FORMULÁR NA ZDOKUMENTOVANIE PORUŠENIA OCHRANY OSOBNÝCH ÚDAJOV

Tento záznam o porušení ochrany osobných údajov bol vypracovaný v súlade s čl. 33 ods. 5 GDPR a slúži na zdokumentovanie porušenia a evidenciu o prijatých bezpečnostných opatreniach a postupoch na zmiernenie rizika pre práva a slobody pre fyzické osoby (ďalej len ako „záznam“).

Spoločnosť/ambulancia: .....
Sídlo: .....
IČO: .....
Zápis: .....
Kontaktné údaje: .....
(ďalej len ako „**Prevádzkovateľ**“)

Keďže:

(A) V zmysle čl. 4 bod 12 GDPR: *„porušenie ochrany osobných údajov“ je 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* (ďalej len „Porušenie“).

(B) V zmysle čl. 33 ods. 5 GDPR: *„Prevádzkovateľ zdokumentuje každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu. Uvedená dokumentácia musí umožniť dozorným orgánom overiť súlad s týmto článkom.“*

Prevádzkovateľ sa rozhodol zdokumentovať Porušenie nasledovne:

1.	**Dátum, miesto a čas zistenia Porušenia a jeho interné označenie:**	
2.	**Kontaktné údaje zodpovednej osoby, ak je vymenovaná:**	
3.	**Kontaktné údaje IT poradcu alebo IT oddelenia:**	
4.	**Kontaktné údaje na iné osoby disponujúce dôležitými poznatkami o Porušení:**	
5.	**Základný opis Porušenia:**	
6.	**Spôsob zistenia Porušenia:**	
7.	**Popis povahy Porušenia:**	
8.	**Identifikácia prijatých bezpečnostných opatrení, ktoré boli určené na prevenciu pred vznikom Porušenia:**	

9.	**Pravdepodobné príčiny vzniku Porušenia:**	
10.	**Vzťah Porušenia a zostatkového rizika pre práva a slobody fyzických osôb:**	
11.	**Opis pravdepodobných následkov Porušenia:**	
12.	**Opis opatrení prijatých alebo navrhovaných s cieľom napraviť Porušenie:**	
13.	**Opis opatrení určených na zmiernenie nepriaznivých dôsledkov Porušenia:**	
14.	**Navrhované doplnenie bezpečnostných opatrení:**	
15.	**Posúdenie vzniku povinnosti oznámiť Porušenie Úradu na ochranu osobných údajov podľa článku 33 GDPR:**	
16.	**Posúdenie vzniku povinnosti oznámiť Porušenie dotknutej osobe podľa článku 34 GDPR:**	
17.	**Dátum a čas oznámenia Porušenia Úradu na ochranu osobných údajov:**	
18.	**Dôvody zmeškania lehoty na oznámenie Porušenia Úradu na ochranu osobných údajov:**	
19.	**Dátum, čas a spôsobom oznámenia Porušenia dotknutým osobám**	
20.	**Vyjadrenie štatutárneho orgánu Prevádzkovateľa k Porušeniu a ďalšiemu postupu:**	

Na základe vyššie uvedeného zdokumentovania Prevádzkovateľ prijal rozhodnutie (zaškrtnúť možnosť/možností):

☐	neoznámiť Porušenie Úradu na ochranu osobných údajov SR podľa čl. 33 GDPR (v takom prípade sa Porušenie iba zdokumentuje týmto záznamom);	*„pretože Porušenie pravdepodobne **nepovedie k rizikám** pre práva a slobody fyzických osôb“*
☐	oznámiť Porušenie Úradu na ochranu osobných údajov SR podľa čl. 33 GDPR (v takom prípade oznámenie porušenia priloží k tomuto záznamu).	*„pretože Porušenie pravdepodobne **povedie k rizikám** pre práva a slobody fyzických osôb“*
☐	oznámiť Porušenie aj dotknutým osobám podľa čl. 34 GDPR a v súlade s bodom 8.3 Kódexu SAK	*„pretože Porušenie pravdepodobne **povedie k vysokým rizikám** pre práva a slobody fyzických osôb“*
☐	neoznámiť Porušenie dotknutým osobám podľa čl. 34 GDPR a v súlade s bodom 8.3 Kódexu SAK	*„pretože Porušenie pravdepodobne **nepovedie k vysokým rizikám** pre práva a slobody fyzických osôb“*

V ....., dňa.....

