**Návrh**

**VYHLÁŠKA**

**Úradu na ochranu osobných údajov Slovenskej republiky**

z  ............ 2013

**o rozsahu a dokumentácii bezpečnostných opatrení**

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

§ 1

**Predmet úpravy**

Táto vyhláška upravuje podrobnosti o rozsahu a dokumentácii bezpečnostných opatrení na ochranu informačných systémov, v ktorých sú spracúvané osobné údaje dotknutých osôb.

§ 2

**Vymedzenie niektorých pojmov**

Na účely tejto vyhlášky sa rozumie

technickými opatreniami systém fyzickej a informačno-technologickej ochrany informačného systému,

personálnymi opatreniami systém ochrany informačného systému pred zlyhaním ľudského faktora,

organizačnými opatreniami systém koordinácie technických opatrení, personálnych opatrení, prípadne ďalších opatrení prevádzkovateľa zameraných na ochranu informačného systému,

objektom budova alebo iný stavebne alebo inak ohraničený priestor, v ktorom sa nachádzajú chránené priestory,

chráneným priestorom pracovisko určené na spracúvanie osobných údajov oprávnenými osobami prevádzkovateľa,

okolím systému prostredie, v ktorom je informačný systém umiestnený a z ktorého pre informačný systém vyplývajú riziká,

aktívami najmä objekty, hardvér, softvér, osobné údaje, kvalifikované osoby a ďalšie prvky informačného systému, ktoré prevádzkovateľ považuje za dôležité,

bezpečnostným incidentom akýkoľvek spôsob narušenia bezpečnosti informačného systému prevádzkovateľa,

hrozbou možná príčina bezpečnostného incidentu,

bezpečnostným rizikom pravdepodobnosť, že hrozba využije zraniteľnosť aktív, čím nepriaznivo ovplyvní dôvernosť, integritu alebo dostupnosť spracúvaných osobných údajov, ako aj vážnosť dopadu využitia takejto zraniteľnosti,

dôvernosťou osobných údajov záruka ich prístupnosti výlučne oprávneným osobám,

integritou osobných údajov záruka ich celistvosti a neporušenosti,

dostupnosťou osobných údajov záruka, že osobné údaje sú na požiadanie oprávnenej osobe k dispozícii,

zvyškovým rizikom riziko, ktoré po prijatí bezpečnostných opatrení na zníženie alebo elimináciu rizík ostalo nepokryté,

identifikátorom reťazec alfanumerických alebo iných znakov, ktoré jednoznačne identifikujú osobu oprávnenú na spracúvanie osobných údajov; identifikátorom je napríklad prihlasovacie meno a heslo,

identifikáciou jednoznačné určenie identity oprávnenej osoby prostredníctvom identifikátora,

autentizáciou proces overenia totožnosti oprávnenej osoby podľa požadovanej miery záruky na princípe porovnania identifikátora s hodnotou uloženou v informačnom systéme,

autorizáciou priradenie používateľských práv k oprávnenej osobe, ktoré nadväzuje na jej úspešnú identifikáciu a autentizáciu,

prepojením s verejne prístupnou počítačovou sieťou priame (počítač – internet) alebo nepriame (počítač – lokálna sieť – internet) spojenie infomačného systému s verejne prístupnou počítačovou sieťou; informačný systém sa považuje za prepojený s verejne prístupnou počítačovou sieťou aj vtedy, ak je s ňou spájaný príležitostne.

§ 3

**Účel, rozsah a dokumentácia bezpečnostných opatrení**

Účelom prijatia bezpečnostných opatrení je vytvorenie funkčného, efektívneho a z hľadiska finančnej náročnosti optimálneho systému ochrany osobných údajov. Povinnosť prevádzkovateľa prijať primerané bezpečnostné opatrenia podľa § 19 ods. 1 zákona sa vzťahuje na každý informačný systém.

