

164

VYHLÁŠKA

Úradu na ochranu osobných údajov Slovenskej republiky

z 13. júna 2013

o rozsahu a dokumentácii bezpečnostných opatrení

Úrad na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“) podľa § 20 ods. 3 zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) ustanovuje:

§ 1

(1) Rozsah primeraných technických, organizačných a personálnych opatrení (ďalej len „bezpečnostné opatrenia“) musí zodpovedať konkrétnym podmienkam spracúvania osobných údajov v informačnom systéme osobných údajov (ďalej len „informačný systém“) a bezpečnostným rizikám vyplývajúcim z kategórie spracúvaných osobných údajov a zo spôsobu ich spracúvania.

(2) Pri prijímaní bezpečnostných opatrení prevádzkovateľ aplikuje najmä bezpečnostné opatrenia uvedené v prílohe, pričom rozlišuje medzi použitím automatizovaných a iných ako automatizovaných prostriedkov spracúvania osobných údajov. Pri automatizovaných prostriedkoch spracúvania osobných údajov prevádzkovateľ prostredníctvom bezpečnostných opatrení zabezpečí odolnosť automatizovanej časti informačného systému proti škodlivým kódom (napríklad počítačový vírus) a nežiaducim modifikáciám informačného systému, ako aj pravidelné a bezpečné zálohovanie spracúvaných osobných údajov.

(3) Prijatím bezpečnostných opatrení prevádzkovateľ neoprávneným osobám znemožní akýkoľvek nedovolený prístup k spracúvaným osobným údajom, manipuláciu s technickými zariadeniami určenými na spracúvanie osobných údajov alebo na ich ochranu a manipuláciu s nosičmi osobných údajov a oprávneným osobám zabezpečí prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení podľa § 21 zákona.

§ 2

(1) Dokumentácia prijatých bezpečnostných opatrení (ďalej len „dokumentácia“) popisuje celý proces spracúvania osobných údajov od ich získavania po ich likvidáciu; obsah dokumentácie sa zhoduje so skutočným stavom pri spracúvaní osobných údajov.

(2) Bezpečnostné opatrenia musia byť zdokumentované prehľadne a jednoznačne. Dokumentácia uvedená v § 3, 4 a 5 môže obsahovať presné odkazy na iné dokumenty prevádzkovateľa alebo na ich časti, kde sú

prijaté bezpečnostné opatrenia už zdokumentované;¹⁾ v uvedenom prípade sa iné dokumenty prevádzkovateľa alebo ich časti považujú za dokumentáciu podľa § 3, 4 a 5.

§ 3

Ak sú osobné údaje spracúvané v informačnom systéme, ktorý nie je prepojený s verejne prístupnou počítačovou sieťou, pričom nejde o spracúvanie osobitných kategórií osobných údajov podľa § 13 zákona, dokumentácia podľa § 19 ods. 1 zákona obsahuje

- a) písomnú zmluvu podľa § 8 zákona, ak prevádzkovateľ poveril spracúvaním osobných údajov sprostredkovateľa,
- b) písomné záznamy o poučení oprávnených osôb podľa § 21 zákona,
- c) písomné poverenie zodpovednej osoby podľa § 23 zákona, ak prevádzkovateľovi taká povinnosť vznikla,
- d) záznamy o kontrolnej činnosti prevádzkovateľa zameranej na dodržiavanie bezpečnosti informačného systému podľa § 4 ods. 1 písm. d),
- e) záznamy o zistených bezpečnostných incidentoch vplyvajúcich na bezpečnosť osobných údajov a záznamy o naviazaných postupoch, ktorými prevádzkovateľ zabezpečil obnovenie bezpečnosti informačného systému.

§ 4

Bezpečnostná smernica podľa § 19 ods. 2 zákona obsahuje

- 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,
- c) rozsah zodpovednosti oprávnených osôb a zodpovednej osoby,
- d) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení,
- e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení

¹⁾ Napríklad § 28 výnosu Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy.

na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

§ 5

(1) Bezpečnostný projekt informačného systému (ďalej len „bezpečnostný projekt“) podľa § 19 ods. 3 zákona obsahuje

- a) názov informačného systému, na ktorý sa vzťahuje,
- b) bezpečnostný zámer,
- c) analýzu bezpečnosti informačného systému,
- d) bezpečnostnú smernicu podľa § 4.

(2) 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.

(3) 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 zraniteľnosti zneužívateľných 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 noriem²⁾ a určením iných metód a prostriedkov ochrany osobných údajov.

(4) Ak prevádzkovateľ spracúva osobné údaje vo viacerých informačných systémoch, z ktorých aspoň jeden vyžaduje vypracovanie bezpečnostného projektu, môže vypracovať jeden bezpečnostný projekt pre všetky informačné systémy, v ktorom zreteľne označí časti týkajúce sa jednotlivých informačných systémov.

§ 6

Táto vyhláška nadobúda účinnosť 1. júla 2013.

Eleonóra Kročianová v. r.