Vypracoval: .....

Schválil: .....

Prílohy:
- *Kópia oznámenia Porušenia Úradu na ochranu osobných údajov, v prípade, že je incident oznámený.*
- *Kópia oznámenia Porušenia dotknutým osobám, v prípade, že je incident oznámený.*

PODROBNÝ NÁVOD NA VYPLNENIE FORMULÁRA O PORUŠENÍ OCHRANY OSOBNÝCH ÚDAJOV

1.	**Dátum, miesto a čas zistenia Porušenia a jeho interné označenie:**	*/uvedie sa dátum, miesto a presný čas zistenia Porušenia, odporúča sa číslovať záznamy o Porušení alebo inak označovať/*
2.	**Kontaktné údaje zodpovednej osoby, ak je vymenovaná:**	*/uvedie sa titul, meno, priezvisko, email a telefónne číslo zodpovednej osoby, ak bola vymenovaná/*
3.	**Kontaktné údaje IT poradcu alebo IT oddelenia:**	*/uvedie sa titul, meno, priezvisko, email a telefónne číslo kontaktnej osoby IT poradcu vedúceho IT oddelenia/*
4.	**Kontaktné údaje na iné osoby disponujúce dôležitými poznatkami o Porušení:**	*/napr. interný zamestnanec, ktorý zistil alebo oznámil ambulancii Porušenie/*
5.	**Základný opis Porušenia:**	*/ambulancia vlastnými slovami opíše čo sa stalo/*
6.	**Spôsob zistenia Porušenia:**	*/napr. chýbajúce dokumenty alebo súbory, prijatie automatickej notifikácie z bezpečnostného softvéru, notifikácia neobvyklých javov v sieťovej činnosti, notifikácia analýzy logovacích údajov, hlásenie zamestnanca, hlásenie IT poradcu, oznámenie od sprostredkovateľa, činnosť zodpovednej osoby, medializácia, prijatie podozrivej elektronickej pošty, prijatie žiadosti kyber zločinca pri ransomvérovom útoku, výpadok funkcií online služieb v dôsledku Ddos útoku, poznatky získané v dôsledku aplikácie kontrolných mechanizmov zamestnávateľa voči zamestnancom a pod./*
7.	**Popis povahy Porušenia:**	*/charakterizuje sa konkrétna udalosť, ktorá bola zistená, a ktorá má potenciál ohroziť alebo porušiť integritu, dôvernosť, či dostupnosť dát, ktoré obsahujú osobné údaje. Rovnako sa vždy presne charakterizuje udalosť, ktorá viedla k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov alebo neoprávnenému prístupu k dátam obsahujúcim osobné údaje. Zároveň sa uvedie okruh dotknutých osôb zasiahnutých Bezpečnostným incidentom a ich (približný) počet, zoznam potenciálne kompromitovaných osobných údajov, ktorý je predmetom spracúvania a kvantifikácia počtu ohrozených alebo porušených dát (napr. počtom záznamov a veľkosťou dát v MB, GB, TB)./*
8.	**Identifikácia prijatých bezpečnostných opatrení, ktoré boli určené na prevenciu pred vznikom Porušenia:**	*/uvedú sa bezpečnostné opatrenia a postupy, ktoré boli v zmysle interných politík, smerníc alebo bezpečnostných projektov, určených na ochranu pred vznikom zisteného Porušenia/*
9.	**Pravdepodobné príčiny vzniku Porušenia:**	*/v prípade Porušenia s reálnym vplyvom na vznik rizika a/alebo vysokého rizika pre práva a slobody dotknutých osôb, sa interné vyšetrovanie a kontrolná činnosť Spoločnosti zameria aj na identifikáciu príčin vzniku Porušenia, pričom sa popíšu všetky relevantné skutočnosti, ktoré mali vplyv na vznik, priebeh a dopady zisteného Porušenia/* */tiež sa odporúča uviesť chronologický opis priebehu incidentu, opis hrozieb, ktoré sa realizovali, identifikáciu zraniteľností, ktoré boli využité a spôsob, akým to celé prebehlo, ďalej sa odporúča tiež uviesť zoznam dotknutých aktív, ktoré boli zasiahnuté Porušením, identifikovať a vymedziť prekonané bezpečnostné opatrenia, ak Porušenie vzniklo aj napriek prijatiu adekvátneho bezpečnostného opatrenia a uviesť predpokladaný dôvod prekonania takéhoto bezpečnostného opatrenia/* */tiež sa odporúča uviesť záznam o tom, ktoré konkrétne bezpečnostné opatrenia alebo prijaté postupy boli porušené, ak je medzi vznikom Porušenia a porušením príčinná súvislosť, ako aj pokúsiť sa identifikovať osobu alebo osoby zodpovedné za*

