OZNAMOVANIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV

Obsah

Terminológia

Bezpečnosť informácií – zachovanie dôvernosti, integrity a dostupnosti informácií (ISO/IEC 27000:2017)

Cieľ – výsledok, ktorý má byť dosiahnutý (ISO/IEC 27000:2017)

Dotknutá osoba - každá fyzická osoba, ktorej osobné údaje sa spracúvajú (Zákon č. 18/2018 Z. z. o ochrane osobných údajov)

Dostupnosť – vlastnosť vyjadrujúca prístupnosť a použiteľnosť na žiadosť oprávnenej osoby (ISO/IEC 27000:2017)

Dozorný orgán – orgán štátnej správy s celoslovenskou pôsobnosťou, ktorý sa podieľa na ochrane základných práv fyzických osôb pri spracúvaní osobných údajov, a ktorý vykonáva dozor nad ochranou osobných údajov (Zákon č. 18/2018 Z. z. o ochrane osobných údajov)

Úrad na ochranu osobných údajov Slovenskej republiky, Hraničná 12, 820 07, Bratislava 27, Slovenská republika, IČO: 36064220, tel.: 02/32313214, email.: statny.dozor@pdp.gov.sk

Dôvernosť – vlastnosť, že informácia nie je dostupná alebo nie je odhalená neoprávneným osobám, entitám alebo procesom (ISO/IEC 27000:2017)

Incident bezpečnosti informácií (bezpečnostný incident) – nežiaduca alebo neočakávaná udalosť bezpečnosti informácií alebo séria nežiaducich alebo neočakávaných udalostí bezpečnosti informácií, ktoré môžu s významnou pravdepodobnosťou ohroziť operácie súvisiace s činnosťou organizácie a ohrozenia bezpečnosti informácií (ISO/IEC 27000:2017)

Informačný systém – 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 (GDPR 2016/679)

Integrita – zaistenie presnosti a úplnosti (ISO/IEC 27000:2017)

Následok – výsledok udalosti pôsobiaci na ciele (ISO/IEC 27000:2017)

Oprávnená osoba – fyzická osoba, ktorá prichádza do kontaktu s osobnými údajmi u prevádzkovateľa v rámci plnenia svojich pracovných (služobných) povinností, alebo obdobného vzťahu s prevádzkovateľom (založeného napr. na základe poverenia, vymenovania, zvolenia alebo v rámci výkonu verejnej funkcie), a ktorá vykonáva prevádzkovateľom určené spracovateľské operácie s osobnými údajmi (Zákon č. 122/2013 Z. z. o ochrane osobných údajov)

Porušenie ochrany osobných údajov – 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 (GDPR 2016/679)

Pravdepodobná možnosť výskytu (likelihood) – možnosť, že niečo nastane (ISO/IEC 27000:2017)

Prevádzkovateľ – fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov (**Žilinský samosprávny kraj, Komenského 48, Žilina 011 09, IČO: 37 808 427**)

Riadenie incidentov bezpečnosti informácií – procesy na detegovanie, posudzovanie a riešenie incidentov bezpečnosti informácií, na podávanie správ o incidentoch bezpečnosti informácií, na odozvu na incidenty bezpečnosti informácií a na poučenie sa z incidentov bezpečnosti informácií (ISO/IEC 27000:2017)

Riziko – účinok (odchýlka od očakávaného) neistoty na dosiahnutie cieľov (ISO/IEC 27000:2017)

Sprostredkovateľ –fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa (GDPR 2016/679)

Úroveň (stupeň) rizika – veľkosť rizika vyjadrená ako kombinácia následkov a ich pravdepodobnej možnosti výskytu (ISO/IEC 27000:2017)

Zodpovedná osoba – oprávnená osoba, ktorá zabezpečuje dohľad nad ochranou osobných údajov pri spracúvaní osobných údajov u prevádzkovateľa alebo sprostredkovateľa. (Zákon č. 122/2013 Z. z. o ochrane osobných údajov) uvedená na webovom sídle www.zilinskazupa.sk

