# Smernica č. 4/2024 pre riešenie bezpečnostných incidentov v oblasti ochrany osobných údajov

**účinná odo dňa 16. 09. 2024**

**vydaná zamestnávateľom:**

**Obec Malé Ozorovce**
**Hlavná 108/29, Malé Ozorovce 07801**
**IČO: 00331708**

## Obsah

## Čl. 1 Úvodné ustanovenia

1) Smernica upravuje povinnosti všetkých zamestnancov Obec Malé Ozorovce Hlavná 108/29, Malé Ozorovce 07801 IČO: 00331708 (ďalej len ako „Prevádzkovateľ“ )pri hlásení a riešení bezpečnostných incidentov.

## Čl. 1 Základné pojmy

1) **Aktíva informačných technológií (IT aktíva) –** všetky technické a softvérové prostriedky, ktoré slúžia na ukladanie, prenos a spracovanie informácií v digitálnej podobe, bez ohľadu na účel tohto spracovania.
2) **Autentizácia** – je nástroj, pomocou ktorého sa zabezpečuje prístup určených osôb k IT aktívu a zároveň zamedzuje prístup ostatným osobám k IT aktívu.
3) **Bezpečnostný incident** – situácia, stav, kedy môže dôjsť, dochádza alebo došlo k narušeniu existujúcej ochrany osobných údajov.
4) **Dotknutá osoba –** je každá fyzická osoba, ktorej sa osobné údaje spracovávajú.
5) **Hrozby** – vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva organizácie tak, že ich organizácia nemôže využívať, alebo inak ohrozujú oprávnené záujmy organizácie.
6) **Oprávnená osoba –** každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21 Zákona č. 18/2018 Z. z. o ochrane osobných údajov.
7) **Osobné údaje** – údaje, týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu, alebo sociálnu identitu.
8) **Prevádzkovateľ** – subjekt, ktorý spracúva osobné údaje vo vlastnom mene, v tejto smernici je to spoločnosť AirExplore, s. r. o., Krajná 29, 821 04 Bratislava, IČO: 44168802 (ďalej len ako „Prevádzkovateľ“)
9) **Realizujúca sa hrozba –** stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva, alebo ohrozenie záujmov organizácie.
10) **Správca IT aktíva** – osoba zodpovedná za starostlivosť o aktívum.
11) **Zákon** – zákon č. 18/2018 Z. z. o ochrane osobných údajov.
12) **Zodpovedná osoba** – osoba poverená výkonom dohľadu nad ochranou osobných údajov.

## Čl. 3 Bezpečnostné incidenty

1) Bezpečnostné incidenty môžeme definovať aj ako proces, ktorý sa pripravuje, vzniká, má svoj priebeh a zaniká a ktorý má za následok zhoršenie bezpečnostnej situácie.
2) Bezpečnostný incident je akýkoľvek spôsob narušenia bezpečnosti informačného systému, ktorý vzniká ako následok porušenia bezpečnostnej politiky alebo zlyhania bezpečnostných opatrení.
3) Bezpečnostný incident na informačnom systéme je úmyselné využitie zraniteľnosti na spôsobenie škody alebo straty na aktívach informačného systému, alebo neúmyselné vykonanie akcie, ktorej výsledkom je škoda na aktívach.

## Čl. 4 Detekcia bezpečnostných incidentov

1) Detekcia incidentov je súbor činností a opatrení vedúci k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu, že hrozba pôsobí na niektoré aktívum.
2) Detekcia sa vykonáva nasledovným spôsobmi:
   a) automatizovanými technickými prostriedkami – sú to napr. prostriedky hlásiace výskyt požiaru, senzory zisťujúce pohyb a pod.,
   b) automatickými informatickými (programovými) prostriedkami – sú to špecializované programy, ktoré vyhodnocujú prevádzkové záznamy a indikujú potenciálny incident,
   c) sústavnou činnosťou zamestnancov – primeranou ostražitosťou zamestnancov, najmä správcov IT aktív a bezpečnostného správcu a výkonom kontrolnej činnosti.
3) Monitorovacie a kontrolné postupy majú byť schopné odhaliť nielen zrealizované narušenia, ale aj pokusy o narušenie.

