

# POSÚDENIE VPLYVU NA OCHRANU ÚDAJOV TÝKAJÚCE SA MERANIA TELESNEJ TEPLoty V SÚVISLOSTI S COVID-19

v súlade s článkom 35 článkom 13 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“)

## IDENTIFIKAČNÉ ÚDAJE A KONTAKTNÉ ÚDAJE PREVÁDZKOVATEĽA

Obchodné meno: **Základná škola s materskou školou**  
Sídlo: Školská 155/17, 034 91 Ľubochňa  
IČO: 37812971  
Kontakt: +421 444 391 229 ; zslubochna@centrum.sk  
Zodpovedná osoba: V prípade otázok, ktoré sa týkajú ochrany osobných údajov nás môžete kontaktovať na nasledujúcich kontaktných údajoch: Tel: +421915206025; Email: eva@holdosova.com

## 1. SYSTEMATICKÝ OPIS SPRACÚVANIA [článok 35 ods. 7 písm. a) GDPR]

### 1.1. Zohľadnenie povahy, rozsahu, kontextu a účelov spracúvania (odôvodnenie 90)

<b>Povaha</b>	Ide o spracúvanie osobitnej kategórie OÚ, resp. citlivých údajov?	<b>ÁNO</b>	Ide o získavanie údajov týkajúcich sa zdravia, konkrétne meranie telesnej teploty.
<b>Rozsah</b>	Ide o rozsiahle spracúvanie OÚ (vo veľkom rozsahu)?	<b>NIE</b>	
<b>Kontext</b>	Ide o obvyklé a primerane očakávané spracúvanie OÚ na danom právnom základe?	<b>ÁNO</b>	Počas obdobia zvýšeného rizika infekcie COVID-19, meranie telesnej teploty pri vstupe do budovy je obvyklé a primerane očakávané. RÚVZ SR to priamo nariadil pre nemocnice a priemyselné podniky.
<b>Účel</b>	Ide o konkrétne určený, výslovne uvedený a oprávnený účel spracúvania OÚ?	<b>ÁNO</b>	
<b>Využitie nových technológií</b>	Sú pri spracúvaní OÚ použité nové/innovatívne technológie?	<b>NIE</b>	

### 1.2. Zaznamenávanie osobných údajov, príjemcovia a obdobie, na ktoré sa budú osobné údaje uchovávať

#### Získavanie a zaznamenávanie osobných údajov

Poverená osoba pri vstupe do budovy vo vyčlenenom priestore vykoná certifikovaným teplomerom tzv. základnú kontrolu telesnej teploty. Základná kontrola telesnej teploty je určená iba na meranie telesnej teploty, po ktorej nenasleduje registrácia, dokumentácia alebo iné spracúvanie osobných údajov jednotlivca.

Ak poverená osoba vykonala minimálne dva merania telesnej teploty, ktoré vykazovali zvýšenú telesnú teplotu 37°C a viac (vrátane 37°C), poverená osoba požiada danú osobu, aby jej poskytla základné identifikačné údaje v rozsahu: meno, priezvisko, tel. kontakt.

Následne požiada danú osobu, aby z bezpečnostných preventívnych dôvodov týkajúcich sa ochorenia COVID-19 opustila budovu, resp. sa jej zakáže vstup do budovy a odporučí sa jej aby ona sama kontaktovala svojho lekára, prípadne aj zamestnávateľa.

Poverená osoba vedie evidenciu osôb, u ktorých bola zistená zvýšená teplota v minimálnom, nevyhnutnom rozsahu vzhľadom na účel tejto evidencie.

**Rozsah evidovaných osobných údajov:** meno, priezvisko, telefonický kontakt, nameranú telesnú teplotu, dátum a čas merania.

#### **Obdobie, na ktoré sa budú osobné údaje uchovávať**

Osobné údaje týkajúce sa merania telesnej teploty sa budú archivovať **po dobu 14 dní od ich získania**, následne sa bezpečným spôsobom vymažú z každého zariadenia, úložiska a pod. a papierové dokumenty sa skartujú.