Hlásenie bezpečnostných incidentov

1) Každý zamestnanec a iná oprávnená osoba informačného systému je povinná bezodkladne po zistení bezpečnostného incidentu súvisiaceho so spracúvaním osobných údajov nahlásiť ho zodpovednej osobe.
2) Za bezpečnostný incident sa považuje hlavne:
    a) poskytnutie alebo získanie neoprávnených prístupových práv alebo prístupu k informáciám (napr. prihlasovacie údaje do softvérovej aplikácie, odoslanie emailu adresátovi, nájdenie papierovej dokumentácie),
    b) zničenie, poškodenie, strata alebo krádež prideleného prostriedku výpočtovej techniky (napr. notebook, pracovná stanica, server, mobilný telefón, prenosné pamäťové médium),
    c) zničenie, poškodenie, strata alebo krádež papierovej dokumentácie,
    d) podozrenie na prezradenie, stratu, odcudzenie alebo odtajnenie autentifikačných informácií alebo zariadení (napr. vstupná karta, token, čip),
    e) opakované odopretie služby (napr. prístup na internet, e-mail, prístup do softvérovej aplikácie, operačného systému),
    f) neoprávnený vzdialený prístup počas dodávateľského a outsourcingového servisu,
    g) opakované výstražné hlásenia o prítomnosti škodlivého, zlomyseľného kódu, t. j. počítačových vírusoch, trojanoch, ransomwaroch, keyloggeroch, phisingoch,
    h) hlásenie o neznámych alebo podozrivých aktivitách v sieťovej infraštruktúre alebo na sledovaných zariadeniach,
    i) hlásenie o zmenách, úpravách alebo informáciách o stave zariadení,
    j) hlásenie o aktivitách na zistenie informácií o možných cieľoch spoločnosti (napr. opakované pokusy o scannovanie portov),
    k) hlásenie o možnom zahladzovaní stôp po prieniku na nejaké zariadenie,
    l) hlásenie o pokusoch o neoprávnený prístup na poskytované služby, o neoprávnených pokusoch o autentizáciu alebo pokusoch zmeniť alebo zabezpečiť autorizáciu práv na zariadenie alebo účty,
    m) zvýšený počet doručenej nevyžiadanej pošty – spamu,
    n) samovoľné spúšťanie niektorých aplikácií,
    o) výrazné zníženie výkonnosti počítača,
    p) výpadok dodávky elektrickej energie,
    q) porušenie režimových opatrení fyzickej a objektovej bezpečnosti,
    r) neoprávnený zásah do výpočtovej techniky.

Povinnosti zodpovednej osoby

1) Po nahlásení bezpečnostného incidentu zodpovedná osoba prijme nápravné opatrenia na minimalizáciu jeho následkov a spracuje záznam o bezpečnostnom incidente (Príloha 1: Záznam o vzniku bezpečnostného incidentu).
2) Zodpovedná osoba vytvára a eviduje záznamy o vzniku bezpečnostného incidentu.
3) Zodpovedná osoba zhodnotí závažnosť bezpečnostného incidentu vo vzťahu k porušeniu ochrany osobných údajov (Príloha 2: Záznam o porušení ochrany osobných údajov), t. j. či bezpečnostný incident predstavuje zároveň porušenie ochrany osobných údajov.
4) V prípade, ak porušenie ochrany osobných údajov nepovedie k žiadnemu riziku pre práva a slobody fyzických osôb (Príloha 5: Stanovenie veľkosti rizika pre práva a slobody fyzických osôb), nie je potrebné toto porušenie oznámiť dozornému orgánu.
5) V prípade, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb (Príloha 5: Stanovenie veľkosti rizika pre práva a slobody fyzických osôb), zodpovedná osoba bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti

dozvedela[1], oznámi porušenie ochrany osobných údajov dozornému orgán, a to na webovej stránke: https://dataprotection.gov.sk/uoou/dp/dp-breach.

