BEZPEČNOSŤ OSOBNÝCH ÚDAJOV – BEZPEČNOSTNÝ PROJEKT

Dňa 01.07.2013 nadobudol účinnosť zákon č. 122/2013 Z.z. o ochrane osobných údajov, ktorý nahradil doterajší zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov. V tejto súvislosti sa poskytovatelia zdravotnej starostlivosti na základe ponúk od rôznych spoločností na vypracovanie bezpečnostného projektu pýtajú, či sú povinní mať vypracovaný bezpečnostný projekt.

Ak boli splnené podmienky doterajšieho zákona č. 428/2002 Z.z., museli mať poskytovatelia zdravotnej starostlivosti bezpečnostný projekt vypracovaný aj pred nadobudnutím účinnosti zákona č. 122/2013 Z.z., pričom možno konštatovať, že táto povinnosť sa vzťahovala na väčšinu poskytovateľov zdravotnej starostlivosti.

Kto je povinný mať vypracovaný bezpečnostný projekt a kto môže bezpečnostný projekt vypracovať?

Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ. Prevádzkovateľom je každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky ich spracúvania a spracúva osobné údaje vo vlastnom mene. Ak účel, prípadne aj podmienky spracúvania osobných údajov ustanovuje všeobecne záväzný predpis prevádzkovateľom je ten, kto je na plnenie účelu spracúvania za prevádzkovateľa ustanovený alebo kto spĺňa zákonom, podmienky. Každý poskytovateľ zdravotnej starostlivosti vzhľadom k tomu, že spracováva osobné údaje pacientov má právne postavenie prevádzkovateľa.

Prevádzkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel prijme primerané technické, organizačné a personálne opatrenia (ďalej len „bezpečnostné opatrenia“) zodpovedajúce spôsobu spracúvania osobných údajov, pričom berie do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.

Bezpečnostné opatrenia prevádzkovateľ informačného systému zdokumentuje v **bezpečnostnej smernici**, ak v informačnom systéme
a) prepojenom s verejne prístupnou počítačovou sieťou nespracúva osobitné kategórie osobných údajov[1], alebo
b) neprepojenom s verejne prístupnou počítačovou sieťou spracúva osobitné kategórie osobných údajov.

Bezpečnostné opatrenia podľa prevádzkovateľ zdokumentuje v **bezpečnostnom projekte informačného systému**, ak
a) v informačnom systéme prepojenom s verejne prístupnou počítačovou sieťou spracúva osobitné kategórie osobných údajov, alebo
b) informačný systém slúži na zabezpečenie verejného záujmu podľa § 3 ods. 1 zákona č. 122/2013 Z.z.;

Každý poskytovateľ zdravotnej starostlivosti, ktorý spracováva rodné číslo alebo zdravotnú dokumentáciu v počítači pripojenom na internet, je povinný prijať bezpečnostné opatrenia vo forme bezpečnostného projektu. Ak tieto údaje spracúva v počítači nepripojenom na internet, musí prijať bezpečnostné opatrenia vo forme bezpečnostnej smernice, bezpečnostný projekt vypracovať nemusí. Avšak vzhľadom na plánovanú elektronizáciu zdravotníctva sa poskytovatelia zdravotnej starostlivosti v budúcnosti tejto povinnosti zrejme nevyhnú.

Na vypracovanie bezpečnostného projektu nie je potrebné osobitné oprávnenie. Bezpečnostný projekt si môže prevádzkovateľ informačného systému vypracovať aj sám.

---

1 Osobitné kategórie osobných údajov - osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách, údaje týkajúce sa zdravia alebo pohlavného života, rodné číslo, údaje o psychickej identite fyzickej osoby alebo o jej psychickej pracovnej spôsobilosti, biometrické údaje, údaje o porušení ustanovení zakladajúcich trestnú zodpovednosť alebo administratívnoprávnu zodpovednosť.

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.

Čo je bezpečnostný projekt a čo musí obsahovať?

Bezpečnostný projekt vymedzuje rozsah a spôsob bezpečnostných opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

Bezpečnostný projekt musí obsahovať:
1. názov informačného systému, na ktorý sa vzťahuje,
2. bezpečnostný zámer,
3. analýzu bezpečnosti informačného systému,
4. bezpečnostnú smernicu.

Ad) 1

Okrem názvu informačného systému (poskytovatelia zdravotnej starostlivosti spravidla prevádzkujú minimálne dva informačné systémy, v ktorých spracúvajú osobné údaje: informačný systém zdravotná dokumentácia, personálny a mzdový informačný systému), je potrebné v bezpečnostnom projekte identifikovať prevádzkovateľa informačného systému (poskytovateľa zdravotnej starostlivosti), zoznam chránených osobných údajov, identifikovať osobu zodpovednú za vypracovanie bezpečnostného projektu.

Ad 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 - definujú sa ciele napr. ochrana informačného systému pred neoprávneným prístupom, poškodením, odcudzením. Minimálne požadované bezpečnostné opatrenia tvorí zoznam bezpečnostných opatrení, ktoré prevádzkovateľ minimálne požaduje, aby boli zabezpečené definované ciele – napr. uzamykateľná ohňovzdorná kartotéka, bezpečnostné dvere, elektronické zabezpečovacie systémy.

b) špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia - popis všetkých bezpečnostných opatrení zabezpečujúcich ochranu informačného systému v čase vypracovávania bezpečnostného projektu. Zoznam možných bezpečnostných opatrení obsahuje príloha vyhlášky Úradu na ochranu osobných údajov č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení.

c) vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti informačného systému – v tejto časti bezpečnostný projekt obsahuje najmä:

- adresy objektov, v ktorých sa informačný systém nachádza, opis týchto objektov a chránených priestorov s vymedzením hranice chránených priestorov spolu s opisom činností, ktoré sa budú v chránených priestoroch vykonávať.
- identifikácia softvéru použitého pri spracúvaní osobných údajov s použitím automatizovaných prostriedkov spracúvania,
- zoznam hlavných aktív spracúvania osobných údajov – najmä počítače a ich množstvo, zdravotná dokumentácia, nosiče dátových informácii
- opis technológie prepojenia informačného systému na verejne prístupnú počítačovú sieť spolu s opisom bezpečnostných mechanizmov prepojenia a spôsob prenosu osobných údajov medzi jednotlivými aktívami informačného systému, vymedzenie oprávnených osôb a úrovní ich prístupov.

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 – napr. narušenie bezpečnosti osobných údajov z dôvodu živelnej pohromy (zemetrasenie), dlhodobého výpadku elektrickej energie, vyhlásenia vojnového stavu.

Ad 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 zraniteľností zneužiteľných hrozbami a na identifikácii dopadov na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti - hrozbami sú najmä: neoprávnený prístup k aktívam, použitie aktív neoprávnenými osobami, výpadok alebo kolísanie elektrického prúdu, škodlivý softvér, požiar, povodeň, blesk alebo iné živelné pohromy.

b) analýzou a ohodnotením rizík založených na určení dopadov, ktoré môžu vyplynúť zo zlyhania bezpečnosti – napr.

Hrozba	**Možné riziko**	**Dopad rizika**
Prístup neoprávnených osôb	Zmena, likvidácia alebo zneužitie osobných údajov	Vážny

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 – napr.

Hrozba	**Pravdepodobnosť výskytu**	**Úroveň rizika**
Zemetrasenie	Nízka	Nízka - riziko je akceptovateľné, nevyžaduje sa prijatie žiadneho opatrenia
Výpadok elektrickej energie	Nízka	Stredná - opatrenie za účelom eliminácie rizika by malo byť prijaté
Prístup neoprávnených osôb	Vysoká	Vysoká - opatrenie za účelom eliminácie rizika by musí byť prijaté

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, napr.

Hrozba	**Úroveň rizika**	**Existujúce opatrenia**	**Navrhované opatrenie na minimalizáciu rizika**
Prístup neoprávnených osôb	Vysoká	Žiadne	Kontrola vstupu do objektu a chránených priestorov video-zvončekom

e) výberom cieľov a opatrení na ošetrenie rizík a vymedzením súpisu nepokrytých rizík, použitím technických noriem a určením iných metód a prostriedkov ochrany osobných údajov – na základe vykonanej analýzy sa vyberú ciele a opatrenia za účelom zvýšenie ochrany osobných údajov; zoznam rizík, resp. hrozieb, ktoré ostanú nepokryté navrhovanými bezpečnostnými opatreniami – napr. živelné pohromy, prírodná katastrofa (zemetrasenie, povodeň).

Ad 4) Bezpečnostná smernica obsahuje:

a) popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach – uvedie sa napĺňanie konkrétnych technických, organizačných bezpečnostných opatrení v praxi (napr. bezpečnostné dvere, poučenie oprávnených osôb, automatická aktualizácia antivírových programov, periodické vytváranie záloh, likvidácia osobných údajov).

Zoznam možných bezpečnostných opatrení obsahuje príloha vyhlášky Úradu na ochranu osobných údajov č. 164/2013 Z.z. o rozsahu a dokumentácii bezpečnostných opatrení.

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 – potrebné vymedziť jednotlivé oprávnené osoby spravidla podľa pracovných pozícii, ktoré prichádzajú do styku s osobnými údajmi a spracúvavajú ich v rozsahu a spôsobom určeným v poučení, vymedziť operácie, na ktoré sú konkrétne oprávnené osoby pri spracúvaní osobných údajov oprávnené (zoskupovanie, likvidácia, využívanie, prepracúvanie); spôsobom identifikácie a autentizácie jednotlivých oprávnených osôb sa rozumie napríklad prihlásenie sa do počítača, počítačovej siete, aplikácie, v ktorej je vedená zdravotná dokumentácia heslom, heslom a prihlasovacím menom, prípadne iným spôsobom.

c) rozsah zodpovednosti oprávnených osôb a zodpovednej osoby,

Oprávnené osoby sú napr.:

- povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku,
- povinné dodržiavať prevádzkový poriadok objektu, bezpečnostné požiarne smernice,
- nesmú dočasne alebo na trvalo vypínať antivírový softvér,
- sú povinné bezodkladne oznamovať poverenej osobe poruchy na osobnom počítači, serveri, výstražné hlásenia antivírového softvéru, resp. iné havárie na technickom vybavení.

Povinnosti zodpovednej osoby vymenúva § 27 zákona č. 122/2013 Z.z.

d) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení - kontrolné činnosti by sa vzhľadom na charakter osobných údajov, ktoré poskytovatelia zdravotnej starostlivosti spracuvávajú mali vykonávať aspoň štvrťročne. Predmetom kontroly je najmä napĺňanie bezpečnostných opatrení v praxi. Spôsob a forma zavisí od konkrétneho prevádzkovateľa a konkrétneho bezpečnostného opatrenia. O kontrole sa vyhotovuje záznam.

e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení – táto časť obsahuje najmä: identifikáciu možných havárii, porúch a mimoriadnych situácii, identifikácia aktív a subjektov dotknutých týmito udalosťami, preventívne opatrenia smerujúce k zníženie negatívnych následkov týchto udalostí (napr. zálohovanie), postup obnovy informačného systému, čas a náklady potrebné na obnovu informačného systému, aby sa informačný systém obnovil do riadnej prevádzky (rekonštrukcia zdravotnej dokumentácie).

<u>Ďalšie dokumenty, ktoré je potrebné mať vypracované v súvislosti s ochranou osobných údajov:</u>

- písomná zmluva podľa § 8 zákona č. 122/2013 Z.z., ak prevádzkovateľ poveril spracúvaním

osobných údajov sprostredkovateľa (osoba, ktorá spracuváva osobné údaje v mene prevádzkovateľa - napr. firma poskytujúca prevádzkovateľovi účtovnícke a personalistické služby).

- písomné záznamy o poučení oprávnených osôb[2] podľa § 21 zákona č. 122/2013 Z.z.
  - prevádzkovateľ je povinný poučiť oprávnenú osobu o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie pred uskutočnením prvej operácie s osobnými údajmi. Poučenie obsahuje najmä rozsah oprávnení, popis povolených činností a podmienky spracúvania osobných údajov.

- písomné poverenie zodpovednej osoby podľa § 23 zákona, ak prevádzkovateľovi taká povinnosť vznikla a oznámenie o poverení zodpovednej osoby - ak prevádzkovateľ spracúva osobné údaje prostredníctvom 20 a viac oprávnených osôb, je povinný najneskôr v lehote 60 dní od začatia ich spracúvania výkonom dohľadu písomne poveriť zodpovednú osobu alebo viaceré zodpovedné osoby. Zároveň o poverení zodpovednej osoby je je povinný informovať Úrad na ochranu osobných údajov bez zbytočného odkladu, najneskôr do 30 dní odo dňa poverenia zodpovednej osoby doporučenou zásielkou.

- záznamy o kontrolnej činnosti prevádzkovateľa zameranej na dodržiavanie bezpečnosti informačného systému – záznam obsahuje najmä: meno a priezvisko kontrolujúcej osoby, predmet kontroly, kontrolné zistenia, opatrenia na odstránenie nedostatkov zistených kontrolou, dátum kontroly, podpis kontrolujúcej osoby.

- záznamy o zistených bezpečnostných incidentoch vyplývajúcich na bezpečnosť osobných údajov a záznamy o nadväzných postupoch, ktorými prevádzkovateľ zabezpečil obnovenie bezpečnosti informačného systému.

- evidencia informačného systému, ak informačný systém nepodliehajú registrácii alebo osobitnej registrácii. Vzor evidencie je možné nájsť na stránke Úradu na ochranu osobných údajov. Povinnosť registrácie sa vzťahuje na všetky informačné systémy, v ktorých sa spracúvajú osobné údaje úplne alebo čiastočne automatizovanými prostriedkami spracúvania s výnimkou informačných systémov vymenovaných v § 34 ods. 2 zákona č. 122/2013 Z.z.. Informačný systém zdravotná dokumentácia nepodlieha registrácii.

Ďalšie zmeny pri ochrane osobných údajov v súvislosti prijatím zákona č. 122/2013 Z.z.

- za porušenie zákon musí Úrad na ochranu osobných údajov uložiť pokutu; podľa doterajšie zákona č. 428/2002 Z.z. pokutu uložiť nemusel

- zavádza inštitút oprávnenej osoby

- upravujú sa nové podmienky na poverenie zodpovednej osoby.

Do 31.12.2013 sú prevádzkovatelia:

- a sprostredkovatelia povinní vykonať poučenie oprávnených osôb podľa § 21 zákona č. 122/2013 Z.z.

- zosúladiť všetky informačné systémy, v ktorých spracúva osobné údaje so zákonom č. 122/2013 Z.z.

---

2 oprávnenou osobou je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21 zákon č. 122/2013 Z.z. Fyzická osoba sa stáva oprávnenou osobou dňom jej poučenia a teda oprávnenie spracúvať osobné údaje nadobúda až po poučení

- nanovo prihlásiť informačný systém na registráciu alebo osobitnú registráciu na Úrade na ochranu osobných údajov, ak informačné systémy podliehajú registrácii alebo osobitnej registrácii

Do 31.03.2014 sú prevádzkovatelia a sprostredkovatelia povinní zosúladiť prijaté bezpečnostné opatrenia so zákonom č. 122/2013 Z.z..

Do 30.06.2014 sú prevádzkovatelia a sprostredkovatelia povinní:

- upraviť vzájomný zmluvný vzťah podľa požiadaviek § 8 zákona č. 122/2013Z.z. zosúladiť prijaté bezpečnostné opatrenia so zákonom č. 122/2013 Z.z.

- písomne poveriť zodpovednú osobu o poverenie oznámiť Úradu na ochranu osobných údajov.