#### **Príjemcovia**

Osobné údaje môžu byť poskytnuté alebo sprístupnené nasledujúcim kategóriám príjemcov alebo tretích strán:

- Štátne orgány alebo inštitúcie na úseku verejného zdravia ako napr. ÚVZ SR na základe a v rozsahu príslušných právnych predpisov,
- Poskytovateľ IT servisu/údržby.

### **1.3. Funkčný opis spracovateľskej operácie a jeho bezpečnostné zabezpečenie**

- Pri vstupe do budovy je umiestnená informačná tabuľa o tom, že v budove je zavedený systém kontroly teploty.
- Poverená osoba pri vstupe do budovy vo vyčlenenom priestore vykoná certifikovaným teplomerom tzv. základnú kontrolu telesnej teploty.
- Ak poverená osoba nameria telesnú teplotu menšiu ako 37°C, nevykoná žiadny záznam, ani evidenciu údajov.
- Ak sa u osoby pri vstupe do budovy zistí zvýšená telesná teplota, poverená osoba je povinná vykonať druhé opätovné kontrolné meranie.
- Ak sa pri opätovnom meraní zistí zvýšená telesná teplota, poverená osoba v diskkrétnej zóne požiada danú osobu, aby jej poskytla základné identifikačné údaje v rozsahu: meno, priezvisko, tel. kontakt a požiada ju, aby opustila budovu.
- Následne poverená osoba vykoná záznam do príslušnej evidencie v rozsahu: dátum, čas, meno, priezvisko, telefonický kontakt a nameraná telesná teplota.

#### **Zabezpečenie:**

- Transparentnosť a informačná povinnosť je zabezpečená prostredníctvom informačnej tabule, ktorá je pred vstupom do budovy.
- Meranie a evidenciu vykonáva poverená osoba, ktorá je vopred poučená a zaviazaná mlčanlivosťou.
- Evidujú sa len záznamy osôb, ktorým bolo opätovne nameraná zvýšená teplota a údaje sa evidujú len v minimálnom rozsahu.
- Evidencia záznamov sa vykonáva v papierovej podobe, tak aby informačný systém týkajúci sa merania telesnej teploty fungoval nezávisle a nebol prepojený so žiadnym iným IT systémom.

- Uchovávanie záznamov a súvisiacej dokumentácie: dokumentácia sa ukladá do uzamykateľných skríň na to určených, alebo do iných uzamykateľných zariadení, ktoré sa nachádzajú v uzamykateľnej miestnosti. Prístup ku kľúčom sa spravuje tzv. kľúčovým poriadkom.
- Osobné údaje sa budú archivovať po dobu 14 dní od ich získania, následne sa papierové dokumenty sa skartujú a elektronické údaje sa bezpečným spôsobom vymažú z každého zariadenia napr. teplomeru.
- Poskytovanie, sprístupňovanie alebo zverejňovanie záznamov, výsledkov alebo akýchkoľvek informácií týkajúcich sa merania telesnej teploty podlieha poradenstvu so zodpovednou osobou a je možné len v súlade s jej pokynmi.
- Osobné údaje týkajúce sa merania telesnej teploty musia byť pri použití elektronickej pošty prenášané šifrovane napríklad prostredníctvom aplikácie PGP alebo SMIME alebo musia byť uložené do šifrovaného archívu napr. ZIP, RAR, pričom heslo k šifrovaným archívom musí byť adresátovi doručené iným neverejným komunikačným kanálom (napr.: telefonicky alebo SMS správou) a heslo musí spĺňať náležitosti tzv. kvalitného hesla v súlade s heslovou politikou.

#### **1.4. Identifikácia aktív, ktoré vplyvajú na spracovanie osobných údajov (hardvér, softvér, siete, ľudia, papier alebo kanály na prenos papiera)**

**Ľudia:** len interný pracovníci, ktorí sú vopred poučení a zaviazaní mlčanlivosťou.

**Spôsob vedenia evidencie: v papierovej podobe,** tak aby informačný systém týkajúci sa merania telesnej teploty fungoval nezávisle a nebol prepojený so žiadnym iným IT systémom.