6) Riziko pre práva a slobody fyzických osôb sa môže časom zmeniť a je potrebné ho následne prehodnotiť vo vzťahu k právam a slobodám fyzických osôb (napr. zverejnením šifrovacieho algoritmu, odhalením zraniteľných miest v šifrovacom softvéri).
7) Po tom, čo bola zodpovedná osoba informovaná jednotlivcom (napr. zamestnanec, zákazník, občan) cez médiá alebo iné zdroje alebo, ak sami incident odhalili, môžu po určitú krátku dobu (maximálne 3 dni) vykonávať šetrenie, aby zistili, či k porušeniu ochrany osobných údajov skutočne došlo.
8) Ak oznámenie nebolo dozornému orgánu predložené do 72 hodín, pripojí sa k nemu zdôvodnenie omeškania (napr. predpoklad oznámenia viacerých porušení ochrany osobných údajov).
9) Omeškanie oznámenia dozornému orgánu sa nesmie považovať za bežnú prax.
10) Ak nie je možné poskytnúť informácie dozornému orgánu v stanovenom rozsahu, je možné informácie poskytnúť vo viacerých etapách, ale bez ďalšieho zbytočného odkladu (napr. v prípade forenzného šetrenia bezpečnostného incidentu).
11) V prípade, ak sa porušenie ochrany osobných údajov týka prevádzkovateľa, v ktorého mene organizácia spracúva osobné údaje, zodpovedná osoba sprostredkovateľa podá prevádzkovateľovi oznámenie bez zbytočného odkladu, najneskôr do 2 dní po tom, čo sa o porušení ochrany osobných údajov dozvedela (Príloha 3: Oznámenie porušenia ochrany osobných údajov).
12) V prípade, že dôjde k porušeniu ochrany osobných údajov jednotlivcov z viac ako jedného členského štátu, je potrebné túto skutočnosť oznámiť všetkým dotknutým dozorným orgánom.
13) V prípade, že sú osobné údaje spracovávané v mene viacerých prevádzkovateľov, je zodpovedná osoba povinná bez zbytočného odkladu podať oznámenie všetkým prevádzkovateľom.
14) Sprostredkovateľ môže v mene prevádzkovateľa oznámiť porušenie ochrany osobných údajov iba v prípade, pokiaľ je toto oprávnenie sprostredkovateľovi výslovne povolené v platnom poverení (v zmluve) so sprostredkovateľom.
15) V prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb (Príloha 5: Stanovenie veľkosti rizika pre práva a slobody fyzických osôb), zodpovedná osoba bez zbytočného odkladu oznámi porušenie ochrany osobných údajov dotknutým osobám, ktorých sa porušenie týka (Príloha 4: Oznámenie o porušení ochrany osobných údajov dotknutej osobe).
16) K oznámeniu dotknutej osobe by mala byť využitá samostatná správa, ktorá nesmie byť dopĺňaná ďalšími informáciami (napr. oznámenie nesmie byť súčasťou faktúry alebo propagačného materiálu).
17) Oznámenie musí byť jasné a transparentné (napr. SMS, email, poštová komunikácia, priama správa, výrazné bannery alebo oznámenia na webových stránkach, nápadné oznamy v tlačených médiách).
18) Skryté oznámenie v tlačovej správe alebo firemnom blogu sa nepovažuje za účinný prostriedok oznámenia dotknutej osobe.
19) Na oznámenie dotknutej osobe nie je možné využiť kanál, ktorý bol predmetom porušenia ochrany osobných údajov, nakoľko ten môže byť využitý útočníkom predstierajúcim identitu prevádzkovateľa.
20) Je potrebné zabezpečiť, aby oznámenia boli vo vhodných formátoch a relevantných jazykoch.
21) Oznámenie dotknutej osobe sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok:
    a) prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie,
    b) prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky.
22) Zodpovedná osoba vytvára a eviduje záznamy o porušení ochrany osobných údajov a oznámenia porušenia ochrany osobných údajov.