Bezpečnostné opatrenia určujú záväzné pravidlá spracúvania osobných údajov, ktoré zabezpečujú primeranú úroveň ochrany informačných systémov z hľadiska ich bezpečnosti, spoľahlivosti a funkčnosti, ako aj z hľadiska zachovania dôvernosti, integrity a dostupnosti spracúvaných osobných údajov. Rozsah bezpečnostných opatrení zodpovedá najmä bezpečnostným rizikám vyplývajúcim z kategórie spracúvaných osobných údajov a zo spôsobu ich spracúvania.

Bezpečnostné opatrenia prijme prevádzkovateľ v rozsahu zodpovedajúcom konkrétnym podmienkam spracúvania osobných údajov, pričom prihliada najmä na dôvernosť a dôležitosť spracúvaných osobných údajov, na riziká spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému a na potenciálne dopady bezpečnostných incidentov, najmä na počet dotknutých osôb a mieru ohrozenia ich súkromného a rodinného života.

Prevádzkovateľ dokumentuje prijaté bezpečnostné opatrenia prehľadne a jednoznačne, pričom rozlišuje použitie automatizovaných a iných ako automatizovaných prostriedkov spracúvania osobných údajov. Dokumentácia prijatých bezpečnostných opatrení (ďalej len „dokumentácia“) popisuje celý proces spracúvania osobných údajov od ich získavania po likvidáciu. Za zhodu obsahu dokumentácie so skutočným stavom zodpovedá prevádzkovateľ.

Rozsah dokumentácie zodpovedá najmä bezpečnostným rizikám vyplývajúcim z kategórie spracúvaných osobných údajov a zo spôsobu ich spracúvania. Dokumentácia môže obsahovať presné odkazy na iné dokumenty prevádzkovateľa alebo na ich časti, kde sú prijaté bezpečnostné opatrenia už zdokumentované.

Zameranie bezpečnostných opatrení je uvedené v Prílohe č. 1; tým nie je dotknutá povinnosť prevádzkovateľa postupovať podľa § 19 ods. 1 zákona.

§ 4

**Základná dokumentácia**

(1) Ak prevádzkovateľ spracúva osobné údaje v informačnom systéme, ktorý nie je prepojený s verejne prístupnou počítačovou sieťou, pričom nejde o spracúvanie osobitných kategórií osobných údajov podľa § 13 zákona, okrem povinností vyplývajúcich zo zákona priebežne dokumentuje aj kontrolné činnosti zamerané na dodržiavanie bezpečnosti informačného systému a bezpečnostné incidenty. Povinnosti prevádzkovateľa ustanovené v § 19 ods. 1 a 5 zákona tým nie sú dotknuté.

(2) Dokumentácia podľa odseku 1 obsahuje najmä

písomnú zmluvu podľa § 8 zákona, ak prevádzkovateľ poveril spracúvaním osobných údajov sprostredkovateľa,

písomné záznamy o poučení oprávnených osôb podľa § 21 zákona,

písomné poverenie zodpovednej osoby podľa § 23 zákona, ak prevádzkovateľovi taká povinnosť vznikla,

písomné záznamy o kontrolnej činnosti prevádzkovateľa zameranej na dodržiavanie bezpečnosti informačného systému podľa § 5 ods. 2 písm. d),

písomné záznamy o zistených bezpečnostných incidentoch a písomné záznamy o postupoch, ktorými prevádzkovateľ zabezpečil obnovenie bezpečnosti systému.

§ 5

**Bezpečnostná smernica**

(1) Povinnosť zdokumentovať bezpečnostné opatrenia v bezpečnostnej smernici sa vzťahuje na prevádzkovateľa, ktorý spracúva osobné údaje v informačnom systéme podľa § 19 ods. 2 zákona.

(2) Bezpečnostná smernica obsahuje najmä

popis technických,  organizačných a  personálnych opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,

rozsah oprávnení, popis povolených činností a spôsob identifikácie a autentizácie jednotlivých oprávnených osôb,

rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,

spôsob, formu a  periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,

postupy pri haváriách, poruchách a  iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie rizika vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou, poruchou alebo inou mimoriadnou situáciou.