**Hardvér:** certifikovaný teplomer alebo iné zariadenie na meranie telesnej teploty.

**Softvér a siete:** nie sú

**Kanály na prenos:** osobné údaje týkajúce sa merania telesnej teploty musia byť pri použití elektronickej pošty prenášané **šifrovane**. (Telefonicky prenos sa neodporúča.)

#### **1.5. Dodržiavanie schválených kódexov správania (článok 35 ods. 8)**

Kódex správania prevádzkovateľ zatiaľ nemá.

## **2. POSÚDENIE NUTNOSTI A PRIMERANOSTI [článok 35 ods. 7 písm. b) GDPR]:**

### **2.1. Opatrenia na dosiahnutie súladu s nariadením**

#### **2.1.1. Opatrenia prospievajúce k primeranosti a nutnosti spracúvania**

##### **2.1.1.1. Konkrétne určený, výslovne uvedené a legitímny účel [článok 5 ods. 1 písm. b)]**

#### **Účel spracúvania osobných údajov:**

Účelom spracúvania osobných údajov je zabezpečenie ochrany života, zdravia pracovníkov a návštevníkov prevádzkovateľa v súvislosti s ochorením COVID-19, pričom meranie telesnej teploty predstavuje jedno z naliehavých opatrení určených na prevenciu pred vírusom COVID-19 (Coronavirus) a na kontrolu vstupu osôb do priestorov prevádzkovateľa počas obdobia zvýšeného rizika infekcie COVID-19.

### 2.1.1.2. Zákonnosť spracúvania (článok 6)

Právnym základom pre spracúvanie tzv. citlivých osobných údajov je článok 9 ods. 2 písm. i) GDPR – spracúvanie je nevyhnutné z dôvodov verejného záujmu v oblasti verejného zdravia, ako je ochrana proti závažným cezhraničným ohrozeniam zdravia, na základe práva Únie alebo práva členského štátu, ktorým sa stanovujú vhodné a konkrétne opatrenia na ochranu práv slobôd dotknutej osoby.

Následným právnym základom je článok 6 ods.1 písm. e) GDPR – spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme. Verejný záujem predstavuje:

- záujem spoločnosti zabezpečiť osobnú bezpečnosť a ochranu ústavných činiteľov a členov záujem spoločnosti predchádzať šíreniu nebezpečnej nákazlivej ľudskej choroby v zmysle trestnoprávných predpisov;
- záujem spoločnosti dodržiavať opatrenia týkajúce sa bezpečnosti a ochrany zdravia pri práci v súvislosti s povinnosťou zamestnávateľa prijať preventívne opatrenia na ochranu života a zdravia svojich zamestnancov v súlade so zákonom č. 124/2006 Z. z.o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov.

### 2.1.1.3. Primeranosť, relevantnosť a obmedzenia na to, ktoré údaje sú potrebné [článok 5 ods. 1 písm. c)]

Relevantnosť spracúvania osobných údajov je daná nasledujúcimi dôvodmi:

- záujem prevádzkovateľa predchádzať šíreniu nebezpečnej nákazlivej ľudskej choroby v zmysle trestnoprávných predpisov;
- záujem prevádzkovateľa dodržiavať opatrenia týkajúce sa bezpečnosti a ochrany zdravia pri práci v súvislosti s povinnosťou zamestnávateľa prijať preventívne opatrenia na ochranu života a zdravia svojich zamestnancov v súlade so zákonom č. 124/2006 Z. z.o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov.

Vyššie uvedené záujmy prevádzkovateľa sú:

- dostatočne konkrétne a jasne formulované,
- povolené právom EÚ a právom Slovenskej republiky,
- skutočné a existujúce záujmy.

