

# BEZPEČNOSTNÝ PROJEKT OCHRANY INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

<b>Identifikačné údaje prevádzkovateľa</b>		
<b>Vypracoval:</b> funkcia:	<b>Dňa:</b>	<b>Podpis:</b>
<b>Schválil:</b> funkcia:	<b>Dňa:</b>	<b>Podpis:</b>

Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov ako i vyhláška Úradu na ochranu osobných údajov SR 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení stanovuje minimálne obsahové požiadavky na bezpečnostný projekt informačného systému.

### **Bezpečnostný projekt informačného systému musí obsahovať**

- a) názov informačného systému, na ktorý sa vzťahuje,
- b) bezpečnostný zámer,
- c) analýzu bezpečnosti informačného systému,
- d) bezpečnostnú smernicu podľa

**Bezpečnostný zámer** vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu osobných údajov pred ohrozením ich bezpečnosti. Bezpečnostný zámer obsahuje

- a) formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- b) špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia,
- c) vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti informačného systému,
- d) vymedzenie hraníc určujúcich množinu zostatkových rizík; zostatkovým rizikom sa rozumie bezpečnostné riziko, ktoré zostane úplne alebo čiastočne nepokryté bezpečnostnými opatreniami z dôvodu, že jeho miera je pre prevádzkovateľa akceptovateľná alebo ju nie je možné eliminovať vhodnými a efektívnymi bezpečnostnými opatreniami.

**Analýza bezpečnosti informačného systému** je podrobný rozbor stavu bezpečnosti informačného systému s vymedzením rozsahu jeho odolnosti a zraniteľnosti. Analýza bezpečnosti obsahuje najmä kvalitatívnu analýzu rizík tvorenú

- a) identifikáciou rizík založenou na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužitelných hrozbami a na identifikácii dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti,
- b) analýzou a ohodnotením rizík založených na určení dopadov, ktoré môžu vyplývať zo zlyhania bezpečnosti,
- c) určením reálnej pravdepodobnosti výskytu zlyhania bezpečnosti a odhadom úrovne rizík vymedzujúcim, či je riziko akceptovateľné alebo vyžaduje prijatie ďalších opatrení za využitia vopred určených kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
- d) identifikáciou a ohodnotením možností minimalizácie rizík, napríklad aplikovaním vhodných bezpečnostných opatrení, vedomým a objektívnym akceptovaním rizík, vyhnutím sa rizikám alebo prenesením súvisiacich rizík na tretie strany,

- e) výberom cieľov a opatrení na ošetrovanie rizík a vymedzením súpisu nepokrytých rizík, použitím technických noriem a určením iných metód a prostriedkov ochrany osobných údajov.

**Bezpečnostná smernica** musí obsahovať

- a) popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
- b) rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb; ak to automatizované prostriedky spracúvania osobných údajov umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby, miesta a času zabezpečí zaznamenanie každého vstupu oprávnenej osoby do informačného systému,
- b) rozsah zodpovednosti oprávnených osôb a zodpovednej osoby,
- c) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení,
- d) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možnosti efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

Uvedené body predstavujú zákonom stanovené požiadavky na bezpečnostný projekt. (Zákon č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, Vyhláška Úradu na ochranu osobných údajov SR 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení)

Nakoľko ide o pomerne komplikovanú problematiku, nedá sa poskytnúť univerzálny vzor bezpečnostného projektu. Bezpečnostný projekt musí byť vždy vypracovaný „na mieru“ konkrétneho subjektu.