		porušenie povinnosti a interných pravidiel, a s tým súvisiaci vznik Porušenia/
10.	**Vzťah Porušenia a zostatkového rizika pre práva a slobody fyzických osôb:**	*/osobitne sa posúdi povaha Porušenia vo vzťahu k zostatkovým rizikám a nepokrytým rizikám, ktoré ambulancia zdokumentovala napr. vo svojom bezpečnostnom projekte podľa predchádzajúcej legislatívy*
11.	**Opis pravdepodobných následkov Porušenia:**	*/popíšu sa zistené a pravdepodobné negatívne dopady Porušenia nie len na ambulanciu a jej aktíva, ale aj napr. na povinnosť zachovávať mlčanlivosť, na osoby ktorých sa inkriminované osobné údaje týkali, na oprávnené záujmy klienta/*
12.	**Opis opatrení prijatých alebo navrhovaných s cieľom napraviť Porušenie:**	*/ambulancia uvedie všetky úkony, ktoré boli vykonané alebo ktoré sa navrhujú vykonať v konkrétnych termínoch konkrétnymi poverencami s cieľom napraviť Porušenie /*
13.	**Opis opatrení určených na zmiernenie nepriaznivých dôsledkov Porušenia:**	*/ambulancia uvedie všetky úkony, ktoré boli vykonané, alebo ktoré sa navrhujú vykonať v konkrétnych termínoch, konkrétnymi poverencami s cieľom zmierniť nepriaznivé dôsledky Porušenia/*
14.	**Navrhované doplnenie bezpečnostných opatrení:**	*/ambulancia zdokumentuje aké opatrenia sa prijali na predchádzanie obdobným incidentom ako je Porušenie v budúcnosti./*
15.	**Posúdenie vzniku povinnosti oznámiť Porušenie Úradu na ochranu osobných údajov podľa článku 33 GDPR:**	*/ambulancia odpovedá na otázku: je pravdepodobné, že Porušenie povedie k riziku pre práva a slobody fyzických osôb? Ambulancia uvedie zdôvodnenie odpovede. /*
16.	**Posúdenie vzniku povinnosti oznámiť Porušenie dotknutej osobe podľa článku 34 GDPR:**	*/ambulancia odpovedá na otázku: je pravdepodobné, že Porušenie povedie k vysokému riziku pre práva a slobody fyzických osôb spolu so zdôvodnenmí. Ambulancia by mala oznamovať Porušenie podľa čl. 34 GDPR len klientom a zamestnancom, ale nie iným fyzickým osobám/*
17.	**Dátum a čas oznámenia Porušenia Úradu na ochranu osobných údajov:**	*/uvedie sa presný dátum a čas oznámenia a priloží sa písomný dôkaz o vykonaní tohto úkonu - vypĺňa sa iba v prípade pozitívneho záveru o oznámení/*
18.	**Dôvody zmeškania lehoty na oznámenie Porušenia Úradu na ochranu osobných údajov:**	*/odôvodnenie pre nedodržanie predmetnej lehoty 72 hodín (3 dní) – vypĺňa sa iba v prípade pozitívneho záveru o oznámení a zmeškaní lehoty/*
19.	**Dátum, čas a spôsobom oznámenia Porušenia dotknutým osobám**	*/uvedie sa presný dátum a čas oznámenia, ako aj spôsob oznámenia Porušenia vo vzťahu k dotknutým osobám – Ambulancia by mala oznamovať Porušenie podľa čl. 34 GDPR len klientom a zamestnancom, ale nie iným fyzickým osobám /*
20.	**Vyjadrenie štatutárneho orgánu Prevádzkovateľa k Porušeniu a ďalšiemu postupu:**	*/štatutárny orgán sa vyjadrí k vyššie uvedenému obsahu a schváli ďalší postup (najmä rozhodnutie o oznámení/neoznámení Porušenia/*