V zmysle zásady minimalizácie osobných údajov je povolené získavať len minimálny a nevyhnutný rozsah údajov: meno, priezvisko, telefonický kontakt, nameranú telesnú teplotu, dátum a čas merania.

### 2.1.1.4. Obmedzenej doby uchovávaní [článok 5 ods. 1 písm. e)]

Osobné údaje týkajúce sa merania telesnej teploty sa budú archivovať po dobu 14 dní od ich získania, následne sa papierové dokumenty skartujú a elektronické údaje sa bezpečným spôsobom vymažú z každého zariadenia.

## 2.1.2. Opatrenia prispievajúce k právam dotknutých osôb:

### 2.1.2.1. Informácie poskytnuté dotknutej osobe (články 12, 13 a 14)

Dotknutá osoba bola informovaná v súlade s článok 13 GDPR a zároveň pri vstupe do budovy je umiestnená informačná tabuľa o tom, že v budove je zavedený systém kontroly teploty.

#### 2.1.2.2. Právo na prístup k údajom a právo na prenosnosť údajov (články 15 a 20)

Je zabezpečené, dotknutá osoba za účelom uplatňovania svojho práva môže použiť *Formulár pre uplatnenie práv dotknutej osoby*, ktorý je dostupný na konci dokumentu Informačné poučenie podľa čl. 13 GDPR.

#### 2.1.2.3. Právo na opravu a právo na vymazanie (články 16, 17 a 19)

Je zabezpečené, dotknutá osoba za účelom uplatňovania svojho práva môže použiť *Formulár pre uplatnenie práv dotknutej osoby*, ktorý je dostupný na konci dokumentu Informačné poučenie podľa čl. 13 GDPR.

#### 2.1.2.4. Právo namietat' a právo na obmedzenie spracúvania (články 18, 19 a 21)

Je zabezpečené, dotknutá osoba za účelom uplatňovania svojho práva môže použiť Formulár pre uplatnenie práv dotknutej osoby, ktorý je dostupný na konci dokumentu Informačné poučenie podľa čl. 13 GDPR.

#### 2.1.2.5. Vzťah so sprostredkovateľom (článok 28)

Prevádzkovateľ nepoveril spracúvaním žiadneho sprostredkovateľa.

#### 2.1.2.6. Záruky v súvislosti s medzinárodným prenosom

Cezhraničný prenos sa neuskutočňuje ani nezamýšľa.

#### 2.1.2.7. Predchádzajúca konzultácia (článok 36)

Prevádzkovateľ sa obrátil so žiadosťou o konzultáciu len na svoju zodpovednú osobu.

### 3.1. RIADENIE RIZÍK PRE PRÁVA A SLOBODY DOTKNUTÝCH OSÔB [článok 35 ods. 7 písm. c) GDPR]

#### 3.1.1. Zhodnotenie pôvodu, povahy, osobitosti a závažnosti rizík (pozri odôvodnenie 84)

##### 3.1.1.1. Zohľadnenie zdroja rizík (odôvodnenie 90),

ZDROJ RIZIKA
Fyzické poškodenie (požiar, poškodenie vodou) zariadenia alebo dokumentácie
Fyzická krádež zariadenia pre meranie tel. teploty alebo papierovej dokumentácie
Úmyselná manipulácia s hardvérom/softvérom s cieľom ho poškodiť
Odpozeranie osobných údajov
Technické zlyhanie zariadenia pre meranie tel. teploty
Podvodné kopírovanie databázy nameraných telesných teplôt zo zariadenia pre meranie tel. teploty alebo z papierovej dokumentácie
Personál
Nedostatočné zabezpečenie internej siete

### 3.1.1.2. Identifikácia prípadných dôsledkov na práva a slobody dotknutých osôb v súvislosti s určitými prípadmi vrátane neoprávneného prístupu, neželaných úprav a straty údajov