[1] Za informovanú zodpovednú osobou možno považovať osobu, ktorá má dôvodný stupeň istoty.

23) Ak by oznámenie dotknutej osobe vyžadovalo neprimerané úsilie, tak v takom prípade dôjde namiesto toho k informovaniu verejnosti (napr. masovokomunikačnými prostriedkami), alebo sa prijme podobné opatrenie, čím sa zaručí, že dotknuté osoby budú informované rovnako efektívnym spôsobom.
24) Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, dozorný orgán môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil, alebo môže rozhodnúť, že je splnená niektorá z podmienok uvedených v odseku 11.
25) Za nedodržanie oznamovacej povinnosti je dozorný orgán oprávnený uložiť správnu pokutu až do výšky 10 000 000 EUR, alebo až do výšky 2 % celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia.
26) Nedodržanie oznamovacej povinnosti môže zároveň znamenať neprimeranosť prijatých technických a organizačných opatrení, a tým viesť k opätovnému uloženiu správnej pokuty.
27) Príklady možných porušení ochrany osobných údajov sú uvedené na: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28327.
28) Proces znázorňujúci požiadavky na oznámenie o porušení ochrany osobných údajov je uvedený v prílohe smernice (Príloha 5: Stanovenie veľkosti rizika pre práva a slobody fyzických osôb).

Spoločné ustanovenie

1) Táto smernica nadobúda účinnosť dňom 01.02.2019 a je záväzná pre všetkých zamestnancov Úradu ŽSK a iné oprávnené osoby.

V Žiline dňa 28.01.2019

.....
Ing. Erika Jurinová
predsedníčka ŽSK

Príloha 1: Záznam o vzniku bezpečnostného incidentu

Oznamovateľ:	[Meno a priezvisko, pozícia]
Dátum a čas:	[Dátum, čas]
Evidenčné číslo:	[interné označenie]

Popis incidentu: [text]

Čas, spôsob a odôvodnenie reakcie na incident: [text]

Predpokladaný následok incidentu: [text]

Navrhované opatrenia na elimináciu pravdepodobnosti vzniku incidentu v budúcnosti: [text]

Dátum:	[Dátum]
Spracoval:	[Meno a priezvisko, pozícia]
Schválil:	[Meno a priezvisko, pozícia]

Príloha 2: Záznam o porušení ochrany osobných údajov

Evidenčné. číslo bezpečnostného incidentu: [interné označenie]

V prípade hláseného bezpečnostného incidentu došlo k:

Bezpečnostný incident – náhodný/neoprávnený	Kategória porušenia ochrany OÚ		
	Dôvernosť	Dostupnosť	Integrita
Zničenie[2] osobných údajov			
Poškodenie[3] osobných údajov			
Strata[4] osobných údajov			
Zmena osobných údajov			
Poskytnutie/získanie[5] osobných údajov			

Predmetom porušenia ochrany osobných údajov boli kategórie osobných údajov odhaľujúce:
□ rasový alebo etnický pôvod
□ politické názory
□ náboženstvo alebo filozofické názory
□ členstvo v odborových organizáciách
□ genetické údaje

resp. kategórie údajov týkajúce sa:
□ zdravia
□ zraniteľných fyzických osôb (najmä detí)
□ sexuálneho života
□ uznania viny zo spáchania trestného činu a priestupku
□ kontaktných údajov
□ obrazových/zvukových stôp
□ osobných identifikátorov
□ výkonnosti v práci
□ majetkových pomerov
□ osobných preferencií alebo záujmov
□ spoľahlivosti alebo správania
□ polohy alebo pohybu

Ktorých informačných systémov sa porušenie ochrany osobných údajov týka: [text]

Kategórie dotknutých osôb: [text]

Predpokladaný počet dotknutých osôb: [text]

[2] Osobné údaje už neexistujú vôbec alebo prinajmenšom nie v podobe, aby boli použiteľné.
[3] Osobné údaje už nie sú kompletné.
[4] Zodpovedná osoba alebo prevádzkovateľ stratili kontrolu nad osobnými údajmi, alebo k nim nemajú prístup.
[5] Poskytnutie osobných údajov príjemcom, ktorí nemajú oprávnenie dáta získať, resp. akékoľvek iné spracovanie údajov, ktoré je v rozpore s nariadením.