(3) Účelom bezpečnostných opatrení podľa odseku 1 a 2 je najmä

a) neoprávneným osobám znemožniť 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,

b) oprávneným osobám prevádzkovateľa zabezpečiť prístup k osobným údajom v rozsahu potrebnom na plnenie ich povinností alebo úloh obsiahnutých v poučení podľa § 21 zákona; ak to automatizované prostriedky spracúvania umožňujú, prevádzkovateľ na účel spätnej identifikácie osoby, miesta a času vstupu osobných údajov, ktorých sa vstup týkal, zabezpečí zaznamenanie každého vstupu oprávnenej osoby do informačného systému,

c) zabezpečiť odolnosť automatizovanej časti informačného systému proti škodlivým kódom (napríklad počítačový vírus) a nežiaducej modifikácii systému, ako aj zabezpečiť pravidelné a bezpečné zálohovanie spracúvaných osobných údajov.

§ 6

**Bezpečnostný projekt**

(1) Povinnosť vypracovať bezpečnostný projekt sa vzťahuje na prevádzkovateľa, ktorý spracúva osobné údaje v informačnom systéme podľa § 19 ods. 3 zákona.

(2) Bezpečnostný projekt obsahuje najmä

názov informačného systému, na ktorý sa vzťahuje,

bezpečnostný zámer,

analýzu bezpečnosti informačného systému,

bezpečnostnú smernicu.

(3) Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému pred ohrozením jeho bezpečnosti. Bezpečnostný zámer obsahuje najmä

formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,

špecifikáciu technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v infomačnom systéme a spôsob ich využitia,

vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti,

vymedzenie hraníc určujúcich množinu zvyškových rizík.

(4) 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, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva infomačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb pre dôvernosť, integritu a dostupnosť spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení na elimináciu alebo minimalizáciu vplyvu rizík a s vymedzením súpisu nepokrytých rizík,

použitie bezpečnostných štandardov[[1]](#footnote-2)) a určenie iných metód a prostriedkov ochrany osobných údajov; súčasťou analýzy bezpečnosti informačného systému je posúdenie zhody navrhnutých bezpečnostných opatrení s použitými bezpečnostnými štandardami, metódami a prostriedkami.

(5) Na bezpečnostnú smernicu sa vzťahujú ustanovenia § 5 ods. 2 a 3.

§ 7

**Spoločné ustanovenie k bezpečnostným opatreniam**

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.

§ 8

**Účinnosť**

Táto vyhláška nadobúda účinnosť 1. apríla 2013.

Príloha č. 1

k vyhláške č. ......../2012 Z. z.

**ZAMERANIE BEZPEČNOSTNÝCH OPATRENÍ**

Technické opatrenia zamerané na fyzickú ochranu informačného systému

* 1. Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. poplachový systém narušenia objektu, protipožiarny systém)
	2. Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia)
	3. Umiestnenie informačného systému v chránenom priestore (ochrana informačného systému pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia)
	4. Bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch)
	5. Zamedzenie náhodného odpozerania osobných údajov zo zobrazovacích jednotiek informačného systému (napr. vhodné umiestnenie zobrazovancích jednotiek)
	6. Zariadenie na likvidáciu fyzických nosičov osobných údajov (napr. zariadenie na skartovanie listín)

Technické opatrenia zamerané na informačno-technologickú ochranu informačného systému

* 1. Ochrana pred neoprávneným prístupom
		1. Šifrová ochrana obsahu dátových nosičov
		2. Pravidlá prístupu tretích strán k informačnému systému, ak k takémuto prístupu dochádza
	2. Riadenie prístupu oprávnených osôb
		1. Identifikácia, autentizácia a autorizácia oprávnených osôb v informačnom systéme
		2. Zaznamenávanie vstupov jednotlivých oprávnených osôb do informačného systému
	3. Ochrana proti škodlivému kódu
		1. Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete
		2. Ochrana pred nevyžiadanou elektronickou poštou
		3. Používanie legálneho a prevádzkovateľom schváleného softvéru
		4. Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete
	4. Sieťová bezpečnosť
		1. Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje, s verejne prístupnou počítačovou sieťou
		2. Evidencia všetkých miest prepojenia sietí vrátane verejne prístupnej počítačove siete
		3. Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (napr. firewall)
		4. Pravidlá prístupu do verejne prístupnej počítačovej siete (napr. zamedzenie pripojenia k určitým webovým sídlam)
		5. Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok)
	5. Zálohovanie
		1. Test funkcionality dátového nosiča zálohy
		2. Vytváranie záloh s vopred zvolenou periodicitou
		3. Test obnovy informačného systému zo zálohy
		4. Bezpečné ukladanie záloh
	6. Likvidácia osobných údajov a dátových nosičov
		1. Bezpečné vymazanie osobných údajov z dátových nosičov
		2. Zariadenie na likvidáciu dátových nosičov osobných údajov
	7. Aktualizácia operačného systému a programového aplikačného vybavenia

Personálne opatrenia

* 1. Písomné poučenie oprávnených osôb pred uskutočnením prvej spracovateľskej operácie s osobnými údajmi
		1. Poučenie o právach a povinnostiach vyplývajúcich zo zákona a zodpovednosti za ich porušenie
		2. Vymedzenie osobných údajov, ku ktorým má mať konkrétna oprávnená osoba prístup na účel plnenia jej povinností alebo úloh
		3. Určenie postupov, ktoré je oprávnená osoba povinná uplatňovať pri spracúvaní osobných údajov
		4. Vymedzenie zakázaných postupov alebo operácií s osobnými údajmi
		5. Vymedzenie zodpovednosti za porušenie zákona
	2. Poučenie oprávnených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov)
	3. Oboznámenie oprávnených osôb s bezpečnostnými smernicami
	4. Vzdelávanie oprávnených osôb (napr. právna oblasť, oblasť informačných technológií)
	5. 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)

Organizačné opatrenia

* 1. Vedenie zoznamu aktív a jeho aktualizácia
	2. Písomné poverenie zodpovednej osoby podľa § 23 zákona, ak prevádzkovateľ spracúva osobné údaje prostredníctvom 20 a viac oprávnených osôb
	3. Riadený prístup oprávnených osôb k osobným údajom
		1. Kontrola vstupu do objektu a chránených priestorov prevádzkovateľa (napr. prostredníctvom technických a personálnych opatrení)
		2. Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov)
		3. Prideľovanie prístupových práv a úrovní prístupu (rolí) oprávnených osôb
		4. Správa hesiel
		5. Vzájomné zastupovanie oprávnených osôb (napr. v prípade nehody, práceneschopnosti, ukončenia pracovného alebo obdobného pomeru)
	4. Organizácia spracúvania osobných údajov
		1. Pravidlá spracúvania osobných údajov v chránenom priestore
		2. Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby
		3. Režim údržby a upratovania chránených priestorov
		4. Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá
			1. Záväzné pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti
			2. Záväzné pravidlá používania automatizovaných prostiedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovednosti
			3. Záväzné pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovednosti
	5. Likvidácia osobných údajov
		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)
	6. Bezpečnostné incidenty
		1. Postup pri ohlasovaní bezpečnostných incidentov a zistených zraniteľných miest informačného systému na účel včasného prijatia preventívnych alebo nápravných opatrení
		2. Evidencia bezpečnostných incidentov a použitých riešení
		3. Postup pri riešení jednotlivých typov bezpečnostných incidentov
		4. Identifikácia, evidencia a odstraňovanie následkov bezpečnostných incidentov
		5. Záväzné postupy pri haváriách, poruchách a iných mimoriadnych situáciách (napr. oznamovanie bezpečnostných incidentov)
		6. Postup pri poruche, údržbe alebo oprave automatizovaných prostiedkov spracúvania (napr. ochrana osobných údajov na pevnom disku opravovaného počítača)
	7. Kontrolná činnosť
		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. Informovanie oprávnených osôb o kontrolnom mechanizme,[[2]](#footnote-3)) ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania)
1. ) Napríklad STN ISO/IEC 27001, STN ISO/IEC 27002, Výnos Ministerstva financií Slovenskej republiky č. 312/2010 o štandardoch pre informačné systémy verejnej správy. [↑](#footnote-ref-2)
2. ) Čl. 11 zákona č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov. [↑](#footnote-ref-3)