Zdroj rizika	Dopad	Dôsledky na práva a slobody dotknutých osôb
Fyzické poškodenie zariadenia alebo dokumentácie	Strata/Zničenie údajov Poškodenie/Nesprávnosť údajov	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Strata podporných služieb	Strata/Zničenie údajov Poškodenie/Nesprávnosť údajov	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> </ul>
Fyzická krádež zariadenia alebo dokumentácie	Neoprávnené poskytnutie/Zverejnenie Zneužitie/Nelegálne spracovanie údajov	<ul style="list-style-type: none"> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Úmyselná manipulácia s hardvérom/softvérom s cieľom ho poškodiť	Poškodenie/Nesprávnosť údajov	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Odpozeranie osobných údajov	Zneužitie/Nelegálne spracovanie údajov	<ul style="list-style-type: none"> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Technické zlyhanie zariadenia	Strata/Poškodenie/Nesprávnosť údajov	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> </ul>

		<ul style="list-style-type: none"> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Podvodné kopírovanie databázy v zariadení alebo z papierovej dokumentácie	Zneužitie/ Nelegálne spracovanie údajov Neoprávnené poskytnutie/Zverejnenie	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Personál	Strata/Zničenie údajov Neoprávnené poskytnutie/Zverejnenie	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>
Nedostatočné zabezpečenie internej siete	Poškodenie/Nesprávnosť údajov Neoprávnené poskytnutie/Zverejnenie	<ul style="list-style-type: none"> <li>- Právo fyzickej osoby na presné meranie a záznamy týkajúce sa meraní telesnej teploty.</li> <li>- Odopretie vstupu do budovy a s tým súvisiace následky.</li> <li>- V prípade nepresného merania, ktorého následkom bude povolený vstup do budovy osobe, ktorá je nakazená COVID-19, sa táto choroba môže šíriť ďalej v budove.</li> <li>- Právo na ochranu súkromia v spojitosti so zverejnením/poskytnutím údajov, že fyzická osoba má jeden z príznakov ochorenia COVID-19 a predstavuje hrozbu šírenia nákazy.</li> </ul>

### 3.1.1.3. Identifikácie hrozieb, ktoré by mohli viesť k neoprávnenému prístupu, neželaným úpravám a strate údajov

<b>ZOZNAM HROZIEB</b>
Nedostatok (fyzického bezpečnostného perimetru) fyzickej ochrany budovy, dverí a okien kancelárie
Umiestnenie zariadenia v oblasti náchylnej na vlhkosť, prach, znečistenie, požiar
Nedostatok alebo neuspokojivé pravidlá spracúvania osobných údajov v chránenom priestore
Nedostatočné zabezpečenie chráneného priestoru
Nedostatočné poučenie osôb vrátane záväzku mlčanlivosti
Nedostatočné riadenie prístupu oprávnených osôb
Nedostatočné prístupové a autentifikačné údaje vrátane heslovej politiky
Nedostatočné zabezpečenie siete a pravidiel prístupu do sietí a sieťových služieb
Nedostatok ochrany pred škodlivým softvérom (najmä Firewall a antivírusovej ochrany)

Nedostatok šifrovania
Nedostatok oddelenia jednotlivých databáz

### 3.1.1.4. Odhadnutie pravdepodobnosti a závažnosti (odôvodnenie 90)

ZOZNAM HROZIEB	PRAVDEPODOBNOŠŤ	ZÁVAŽNOSŤ	MIERA RIZIKA
Spôsob získavania a zaznamenávania údajov	5	4	7
Nedostatok týkajúca uloženia dát	5	4	7
Nedostatok (fyzického bezpečnostného perimetru) fyzickej ochrany budov, dverí a okien kancelárie	4	4	6
Umiestnenie zariadenia v oblasti náchylnej na vlhkosť, prach, znečistenie, požiar	3	2	3
Nedostatočné poučenie osôb vrátane záväzku mlčanlivosti	5	4	7
Nedostatočné riadenie prístupu oprávnených osôb	5	4	7
Nedostatočné prístupové a autentifikačné údaje vrátane heslovej politiky	5	4	7

Metodika hodnotenia pravdepodobnosti a závažnosti incidentu je na základe nasledujúcich kritérií.

#### PRAVDEPODOBNOŠŤ INCIDENTU

	Pravdepodobnosť incidentu	Popis
5	Veľmi vysoká	Takmer isté 95%, udalosť sa pravdepodobne stane v priebehu roka
4	Vysoká	Pravdepodobné 50%, udalosť sa pravdepodobne stane do 2 rokov
3	Stredná	Možné 10%, udalosť sa pravdepodobne stane do 5 rokov
2	Nízka	1%, udalosť sa pravdepodobne stane do 10 rokov
1	Veľmi nízka	0,1%, udalosť sa stane za výnimočných okolností, raz za 50 rokov

#### ANALÝZA ZÁVAŽNOSTI DOPADU INCIDENTU NA PRÁVA SLOBODY DOTKNUTÝCH OSÔB

	Závažnosť dopadu incidentu	Počet dotknutých osôb	Poškodenie zdravia	Majetková ujma (fin. škoda )	Poškodenie dobrého mena, dôstojnosti, súkromia,	Porušenie práv zamestnanca
1	Zanedbateľná	Nie je	Nie je	0-50 EUR	Nie je	Nie je
2	Malá	1	Nie je	0-300EUR	Nie je	Interne vyriešené
3	Značná	2-50	Ujma na zdraví	300-3000 EUR	na úrovni blízkeho okolia/ bydliska FO	konanie o náprave na príslušnom štátnom orgáne
4	Významná	51-100	Ublíženie na zdraví	3000-10 000 EUR	na národnej občianskej úrovni	súdne konanie
5	Katastrofická	101 a viac	Ťažká ujma na zdraví	10 000-200 000 EUR	na národnej občianskej + profesijnej úrovni	súdne konanie na úrovni EÚ

P.S. Popis významu slova: *ujma na zdraví, ublíženie na zdraví, ťažká ujma na zdraví* je uvedený v § 123 Trestného zákona.

**Miera rizika** je určená na základe matice (viď. nasledujúca tabuľka), ktorá zohľadňuje dva kľúčové kritéria: **pravdepodobnosť** vzniku incidentu vo vzťahu k **odhadovanej závažnosti/ dopadu** incidentu na práva slobody dotknutých osôb **pred zavedením bezpečnostného opatrenia**.

#### MIERA RIZIKA

	Pravdepodobnosť incidentu	Veľmi nízka	Nízka	Stredná	Vysoká	Veľmi vysoká
Závažnosť dopadu incidentu	Zanedbateľný	0	1	2	3	4
	Malý	1	2	3	4	5
	Značný	2	3	4	5	6
	Významný	3	4	5	6	7
	Katastrofický	4	5	6	7	8

Pre určenie miery rizika sme použili nasledovnú rizikovú stupnicu na stupnici od 0 do 8:

**Veľmi nízke riziko:** 0  
**Nízke riziko:** 1-2  
**Stredné riziko:** 3-5  
**Vysoké riziko:** 6-7  
**Kritické riziko:** 8

**3.2.1. Stanovenie opatrení na riešenie uvedených rizík [článok 35 ods. 7 písm. d) a odôvodnenie 90] vrátane určenia ratingu zostatkových rizík.**

ZOZNAM HROZIEB	PRIJATÉ BEZPEČNOSTNÉ OPATRENIA	P	Z	KONTROLNÉ SKÓRE	RATING ZOSTATKOVÝCH RIZÍK
Spôsob získavania a zaznamenávania údajov	<ul style="list-style-type: none"> <li>- Transparentnosť a informačná povinnosť je zabezpečená prostredníctvom informačnej tabule, ktorá je pred vstupom.</li> <li>- Meranie a evidenciu vykonáva poverená osoba, ktorá je vopred poučená a zaviazaná mlčanlivosťou.</li> <li>- Evidujú sa len záznamy osôb, ktorým bolo opätovne nameraná zvýšená teplota a údaje sa evidujú sa len v minimálnom rozsahu.</li> <li>- Evidencia záznamov sa vykonáva v papierovej podobe, tak aby informačný systém týkajúci sa merania telesnej teploty fungoval nezávisle a nebol prepojený so žiadnym iným IT systémom.</li> </ul>	5	4	3	33

Nedostatok týkajúca uloženia dát	<ul style="list-style-type: none"> <li>- Evidencia záznamov sa vykonáva v papierovej podobe, tak aby informačný systém týkajúci sa merania telesnej teploty fungoval nezávisle a nebol prepojený so žiadnym iným IT systémom.</li> <li>- Dokumentácia sa ukladá do uzamykateľných skríň na to určených, alebo do iných uzamykateľných zariadení, ktoré sa nachádzajú v uzamykateľnej miestnosti. Prístup ku kľúčom sa spravuje tzv. kľúčovým poriadkom.</li> </ul>	5	4	3	33
Nedostatok (fyzického bezpečnostného perimetru) fyzickej ochrany budov, dverí a okien kancelárie	<ul style="list-style-type: none"> <li>- Dokumentácia sa ukladá do uzamykateľných skríň na to určených, alebo do iných uzamykateľných zariadení, ktoré sa nachádzajú v uzamykateľnej miestnosti. Prístup ku kľúčom sa spravuje tzv. kľúčovým poriadkom.</li> <li>- Meranie a evidencia sa vykonáva vo vymedzenom, diskretnom prostredí.</li> </ul>	4	4	3	27
Umiestnenie zariadenia/dokumentácie v oblasti náchylnej na vlhkosť, prach, znečistenie, požiar	<ul style="list-style-type: none"> <li>- Zariadenia a dokumentácia je umiestnená v zabezpečenom priestore bez zvýšeného rizika vplyvu vlhkosti, prachu, znečistenia alebo požiaru.</li> </ul>	3	2	3	10
Nedostatočné poučenie osôb vrátane záväzku mlčanlivosti	<ul style="list-style-type: none"> <li>- Všetky pracovníci pracujúci so zariadením sú poučení o postupe práce a sú zaviazaní mlčanlivosťou.</li> </ul>	5	4	3	33
Nedostatočné riadenie prístupu oprávnených osôb	<ul style="list-style-type: none"> <li>- Prevádzkovateľ má riadený prístup oprávnených osôb, prostredníctvom stanovenia rozsahu povolených prístupových práv k zariadeniu ako aj jeho výstupom a celej dokumentácie.</li> </ul>	5	4	3	33
Nedostatočné prístupové a autentifikačné údaje vrátane heslovej politiky	<ul style="list-style-type: none"> <li>- Prevádzkovateľ má zavedené prístupové a autentifikačné údaje do informačného systému.</li> </ul>	5	4	3	33
Nedostatok ochrany pred škodlivým softvérom (najmä Firewall a antivírusovej ochrany)	<ul style="list-style-type: none"> <li>- Samotný informačný systém je prepojený s internou dátovou sieťou a je šifrovaný a je tiež chránený Firewallom a antivírusovej ochranou.</li> </ul>	4	4	3	27
Nedostatok šifrovania	<ul style="list-style-type: none"> <li>- Osobné údaje týkajúce sa IS meranie telesnej teploty musia byť pri použití elektronickej pošty prenášané šifrovane napríklad prostredníctvom aplikácie PGP alebo SMIME alebo musia byť uložené do šifrovaného archívu</li> </ul>	5	4	3	33

	napr. ZIP, RAR, pričom heslo k šifrovaným archívom musí byť adresátovi doručené iným neverejným komunikačným kanálom (napr.: telefonicky alebo SMS správou) a heslo musí spĺňať náležitosti tzv. kvalitného hesla v súlade s heslovou politikou.				
Nedostatok oddelenia jednotlivých databáz	- Evidencia záznamov sa vykonáva v papierovej podobe, tak aby informačný systém týkajúci sa merania telesnej teploty fungoval nezávisle a nebol prepojený so žiadnym iným IT systémom.	5	4	3	33