Vyššie uvedené porušenie ochrany osobných údajov môže viesť k:	**Úroveň (stupeň) rizika[6]**
ujme na zdraví	
majetkovej alebo nemajetkovej ujme	
k diskriminácii	
krádeži totožnosti alebo podvodu	
finančnej strate	
poškodeniu dobrého mena/povesti	
strate dôvernosti osobných údajov/strate kontroly nad osobnými údajmi	
neoprávnenej reverznej pseudonymizácii	
závažnému hospodárskemu alebo sociálnemu znevýhodneniu	
pozbaveniu svojich práv a slobôd	
bráneniu kontroly nad svojimi osobnými údajmi	

Bezpečnostný incident predstavoval porušenie ochrany osobných údajov: áno – nie[7]

Prevádzkovateľovi vzniká povinnosť oznámenia porušenia ochrany osobných údajov dozornému orgánu: áno – nie[7]

Prevádzkovateľovi vzniká povinnosť oznámenia porušenia ochrany osobných údajov dotknutej osobe: áno – nie[7]

Poznámky, resp. návrhy k spôsobu oznámenia:

Osoba zodpovedná za oznámenie: [Meno a priezvisko, pozícia]

Dátum: [Dátum]
Spracoval: [Meno a priezvisko, pozícia]
Schválil: [Meno a priezvisko, pozícia]

[6] Stanovenie veľkosti rizika pre práva a slobody dotknutých osôb podľa ISO/IEC 29 134 Information technology -- Security techniques -- Guidelines for privacy impact assessment.
[7] Nehodiace sa prečiarknite.

Príloha 3: Oznámenie porušenia ochrany osobných údajov prevádzkovateľovi

OZNÁMENIE
porušenia ochrany osobných údajov dozornému orgánu podľa článku 33 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

II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa, ak bol vymenovaný a jeho IČO, sídlo a štatutárny orgán	
Meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií	

II. ÚDAJE O PORUŠENÍ OCHRANY OSOBNÝCH ÚDAJOV			
Opis povahy porušenia ochrany osobných údajov			
Kategória porušenia ochrany osobných údajov	Dôvernosť	Dostupnosť	Integrita
Kategórie a približný počet dotknutých osôb, ktorých sa porušenie týka			
Kategórie a približný počet dotknutých záznamov o osobných údajoch			
Opis pravdepodobných následkov porušenia ochrany osobných údajov			
Opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov, vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov			

_____ _____

[Odtlačok pečiatky prevádzkovateľa] [Meno a podpis štatutárneho orgánu]

Príloha 4: Oznámenie o porušení ochrany osobných údajov dotknutej osobe

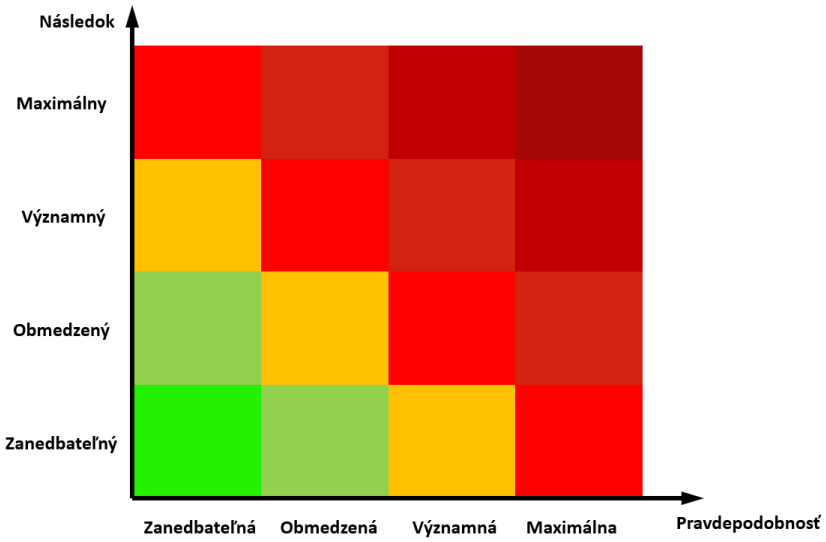
OZNÁMENIE
porušenia ochrany osobných údajov dotknutej osobe podľa článku 34 NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov

I. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa, ak bol vymenovaný a jeho IČO, sídlo a štatutárny orgán	
Meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií[8]	

II. ÚDAJE O PORUŠENÍ OCHRANY OSOBNÝCH ÚDAJOV			
Opis povahy porušenia ochrany osobných údajov			
Kategória porušenia ochrany osobných údajov	Dôvernosť	Dostupnosť	Integrita
Kategórie a približný počet dotknutých záznamov o osobných údajoch			
Opis pravdepodobných následkov porušenia ochrany osobných údajov[8]			
Opis opatrení prijatých s cieľom napraviť porušenie ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov[8]			
Opis opatrení navrhovaných dotknutej osobe s cieľom napraviť porušenie ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov[8]			

[8]povinné informácie podľa požiadaviek nariadenia

Príloha 5: Stanovenie veľkosti rizika pre práva a slobody fyzických osôb



Legenda:

- Tolerovateľné riziko pre práva a slobody dotknutých osôb
- Riziko pre práva a slobody dotknutých osôb
- Vysoké riziko pre práva a slobody dotknutých osôb

Pri stanovení úrovne (stupňa) rizika je potrebné zohľadniť: povahu, citlivosť a objem osobných údajov, náročnosť identifikácie jednotlivca, závažnosť následkov pre jednotlivca, zvláštne charakteristiky jednotlivca, počet dotknutých jednotlivcov, špecifiká prevádzkovateľa a prípadne ich kombinácie.

Pravdepodobná možnosť výskytu

1) Zanedbateľná: Narušenie ochrany osobných údajov nemôže alebo iba v teoretickej rovine môže spôsobiť ujmu dotknutej osobe.
2) Obmedzená: Narušenie ochrany osobných údajov môže spôsobiť ujmu dotknutej osobe.
3) Významná: Narušenie ochrany osobných údajov môže s veľkou pravdepodobnosťou spôsobiť ujmu dotknutej osobe.
4) Maximálna: Narušenie ochrany osobných údajov s určitosťou spôsobí ujmu dotknutej osobe.

Následok

1) Zanedbateľný: Dotknutá osoba, buď nebude ovplyvnená, alebo sa môže stretnúť s niekoľkými nepríjemnosťami, ktoré dokáže bez problémov prekonať (napr. čas strávený opätovným zadávaním informácií, atď.).
2) Obmedzený: Dotknutá osoba sa môže stretnúť s významnými ťažkosťami, ktoré napriek niekoľkým prekážkam dokáže prekonať (napr. dodatočné náklady, odmietnutie prístupu k obchodným službám, strach, nedostatok porozumenia, stres, menšie telesné ťažkosti, atď.).
3) Významný: Dotknutá osoba môže mať závažné následky, ktoré by však mala prekonať, aj keď s vážnymi ťažkosťami (napr. zneužitie finančných prostriedkov, čierna listina, majetkové škody, strata zamestnania, predvolanie, zhoršenie zdravotného stavu, atď.).
4) Maximálny: Dotknutá osoba sa môže stretnúť s významnými alebo dokonca nezvratnými následkami, ktoré nemusí prekonať (napr. finančné ťažkosti, ako napríklad neudržateľný dlh alebo pracovná neschopnosť, dlhodobé psychické alebo fyzické ťažkosti, smrť, atď.).

Príloha 6: Diagram znázorňujúci požiadavky na oznámenie o porušení ochrany osobných údajov