

Výbraté ustanovenia zo zákona:

428/2002 Z. z. o ochrane osobných údajov

v znení zákona č. 602/2003 Z. z., zákona č. 576/2004 Z. z.
a zákona č. 90 /2005 Z. z.

BEZPEČNOSŤ OSOBNÝCH ÚDAJOV

§ 15

Zodpovednosť za bezpečnosť osobných údajov

(1) **Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ a sprostredkovateľ** tým, že ich chráni pred náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením ako aj pred akýmikoľvek inými neprípustnými formami spracúvania. Na tento účel prijme primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania, pričom berie do úvahy najmä

- a) použiteľné technické prostriedky,
- b) rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému,
- c) dôvernosť a dôležitosť spracúvaných osobných údajov.

(2) **Opatrenia podľa odseku 1 prijme prevádzkovateľ a sprostredkovateľ vo forme bezpečnostného projektu informačného systému** (ďalej len „bezpečnostný projekt“) a zabezpečí jeho vypracovanie, ak

- a) sú v informačnom systéme **spracúvané osobitné kategórie osobných údajov podľa § 8 a informačný systém je prepojený na verejne prístupnú počítačovú sieť alebo je prevádzkovaný v počítačovej sieti, ktorá je prepojená na verejne prístupnú počítačovú sieť,**
- b) **sú v informačnom systéme spracúvané osobitné kategórie osobných údajov podľa § 8;** v tomto prípade prevádzkovateľ a sprostredkovateľ **len zdokumentuje prijaté technické, organizačné a personálne opatrenia v rozsahu, ktorý ustanovuje § 16 ods. 3 písm. c) a ods. 6, alebo**
- c) informačný systém slúži na zabezpečenie verejného záujmu podľa § 2 ods. 1; ustanovenie § 16 sa pri vypracúvaní bezpečnostného projektu nepoužije len vtedy, ak pre konkrétny prípad je tu súčasne povinnosť vypracovať bezpečnostný projekt podľa osobitného zákona.^{21a)}

(3) Na požiadanie úradu prevádzkovateľ a sprostredkovateľ preukážu rozsah a obsah prijatých technických, organizačných a personálnych opatrení podľa odseku 1 alebo 2.

^{21a)} Zákon č. 215/2004 Z. z.

(4) Ak sú predmetom kontroly informačné systémy podľa odseku 2, úrad má právo požadovať od prevádzkovateľa alebo sprostredkovateľa predloženie hodnotiacej správy o výsledku auditu bezpečnosti informačného systému (ďalej len „hodnotiaca správa“), ak sú vážne pochybnosti o jeho bezpečnosti alebo o praktickom uplatňovaní opatrení uvedených v bezpečnostnom projekte. Hodnotiacu správu, nie staršiu ako dva roky, bezodkladne predloží prevádzkovateľ alebo sprostredkovateľ úradu, inak zabezpečí vykonanie auditu bezpečnosti informačného systému na vlastné náklady a predloží hodnotiacu správu najneskôr do troch mesiacov odo dňa uloženia povinnosti.

(5) Audit bezpečnosti informačného systému môže vykonať iba externá, odborne spôsobilá právnická osoba alebo fyzická osoba, ktorá sa nepodieľala na vypracovaní bezpečnostného projektu predmetného informačného systému, a nie sú pochybnosti o jej nezáujatosti.

Z dôvodovej správy k zákonu 90/2005 Z.z.

V snahe priblížiť sa čo najviac právu Európskeho spoločenstva, navrhuje sa v súlade s Čl. 17 ods. 1 smernice 95/46/ES spresniť a doplniť znenie § 15 ods. 1, ktorý vytvára základný rámec podmienok týkajúcich sa bezpečnosti spracúvania osobných údajov. Zákon v nových písmenách a) až c) bližšie konkretizuje, čo najmä treba brať do úvahy pri určovaní primeranosti technických, organizačných a personálnych opatrení.

Platné ustanovenie § 15 ods. 2 písm. a) ukladá prevádzkovateľom a sprostredkovateľom povinnosť vypracovať bezpečnostný projekt v prípade, ak je ich informačný systém prepojený na verejne prístupnú počítačovú sieť alebo je prevádzkovaný v počítačovej sieti, ktorá je prepojená na verejne prístupnú počítačovú sieť. Zámerom tohto ustanovenia bolo sprísniť podmienky spracúvania najmä tých osobných údajov, ktoré patria medzi osobitné kategórie osobných údajov (§ 8) a sú vystavené možným hrozbám pri spracúvaní v prostredí, ktoré je prepojené na internet. V tejto súvislosti sa preto navrhuje v písmene a) upresniť túto skutočnosť a výslovne tento zámer deklarovať.

Ustanovenie § 15 ods. 2 písm. b) sa týka informačných systémov, v ktorých sú spracúvané osobitné kategórie osobných údajov, ale nie sú žiadnym spôsobom prepojené na internet ani inú verejne prístupnú počítačovú sieť alebo sú spracúvané inými ako automatizovanými prostriedkami spracúvania. V takýchto prípadoch z dôvodov hospodárnosti a účelnosti aj s ohľadom na doplnený obsah § 15 ods. 1 je postačujúce zo strany prevádzkovateľov a sprostredkovateľov, ak prijaté technické, organizačné a personálne opatrenia len zdokumentujú v rozsahu, ktorý ustanovuje § 16 ods. 3 písm. c) a ods. 6. Navrhuje sa preto písmeno b) doplniť o túto novú podmienku.

Podľa doterajšej právnej úpravy sa ustanovenie § 15 ods. 2 písm. c) týkalo tých informačných systémov, ktoré podliehali osobitným podmienkam ustanoveným v § 2 ods. 2. Na tieto informačné systémy sa požiadavka, aby bezpečnostný projekt splňal náležitosti § 16 tohto zákona, generálne nevzťahovala, čo bolo deklarované zaradením § 16 medzi ustanovenia do § 2 ods. 2. Takúto výnimku smernica 95/46/ES v Čl. 13 nepripúšťa. Aby neprichádzalo ku kolízii zákona o ochrane osobných údajov a zákona č. 215/2004 Z. z. v ustanoveniach, ktoré sa týkajú vypracúvania bezpečnostných projektov, navrhuje sa povinnosť pre prevádzkovateľov, ktorí spracúvajú osobné údaje na základe ustanovenia § 2, spracovať bezpečnostný projekt v súlade s obsahom ustanovenia § 16 tohto zákona len vtedy, ak pre konkrétny prípad tu súčasne nie je povinnosť vypracovať bezpečnostný projekt podľa zákona č. 215/2004 Z. z.

Bezpečnostný projekt

(1) **Bezpečnostný projekt vymedzuje rozsah** a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.

(2) **Bezpečnostný projekt** sa spracúva v súlade so základnými pravidlami bezpečnosti informačného systému vydanými bezpečnostnými štandardmi, právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.

(3) Bezpečnostný projekt obsahuje najmä

- a) bezpečnostný zámer,
- b) analýzu bezpečnosti informačného systému,
- c) bezpečnostné smernice.

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

- a) formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- b) špecifikáciu technických, organizačných 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,
- d) vymedzenie hraníc určujúcich množinu zvyškových rizík.

(5) **Analýza bezpečnosti informačného systému** je podrobný rozbor stavu bezpečnosti informačného systému, ktorá obsahuje najmä

- a) kvalitatívnu analýzu rizík, v rámci ktorej sa identifikujú hrozby pôsobiace na jednotlivé aktíva informačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť; **výsledkom kvalitatívnej analýzy rizík je zoznam hrozieb, ktoré môžu ohroziť dôvernosť, integritu a dostupnosť** spracúvaných osobných údajov, s uvedením rozsahu možného rizika, návrhov opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík, a s vymedzením súpisu nepokrytých rizík,
- b) použitie bezpečnostných štandardov 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.

(6) **Bezpečnostné smernice upresňujú** a aplikujú závery vyplývajúce z bezpečnostného projektu na konkrétne podmienky prevádzkovaného informačného systému a obsahujú najmä

- a) popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach,
- b) rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému,
- c) rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov (§ 19),
- d) spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- e) postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

§ 17

Poučenie

Prevádzkovateľ alebo sprostredkovateľ je povinný poučiť oprávnené osoby o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie. Poučenie vykoná prevádzkovateľ alebo sprostredkovateľ pred vydaním prvého pokynu oprávnenej osobe na vykonanie akejkoľvek spracovateľskej operácie s osobnými údajmi. **Oprávnená osoba poučenie potvrdí svojim podpisom;** o poučení prevádzkovateľ alebo sprostredkovateľ vedie písomný záznam.

Z dôvodovej správy k zákonu 90/2005 Z.z.

Povinnosť prevádzkovateľov a sprostredkovateľov vykonať poučenie podľa § 17 tu bola aj podľa doterajšej právnej úpravy. Dôležitou zmenou je, že poučenie sa bude týkať len tých fyzických osôb, ktoré majú u prevádzkovateľa alebo sprostredkovateľa postavenie „oprávnených osôb“, pretože tie sú zodpovedné za bezpečné spracúvanie osobných údajov. Je len na prevádzkovateľovi a sprostredkovateľovi, či poučí aj ostatné fyzické osoby, ktoré náhodne prídu alebo môžu prísť do styku s osobnými údajmi. Zároveň sa výslovne ustanovuje, že poučenie musí byť písomne zdokumentované a musí sa vykonať pred vydaním prvého pokynu oprávnenej osobe na vykonanie akejkoľvek spracovateľskej operácie s osobnými údajmi.

§ 18

Povinnosť mlčanlivosti

(1) Prevádzkovateľ a sprostredkovateľ sú povinní zachovávať mlčanlivosť o osobných údajoch, ktoré spracúvajú. Povinnosť mlčanlivosti trvá aj po ukončení spracovania. Povinnosť mlčanlivosti nemajú, ak je to podľa osobitného zákona nevyhnutné na plnenie úloh orgánov činných v trestnom konaní; tým nie sú dotknuté ustanovenia osobitných zákonov.²²⁾

(2) **Oprávnená osoba** je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť.

²²⁾ Napríklad § 40 zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení zákona č. 149/2001 Z. z.

(3) Povinnosť mlčanlivosti podľa odseku 2 platí aj pre iné fyzické osoby, ktoré v rámci svojej činnosti (napr. údržba a servis technických prostriedkov) prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa.

(4) Povinnosť mlčanlivosti podľa odseku 2 trvá aj po zániku funkcie oprávnenej osoby alebo po ukončení jej pracovného pomeru alebo obdobného pracovného vzťahu, ako aj štátnozamestnaneckého pomeru alebo vzťahu podľa odseku 3.

(5) Odseky 1 až 4 a ustanovená povinnosť mlčanlivosti prevádzkovateľov, sprostredkovateľov a oprávnených osôb podľa osobitných predpisov²³⁾ sa nepoužijú vo vzťahu k úradu pri plnení jeho úloh (§ 38 až 44).

§ 19

Dohľad nad ochranou osobných údajov

(1) Za výkon dohľadu nad ochranou osobných údajov spracúvaných podľa tohto zákona zodpovedá prevádzkovateľ.

(2) Ak prevádzkovateľ zamestnáva viac ako päť osôb, výkonom dohľadu písomne poverí zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

(3) Odborné **vyškolenie zodpovednej osoby** alebo viacerých zodpovedných osôb **zabezpečí prevádzkovateľ**. Rozsah odborného školenia zodpovedá najmä obsahu tohto zákona a úlohám z neho vyplývajúcim, ako aj obsahu medzinárodných zmlúv o ochrane osobných údajov,²⁴⁾ ktoré boli vyhlásené spôsobom ustanoveným zákonom. Úrad môže od prevádzkovateľa žiadať podanie dôkazu o vykonanom odbornom školení.

(4) **Zodpovedná osoba posúdi pred začatím spracúvania** osobných údajov v informačnom systéme, **či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb**. Zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi; ak prevádzkovateľ po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu.

(5) Prevádzkovateľ, ktorý písomne poveril výkonom dohľadu nad ochranou osobných údajov zodpovednú osobu, je povinný o tom písomne informovať úrad bez zbytočného

²³⁾ Napríklad § 6 ods. 1 zákona č. 150/2001 Z. z. o daňových orgánoch a ktorým sa mení a dopĺňa zákon č. 440/2000 Z. z. o správach finančnej kontroly, § 14 zákona 330/2000 Z. z. o burze cenných papierov, § 134 zákona č. 566/2001 Z.z. o cenných papieroch a investičných službách a o zmene a doplnení niektorých zákonov (zákon o cenných papieroch), § 91 až 93 zákona č. 483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov, § 24 zákona č. 24/1991 Zb. o poisťovníctve v znení neskorších predpisov, § 81 písm. e) a § 240 ods. 5 zákona č. 311/2001 Z. z. Zákonník práce, § 53 ods. 1 písm. e) zákona č. 312/2001 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov, § 9 ods. 2 písm. b) zákona č. 313/2001 Z. z. o verejnej službe, § 8 zákona č. 367/2000 Z. z., § 80 zákona Národnej rady Slovenskej republiky č. 171/1993 Z. z. v znení neskorších predpisov, § 15 ods. 2 a 3 zákona Národnej rady Slovenskej republiky č. 38/1993 Z. z. o organizácii Ústavného súdu Slovenskej republiky a konaní pred ním a o postavení jeho sudcov.

²⁴⁾ Napríklad Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (oznámenie č. 49/2001 Z. z.).

odkladu, najneskôr do 30 dní odo dňa poverenia zodpovednej osoby doporučenou zásielkou. Prevádzkovateľ oznámi úradu tieto údaje:

- a) názov, sídlo alebo trvalý pobyt, právnu formu a identifikačné číslo prevádzkovateľa alebo zástupcu prevádzkovateľa,
- b) titul, meno, priezvisko a dátum narodenia zodpovednej osoby,
- c) pracovné zaradenie zodpovednej osoby,
- d) dátum začiatku platnosti písomného poverenia zodpovednej osoby,
- e) vyhlásenie prevádzkovateľa o tom, že zodpovedná osoba spĺňa podmienky ustanovené v odseku 12.

(6) **Prevádzkovateľ oznámi úradu poverenie jednej zodpovednej osoby**, a to aj vtedy, ak výkonom dohľadu nad ochranou osobných údajov súčasne poveril viac zodpovedných osôb. Ak prevádzkovateľ nahradí zodpovednú osobu, ktorú nahlásil úradu, inou zodpovednou osobou, postupuje podľa odseku 5.

(7) Zodpovedná osoba zabezpečuje

- a) potrebnú súčinnosť s úradom pri plnení úloh patriacich do jeho pôsobnosti; na požiadanie je zodpovedná osoba povinná úradu kedykoľvek predložiť svoje písomné poverenie, písomné oznámenia vystavené pre prevádzkovateľa podľa odseku 4, preukázať rozsah získaných vedomostí odborným školením,
- b) povinnosti podľa odseku 4,
- c) dohľad nad plnením základných povinností prevádzkovateľa podľa § 6,
- d) poučenie oprávnených osôb podľa § 17,
- e) vybavovanie žiadostí dotknutých osôb podľa § 20 až 22,
- f) realizáciu technických, organizačných a personálnych opatrení a dohliada na ich aplikáciu v praxi; ak je prevádzkovateľ povinný vypracovať bezpečnostný projekt v súlade s § 16 alebo dokumentáciu podľa § 15 ods. 2 písm. b), zabezpečuje ich vypracovanie,
- g) dohľad pri výbere sprostredkovateľa podľa § 5 ods. 3 a 4, prípravu písomnej zmluvy alebo písomného poverenia pre sprostredkovateľa v súlade s § 5 ods. 2 a zodpovedá za jeho obsah; počas trvania zmluvného vzťahu alebo poverenia preveruje dodržiavanie dohodnutých podmienok,
- h) dohľad nad cezhraničným tokom osobných údajov,
- i) prihlásenie informačných systémov na osobitnú registráciu a oznamovanie zmien a odhlásenie informačných systémov z osobitnej registrácie; o informačných systémoch, ktoré nepodliehajú registrácii vedie evidenciu v rozsahu ustanovenom týmto zákonom podľa § 29 a 30 a zabezpečuje jej sprístupnenie komukoľvek, kto o to požiada v súlade s § 32.

(8) **Prevádzkovateľ, ktorý zamestnáva menej ako šesť osôb** môže výkonom dohľadu nad ochranou osobných údajov písomne poveriť zodpovednú osobu, ktorá dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

(9) **Prevádzkovateľ, ktorý zamestnáva menej ako šesť osôb** a výkonom dohľadu nad ochranou osobných údajov písomne **nepoveril** zodpovednú osobu, **je povinný prihlásiť na**

registráciu tie informačné systémy, ktoré podľa tohto zákona podliehajú registrácii podľa § 25.

(10) Prevádzkovateľ je povinný umožniť zodpovednej osobe nezávislý výkon dohľadu nad ochranou osobných údajov a prijať jej oprávnené návrhy; upozornenie na nedostatky alebo vyslovenie požiadavky zodpovednou osobou v súvislosti s plnením jej povinností podľa odseku 7 sa nesmie stať podnetom ani dôvodom na konanie zo strany prevádzkovateľa, ktoré by zodpovednej osobe spôsobilo ujmu.

(11) Úrad je oprávnený uložiť prevádzkovateľovi povinnosť písomne poveriť dohľadom nad ochranou osobných údajov inú zodpovednú osobu, ak sa preukáže, že písomne poverená zodpovedná osoba neplnila alebo nedostatočne plnila povinnosti podľa odseku 7, alebo práva a povinnosti uložené prevádzkovateľovi týmto zákonom nesprávne posudzovala alebo ich nesprávne uplatňovala v praxi, alebo nespĺňa podmienky ustanovené v odseku 12. Prevádzkovateľ je povinný bez zbytočného odkladu úradu vyhovieť a dohľadom písomne poveriť inú zodpovednú osobu; ak tomu bránia dôvody hodné osobitného zreteľa, ktoré vie prevádzkovateľ úradu hodnoverne preukázať, úrad určí prevádzkovateľovi lehotu, dokedy je povinný vymeniť zodpovednú osobu, prípadne prihlásiť informačné systémy na registráciu.

(12) **Zodpovednou osobou môže byť** len fyzická osoba, ktorá má spôsobilosť na právne úkony v plnom rozsahu a spĺňa podmienku bezúhonnosti podľa § 35 ods. 4 prvej vety; bezúhonnosť sa preukazuje doložením výpisu z registra trestov nie starším ako tri mesiace, ktorý je prevádzkovateľ povinný uchovávať počas doby výkonu funkcie zodpovednej osoby. Zodpovednou osobou nemôže byť fyzická osoba, ktorá je štatutárnym orgánom prevádzkovateľa a fyzická osoba, ktorá je oprávnená konať v mene štatutárneho orgánu prevádzkovateľa. Zodpovedná osoba má postavenie oprávnenej osoby prevádzkovateľa.

Z dôvodovej správy k zákonu 90/2005 Z.z.

Doplnenie nových odsekov v ustanovení § 19 súvisí s novým prístupom vo veci registrácie informačných systémov. Smernica 95/46/ES predpokladá oznamovanie všetkých spracovateľských operácií prevádzkovateľmi ešte pred samotným začatím spracúvania. Čl. 18 ods. 2 smernice 95/46/ES umožňuje výnimku z takéhoto oznámenia, ak prevádzkovateľ ustanovil zodpovednú osobu, ktorá dohliada na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov. Je však nevyhnutné zároveň zabezpečiť požiadavky smernice, aby takáto zodpovedná osoba vykonávala dohľad odborne a nezávisle. Na takúto osobu sa do istej miery potom nahliada, akoby dozor prostredníctvom tejto zodpovednej osoby vykonával úrad.

Ak prevádzkovateľ zamestnával viac ako päť osôb, aj doteraz bol povinný písomne ustanoviť zodpovednú osobu. To však nemalo vplyv na povinnosť registrácie informačných systémov. Nové odseky v § 19 jednoznačne určujú povinnosti zodpovedných osôb, podmienky ich vymenovania do funkcie a ich ochranu vo vzťahu k prevádzkovateľovi pri plnení úloh zodpovednej osoby. Prevádzkovateľ, ktorý preukáže úradu, že písomne poveril zodpovednú osobu, ktorá je odborne vyškolená a plní svoje úlohy zodpovednej osoby v súlade s ustanoveniami tohto zákona, nemusí svoje informačné systémy registrovať na úrade.