Pre jednoduchšie rozhodovanie týkajúce sa správy rizika sa uvádza pomocné hodnotenie rizika v troch kategóriách ako Rating zostatkových rizík (nízky, stredný, vysoký) – vid'. nasl. Tabuľka

Rating zostatkových rizík	Požiadavka na riadenie rizika/potreba znižovania rizika
<b>NÍZKY</b> s hodnotou <20	Tolerovateľné (akceptovateľné) riziko, ktoré je možné akceptovať, pokiaľ jeho riadenie nevyplýva z iných záväzných požiadaviek (právných, zmluvných a pod.). V prípade rozhodnutia o riadení rizika sa postupuje ako v prípade významných rizík.
<b>STREDNÝ</b> s hodnotou 20-59	Stredne významné riziko. Je potrebné vytvoriť plán zvládania rizika a implementovať opatrenia. Treba sa snažiť o zníženie rizika na tolerovateľnú úroveň.
<b>VYSOKÝ</b> s hodnotou 60 a viac	Netolerovateľné riziko. Procesy nesmú byť spustené skôr, ako sa zníži riziko na akceptovateľnú úroveň. Ak sa riziko týka už prebiehajúcich procesov, treba urýchlene podniknúť potrebné kroky na zníženie rizika. Je potrebné vytvoriť plán zvládania rizika.

Riziko, ktoré bude existovať aj po implementovaní bezpečnostných opatrení, bude tvoriť zvyškové riziko. **Hranicu zvyškových rizík** tvorí taká výška rizika, ktorú:

- už nie je efektívne znižovať, nakoľko zdroje na implementáciu bezpečnostných opatrení na ich zníženie sú vyššie ako možný dopad v prípade realizácie hrozby;
- znižovanie už nie je možné, nakoľko jeho výšku určujú faktory, ktoré už nie je možné efektívne ovplyvniť (napr. ľudský faktor, nepublikované chyby hardvéru a softvéru a pod.)

**Rating zostatkových rizík** zohľadňuje mieru rizika pred implantovaním konkrétneho bezpečnostného opatrenia vzhľadom na pravdepodobnosť a dopad incidentu a kvalitu bezpečnostného opatrenia po jeho aplikovaní prostredníctvom tzv. kontrolného skóra.

#### Vzorec pre výpočet Ratingu zostatkových rizík

*Rating zostatkových rizík = Dopad\*Pravdepodobnosť\*(5/Kontrolné skóre)*

## KONTROLNÉ SKÓRE APLIKOVANÉHO BEZPEČNOSTNÉHO OPATRENIA

	Stupeň	Popis
1	Počítačový Ad Hoc	Bezpečnostné opatrenia (BO) nie sú akcieschopné alebo sú nestále.
2	Intuitívny a opakovaný	<ul style="list-style-type: none"><li>▪ Akcieschopnosť BO</li></ul>
3	Definovaný	<ul style="list-style-type: none"><li>▪ Akcieschopnosť BO</li><li>▪ Dokumentácia (Smernice) BO</li></ul>
4	Riadený	<ul style="list-style-type: none"><li>▪ Akcieschopnosť BO</li><li>▪ Dokumentácia (Smernice) BO</li><li>▪ Záznamy z kontrolnej činnosti BO</li></ul>
5	Optimalizovaný	<ul style="list-style-type: none"><li>▪ Akcieschopnosť BO</li><li>▪ Dokumentácia (Smernice) BO</li><li>▪ Záznamy z kontrolnej činnosti BO</li><li>▪ Monitoring BO</li></ul>

### 4.1. ZAPOJENIE ZAJAHOVANÝCH STRÁN

#### 4.1.1. Poradenstvo zodpovednej osoby

Zodpovedná osoba poskytla v danej veci poradenstvo.