## Čl. 5 Reakcia na bezpečnostný incident

1) Incidenty, ktoré ovplyvňujú bezpečnosť informácií, ako aj osobných údajov, by mali byť čo najrýchlejšie hlásené. Cieľom reakcie je sledovať chyby a minimalizovať škody spôsobené bezpečnostným incidentom.
2) Incident môže byť ohlasovaný telefonicky, hlasovou poštou, osobne, písomne, faxom, emailom, automaticky monitorovacím softvérom alebo môže byť zaznamenaný priamo používateľom, ktorý má prístup do systému na zaznamenávanie incidentov.
3) Všetky incidenty musia byť dôkladne zaznamenané, najmä musia byť zaznamenané všetky relevantné informácie o incidente, aby pomohli k jeho vyriešeniu.
4) Všetky informácie o bezpečnostných incidentoch sa ukladajú na bezpečnom mieste s riadeným prístupom pre analýzu a spracovanie opatrení a prípadné použitie informácií v pracovno-právnom alebo trestno-právnom procese.
5) O každom bezpečnostnom incidente musí byť spracovaný záznam. Záznam spracúva správca IT aktíva. Každý zamestnanec je povinný poskytnúť bezpečnostnému správcovi všetky podklady a údaje, ktoré potrebuje pre spracovanie záznamu o bezpečnostnom incidente.
6) Záznam o bezpečnostnom incidente musí obsahovať:
   a) dátum a čas, kedy bol incident zistený, kedy sa skončil a ak je to možné, zistiť aj to, kedy sa incident začal,
   b) opis spôsobu, ako bol incident zistený, pričom sa uvedie aj zamestnanec, ktorý incident ohlásil,
   c) dátum a čas, kedy bol zmenený bezpečnostný režim,
   d) chronologický opis priebehu incidentu, opis hrozieb, ktoré nastali a spôsob, akým sa realizovali,
   e) zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia,
   f) porovnanie s rizikovou analýzou – doklad či bolo možné incident očakávať, či boli správne odhadnuté rizikové indexy a pod.,
   g) opis prijatých opatrení – doklad, kedy a kým boli prijaté, doklad o ich účinnosti a trvaní,
   h) návrh na prijatie opatrení na zamedzenie opakovania incidentu, záznam o úprave rizikovej analýzy, ak takúto úpravu bolo potrebné vykonať,
   i) záznam o porušení opatrení a nariadení, ktoré mohli spôsobiť, že incident nastal, zoznam zamestnancov, ktorí tieto nariadenia porušili,

j) dátum a podpis správcu aktíva, ktorý záznam vyhotovil.

7) So spracovaným záznamom o bezpečnostnom incidente musia byť preukázateľne oboznámení:
   a) správcovia dotknutých aktív,
   b) nadriadení zamestnancov, ktorí porušili nariadenia a opatrenia, a teda umožnili, že incident mohol nastať.
8) Všetky zistené alebo ohlásené incidenty by mali byť zaregistrované spôsobom, ktorý dovoľuje vyhľadávanie a analyzovanie dôležitých informácií.
9) Ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou zamestnanca, bude sankcionovaný podľa príslušných ustanovení pracovného poriadku a zákonníka práce.

## Čl. 6 Zodpovednosť a postupy pri výskyte bezpečnostného incidentu

1) Vedúci zamestnanec je povinný pri riešení bezpečnostných incidentov alebo narušení ochrany osobných údajov koordinovať svoj postup so správcom IT aktíva.
2) Zamestnanec je povinný oznámiť príslušnému vedúcemu zamestnancovi a zodpovednej osobe každý bezpečnostný incident a oznámiť každé zistenie o nedostatočnej účinnosti existujúcich bezpečnostných opatrení, ktoré boli prijaté na ochranu osobných údajov.
3) Postupy, ktoré by mali byť pripravené v prípade výskytu bezpečnostného incidentu by mali zahŕňať:
   a) identifikovanie bezpečnostného incidentu,
   b) vyhodnotenie závažnosti bezpečnostného incidentu a aktuálnej situácie:
      1. správca IT aktíva alebo zodpovedná osoba zhodnotí závažnosť bezpečnostného incidentu a možný dopad na organizáciu,
      2. správca IT aktíva nahlási výskyt bezpečnostného incidentu nadriadeným,
      3. nadriadení alebo vrcholový manažment preberajú zodpovednosť a kompetencie za riešenie vzniknutej situácie, ktorá nastala,
   c) zváženie prerušenia činnosti v závislosti od závažnosti bezpečnostného incidentu:
      1. zodpovedná osoba zváži, aký dopad bude mať bezpečnostný incident na ochranu osobných údajov,
      2. v prípade potreby správca IT aktíva zabezpečí prerušenie činnosti (prevádzky) informačného systému,
      3. správca IT aktíva je povinný oznámiť túto skutočnosť svojmu nadriadenému,
   d) skontrolovanie auditných záznamov – správca IT aktíva skontroluje auditné záznamy, kvôli identifikovaniu príčin vzniku bezpečnostného incidentu,
   e) zálohovanie dát v závislosti od informačného systému, ktoré vykoná správca IT aktíva,
   f) informovanie zodpovedných zamestnancov o vzniknutej situácii:
      1. z dôvodu potreby zabezpečenia potrebných zdrojov na nápravu škôd spôsobených bezpečnostným incidentom,
      2. správca IT aktíva vyplní a zašle formulár pre bezpečnostne významnú udalosť vedeniu Prevádzkovateľa,
   g) odstránenie následkov bezpečnostného incidentu, za ktoré zodpovedá vedenie prevádzkovateľa:
      1. správca IT aktíva zabezpečí odstránenie následkov bezpečnostného incidentu,
      2. pokiaľ boli bezpečnostným incidentom zasiahnuté osobné údaje, zodpovedná osoba spolupracuje s vedením Prevádzkovateľa pri riešení vzniknutých následkov,

h) správca IT aktíva spolu so zodpovednou osobou vytvoria vhodné opatrenia či návrhy, ktoré zabránia opakovanému výskytu bezpečnostných incidentov, následné prijatie a implementáciu zabezpečí vedenie Prevádzkovateľa,
i) ak bola prerušená prevádzka informačného systému, je potrebné jej obnovenie, za ktoré zodpovedá vedenie Prevádzkovateľa, následne obnovu vykonáva správca IT aktíva,
j) skontrolovanie stavu, funkčnosti a bezpečnosti informačného systému, za ktoré zodpovedá vedenie Prevádzkovateľa,
k) správca IT aktíva v súčinnosti so zodpovednou osobou vypracuje hlásenie s následným doručením vedeniu Prevádzkovateľa.

## Čl. 7 Záverečná správa

1) Záverečná správa o vyšetrovaní incidentu obsahuje najdôležitejšie údaje a informácie o výsledkoch vyšetrenia príčin incidentu. Správa musí ukázať spôsoby, ako urobiť pracovný postup bezpečným za akýchkoľvek okolností, teda aj v prípade nejakej nepredvídateľnej udalosti.
2) Získané informácie z hlásení bezpečnostných incidentov by mali byť použité na aktualizáciu a revíziu zoznamu rizík a ich riadenia. Základné príčiny identifikované v správe sa musia analyzovať z hľadiska ich vplyvu na všetky ostatné činnosti a postupy.
3) Vedenie organizácie bude o incidente informované. Procesy ošetrovania bezpečnostných incidentov budú vopred stanovené. Pre tieto procesy bude vopred určený a vyškolený okruh zodpovedných zamestnancov.
4) Po úspešnom zistení incidentu je potrebný určitý čas na to, aby zodpovedné osoby získali výsledky hrubej analýzy a aby na základe zistených informácií zhodnotili udalosť, ktorá determinuje incident.

## Čl. 8 Prevencia bezpečnostného incidentu

1) Prevencia predstavuje prípravu na incident. Pre úspešné zvládnutie riešenia bezpečnostných incidentov je potrebné:
   a) mať vypracované postupy pre riešenie najpravdepodobnejších bezpečnostných incidentov,
   b) mať definované postupy pre činnosť v prípade objavenia sa bezpečnostného incidentu,
   c) každý bezpečnostný incident analyzovať, pričom je potrebné sa zamerať na príčiny jeho vzniku, na spôsoby prejavov, pôsobenia negatívnych následkov a analýzu časových a priestorových charakteristík,
   d) aktualizovať vypracované preventívne programy a pracovné postupy,
   e) v prípade objavenia sa nových bezpečnostných rizík vypracovať nové plány na riešenie bezpečnostných incidentov.
2) Všetci zamestnanci by mali mať kontaktné údaje na svojho nadriadeného a svojich podriadených, aby mohli v prípade potreby využiť telefonické spojenie na kontaktovanie všetkých zamestnancov.
3) Ak nastal bezpečnostný incident, každý zapojený zamestnanec by si mal zaznamenávať svoje zapojenie do incidentu do vopred pripravených formulárov.

## Čl. 9 Záverečné ustanovenia

1) Vedúci pracovníci prevádzkovateľa sú povinní s touto smernicou oboznámiť všetkých zamestnancov, ktorí sú oprávnenými osobami a majú právomoc poskytovať informácie a údaje dotknutým osobám.
2) Táto Smernica nadobúda účinnosť dňa 16. 09. 2024
3) Táto Smernica je záväzná pre všetky oprávnené osoby prevádzkovateľa.

V Malých Ozorovciach, dňa 16. 09. 2024

_____

Obec Malé Ozorovce

**Príloha č.1 - Záznam o incidentoch**

| Por. č. | Dátum a čas zistenia | Zdroj Incidentu | Dátum a čas zmeny režimu | Dátum a čas začiatku | Dátum a čas skončenia |
|---|---|---|---|---|---|
| | | | | | |
| Opis spôsobu zistenia incidentu: | | | | | |
| Opis vlastného incidentu: | | | | | |
| Zoznam dotknutých aktív: | | | | | |
| Porovnanie s rizikovou analýzou: | | | | | |
| Prijaté opatrenia: | | | | | |
| Opatrenia na zamedzenie opätovného incidentu: | | | | | |
| Opatrenia a nariadenia ktoré boli porušené: | | | | | |

Dátum a podpis správcu aktíva:

| Dátum oboznámenia | Titul, Meno a Priezvisko zamestnanca | Podpis zamestnanca |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |