tejto skutočnosti dozvedel, nepresiahla 72 hodín.

5) Porušenie ochrany osobných údajov sa nahlasuje online na predpísanom formulári Úradu na ochranu osobných údajov SR <https://dataprotection.gov.sk/uouu/sk/dp/dp-breach>, ktorý musí obsahovať tieto skutočnosti:

- a) Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,
- b) Popis porušenia ochrany osobných údajov a to: dátum a čas zistenia porušenia osobných údajov, dátum a čas začiatku a konca porušenia osobných údajov, popis povahy porušenia osobných údajov, popis kategórií dotknutých osôb, ktorých sa porušenie týka, približný počet dotknutých osôb, ktorých sa porušenie týka, popis kategórií záznamov, ktorých sa porušenie týka, približný počet záznamov, ktorých sa porušenie týka, popis pravdepodobných následkov porušenia,
- c) Popis nápravy porušenia ochrany osobných údajov – t.j. popis prijatých opatrení na nápravu porušenia ochrany osobných údajov ako aj opatrení na zmiernenie dopadu porušenia ochrany osobných údajov.

#### Čl. 4

##### Postup pri ohlasovaní bezpečnostných incidentov dotknutým fyzickým osobám

1) V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľa bez zbytočného odkladu v súlade s čl. 34 Nariadenia, oznámi porušenie ochrany osobných údajov dotknutej osobe. Oznámenie má obsahovať jasne

a jednoducho formulovaný opis porušenia, resp. zneužitia jej osobných údajov ako aj informácie o tom, aké opatrenia prijal prevádzkovateľ na ich odstránenie, či kontaktné údaje na prevádzkovateľa (zodpovednú osobu prevádzkovateľa), kde môže dotknutá osoba získať viac informácií.

2) Oznámenie dotknutej osobe sa nevyžaduje v prípadoch, ak prevádzkovateľ:

- a) prijal také opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, iba pre osoby oprávnené – napríklad šifrovanie,
- b) po zistení porušenia osobných údajov prijal také opatrenia, ktoré zabránili tomu, aby riziko pre práva a slobody dotknutých osôb ostalo vysoké,
- c) by musel vynaložiť na informovanie dotknutej osoby neprimerané úsilie. V tomto prípade by však aj napriek tomu malo dôjsť k informovaniu verejnosti formou verejného oznámia, aby zabezpečil, že dotknuté osoby budú efektívne informované.

## Čl. 5

### Evidencia porušení ochrany osobných údajov

- 1) Prevádzkovateľ je sám alebo prostredníctvom zodpovednej osoby alebo inej osoby poverenej na riešenie porušení ochrany osobných údajov – bezpečnostných incidentov, viesť evidenciu všetkých porušení, bez ohľadu na to, či porušením bolo spôsobené nízke, stredné alebo vysoké riziko alebo bez ohľadu na to, či bolo viazané na dotknuté osoby a ich osobné údaje.
- 2) Pokiaľ sa jedná o bezpečnostný incident, ktorý nesúvisí s touto Smernicou, ale napríklad s IT prostredím, je potrebné o tejto skutočnosti bezodkladne informovať príslušného zamestnanca prevádzkovateľa.
- 3) Evidencia porušení ochrany osobných údajov – bezpečnostných incidentov musí obsahovať:
  - a) Údaje o prevádzkovateľovi, u ktorého nastal únik osobných údajov,
  - b) Popis porušenia ochrany osobných údajov a to: dátum a čas zistenia porušenia osobných údajov, dátum a čas začiatku a konca porušenia osobných údajov, popis povahy porušenia osobných údajov, popis kategórií dotknutých osôb, ktorých sa porušenie týka, približný počet dotknutých osôb, ktorých sa porušenie týka, popis kategórií záznamov, ktorých sa porušenie týka, približný počet záznamov, ktorých sa porušenie týka, popis pravdepodobných následkov porušenia,
  - c) Popis nápravy porušenia ochrany osobných údajov – t.j. popis prijatých opatrení na nápravu porušenia ochrany osobných údajov ako aj opatrení na zmiernenie dopadu porušenia ochrany osobných údajov.
  - d) meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident vybavovala.
  - e) meno a priezvisko a funkcia osoby, ktorá bezpečnostný incident nahlásila.
  - f) dátum ukončenia vybavovania.

## Čl. 6

### Záverečné ustanovenie

Táto Smernica nadobúda účinnosť dňom 30.4.2019

V Košiciach, dňa 30.4.2019

.....  
**Ing, Ján Sudzina**  
**prezident Maratónskeho klubu Košice**

**Príloha č. 1 Oznámenie bezpečnostného incidentu**

I. Údaje o kontaktnej osobe/subjekte v ktorej nastal únik OU

<b>Titul, meno, priezvisko, titul</b>	
<b>Telefón, e-mail</b>	
<b>Názov prevádzkovateľa</b>	
<b>Sídlo prevádzkovateľa</b>	
<b>IČO</b>	
<b>Právna forma</b>	

II. Popis porušenia ochrany OU

<b>Dátum a čas zistenia porušenia ochrany OÚ</b>	
<b>Dátum a čas začiatku porušenia ochrany OÚ</b>	
<b>Dátum a čas konca porušenia ochrany OÚ</b>	
<b>Popis povahy porušenia ochrany OÚ</b>	
<b>Popis kategórií dotknutých osôb, ktorých sa porušenie týka</b>	
<b>Približný počet dotknutých osôb, ktorých sa porušenie týka</b>	
<b>Popis kategórií záznamov, ktorých sa porušenie týka</b>	
<b>Približný počet záznamov, ktorých sa porušenie týka</b>	
<b>Popis pravdepodobných následkov porušenia</b>	

III. Popis nápravy porušenia ochrany osobných údajov

<b>Popis prijatých opatrení na nápravu porušenia ochrany OÚ ako aj opatrení na zmiernenie dopadu porušenia ochrany OÚ</b>	
---	--

<b>Meno, priezvisko, funkcia osoby, ktorá bezpečnostný incident nahlásila</b>	
<b>Meno, priezvisko, funkcia osoby, ktorá bezpečnostný incident vybavovala</b>	
<b>Dátum ukončenia vybavovania</b>	