²⁾ Napríklad STN ISO/IEC 27001, STN ISO/IEC 27002, výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z.

**Príloha
k vyhláske č. 164/2013 Z. z.****BEZPEČNOSTNÉ OPATRENIA****1. Technické opatrenia**

- 1.1 Technické opatrenia realizované prostriedkami fyzickej povahy
 - 1.1.1 Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarňa signalizácia)
 - 1.1.2 Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia)
 - 1.1.3 Umiestnenie informačného systému v chránenom priestore (ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia)
 - 1.1.4 Bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov v uzamykateľných skrinách alebo trezoroch)
 - 1.1.5 Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému (napr. vhodné umiestnenie zobrazovacích jednotiek)
 - 1.1.6 Zariadenie na ničenie fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín)
- 1.2 Ochrana pred neoprávneným prístupom
 - 1.2.1 Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí
 - 1.2.2 Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza
- 1.3 Riadenie prístupu oprávnených osôb
 - 1.3.1 Identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme
 - 1.3.2 Zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému
- 1.4 Ochrana proti škodlivému kódu
 - 1.4.1 Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov
 - 1.4.2 Ochrana pred nevyžiadanou elektronickou poštou
 - 1.4.3 Používanie legálneho a prevádzkovateľom schváleného softvéru
 - 1.4.4 Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete
- 1.5 Sieťová bezpečnosť
 - 1.5.1 Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou
 - 1.5.2 Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačovej siete
 - 1.5.3 Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall)
 - 1.5.4 Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam)
 - 1.5.5 Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok)
- 1.6 Zálohovanie
 - 1.6.1 Test funkcionality dátového nosiča zálohy
 - 1.6.2 Vytváranie záloh s vopred zvolenou periodicitou
 - 1.6.3 Test obnovy informačného systému zo zálohy
 - 1.6.4 Bezpečné ukladanie záloh
- 1.7 Likvidácia osobných údajov a dátových nosičov
 - 1.7.1 Bezpečné vymazanie osobných údajov z dátových nosičov
 - 1.7.2 Zariadenie na likvidáciu dátových nosičov osobných údajov
- 1.8 Aktualizácia operačného systému a programového aplikačného vybavenia

2. Organizačné opatrenia**2.1 Personálne opatrenia**

- 2.1.1 Písomné poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi

- 2.1.1.1 Poučenie o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie
- 2.1.1.2 Vymedzenie osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh
- 2.1.1.3 Určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov
- 2.1.1.4 Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi
- 2.1.1.5 Vymedzenie zodpovednosti za porušenie zákona
- 2.1.2 Poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov)
- 2.1.3 Písomné poverenie zodpovednej osoby podľa § 23 zákona, ak prevádzkovateľ spracúva osobné údaje prostredníctvom 20 alebo viac oprávnených osôb
- 2.1.4 Oboznámenie oprávnených osôb s bezpečnostnými smernicami
- 2.1.5 Vzdelávanie oprávnených osôb (napr. právna oblasť, oblasť informačných technológií)
- 2.1.6 Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti)
- 2.2 Vedenie zoznamu aktív a jeho aktualizácia
- 2.3 Riadenie prístupu oprávnených osôb k osobným údajom
 - 2.3.1 Kontrola vstupu do objektu a chránených priestorov prevádzkovateľa (napr. prostredníctvom technických a personálnych opatrení)
 - 2.3.2 Správa kľúčov (individuálne pridelovanie kľúčov, bezpečné uloženie rezervných kľúčov)
 - 2.3.3 Pridelovanie prístupových práv a úrovni prístupu (rolí) oprávnených osôb
 - 2.3.4 Správa hesiel
 - 2.3.5 Vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru)
- 2.4 Organizácia spracúvania osobných údajov
 - 2.4.1 Pravidlá spracúvania osobných údajov v chránenom priestore
 - 2.4.2 Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby
 - 2.4.3 Režim údržby a upratovania chránených priestorov
 - 2.4.4 Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá
 - 2.4.4.1 Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti
 - 2.4.4.2 Pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovednosti
 - 2.4.4.3 Pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovednosti
- 2.5 Likvidácia osobných údajov
 - 2.5.1 Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov)
- 2.6 Bezpečnostné incidenty
 - 2.6.1 Postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení
 - 2.6.2 Evidencia bezpečnostných incidentov a použitých riešení
 - 2.6.3 Postup pri riešení jednotlivých typov bezpečnostných incidentov
 - 2.6.4 Identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov
 - 2.6.5 Postupy pri haváriách, poruchách a iných mimoriadnych situáciách (napr. oznamovanie bezpečnostných incidentov)
 - 2.6.6 Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného počítača)
- 2.7 Kontrolná činnosť
 - 2.7.1 Kontrolná činnosť prevádzkovateľa zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému)
 - 2.7.2 Informovanie oprávnených osôb o kontrolnom mechanizme,³⁾ ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania)

³⁾ Čl. 11 a § 13 zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov.