



Informačné systémy
Bezpečnosť
Infraštruktúra



Aktuálne požiadavky na ochranu osobných údajov

Mgr. Viera Gubková

Novela zákona, po pripomienkovom konaní, bola predložená ÚOOÚ v marci 2011 (rezortné číslo 09911/2011Kp)

Zmeny navrhované v zákone:

- vymedzenie pojmu „osobné údaje“,
- zavádza pojem „právny dôvod spracúvania osobných údajov“ a zároveň sa upozorňuje na základné povinnosti, ktoré nesmie porušiť alebo opomenúť ten, kto pripravuje spracúvanie osobných údajov alebo osobné údaje spracúva,
- konsoliduje sa úprava ustanovení týkajúcich sa prevádzkovateľa a sprostredkovateľa,
- dopĺňa sa inštitút oprávnenej osoby,
- zavádza sa register oprávnených osôb,

- menia sa pravidlá pre monitorovacie systémy,
- spresňujú sa ustanovenia týkajúce sa likvidácie osobných údajov,
- navrhuje sa spriehľadniť existujúce pravidlá týkajúce sa prijímania technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov.,
- inštitút zodpovednej osoby na navrhuje spresniť a doplniť,
- bolo pristúpené ku komplexnému dobudovaniu inštitútu „informačnej povinnosti“, ktorý je základným pilierom práv dotknutých osôb pri spracúvaní ich osobných údajov a prvoradou povinnosťou prevádzkovateľa vo vzťahu k dotknutým osobám,
- navrhuje sa upraviť práva ÚOOÚ,
- boli upravené sankcie.

Najčastejšie problémy prevádzkovateľov

- Zodpovedné osoby sú z radov informatikov,
- spracúvanie osobných údajov nad rámec zákona, na základe ktorého sa získavajú,
- združovanie právneho základu a súhlasu dotknutej osoby,
- absencia dokumentácie súvisiacej s poučením oprávnených osôb,
- nedostatočne vymedzený okruh oprávnených osôb,
- absencia zmluvných základov spracúvania údajov sprostredkovateľmi,
- nesplnenie podmienok monitorovacích systémov,

Najčastejšie problémy prevádzkovateľov

- získavanie osobných údajov kopírovaním, skenovaním a pod. bez súhlasu dotknutých osôb,
- zverejňovanie osobných údajov napr. fotografie na intranete, bez súhlasu zamestnanca,
- zasielanie osobných údajov prostredníctvom elektronickej pošty bez zabezpečenia ochrany osobných údajov
- nevypracovaná dokumentácia k informačným systémom alebo nekvalitne spracovaná dokumentácia,
- nie je vedená evidencia informačných systémov.

Riešenie problémov prevádzkovateľov

- Začať u zodpovednej osoby,
- „zmapovať“ spracúvanie osobných údajov v informačných systémoch,
- zistiť, kto má prístup k osobným údajom a na základe čoho,
- stanoviť zodpovednosť za jednotlivé informačné systémy,
- zabezpečiť evidenciu informačných systémov,
- zabezpečiť školenie zodpovedných osôb,
- zabezpečiť poučenie oprávnených osôb,
- zabezpečiť súlad spracúvania osobných údajov v jednotlivých informačných systémoch,
- zabezpečiť dokumentáciu k informačným systémom .

Čo môžeš urobiť dnes, neodkladaj na zajtra!

Aby nás novela zákona nenašla nepripravených:

- ak vymenúvame zodpovedné osoby , pokúsiť sa splniť návrh novely,
- zistiť, kto má prístup k osobným údajom a na základe čoho, pripraviť si register oprávnených osôb,
- zabezpečiť si zmluvné vzťahy,
- porovnať doposiaľ vypracovanú dokumentáciu k informačným systémom s požiadavkami návrhu,
- zabezpečiť na ďalšie obdobie finančné prostriedky na plnenie úloh, ak by bol prijatý zákon, tak najdlhšia lehota na zosúladenie je jeden rok.

Čo môžeš urobiť dnes, neodkladaj na zajtra!

§ 16 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.

Čo môžeš urobiť dnes, neodkladaj na zajtra!

- (3) Bezpečnostný projekt obsahuje najmä
- a) bezpečnostný zámer,
 - b) analýzu bezpečnosti informačného systému,
 - c) bezpečnostné smernice.

Čo môžeš urobiť dnes, neodkladaj na zajtra!

- (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.

Čo môžeš urobiť dnes, neodkladaj na zajtra!

- (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 dôvernú, 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 štandardmi, metódami a prostriedkami.

Čo môžeš urobiť dnes, neodkladaj na zajtra!

- (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.

Čo musí obsahovať zmluva so sprostredkovateľom

- Údaje o zmluvných stranách (ďalej len „identifikačné údaje“),
- deň začatia spracúvania osobných údajov sprostredkovateľom,
- účel spracúvania osobných údajov,
- názov informačného systému,
- zoznam osobných údajov, ktoré sú predmetom spracúvania; možno ho nahradiť rozsahom osobných údajov, ak vzhľadom na účel spracúvania nemožno vopred presne určiť jednotlivé osobné údaje,
- okruh dotknutých osôb, ktorých osobné údaje sa spracúvajú,
- podmienky spracúvania osobných údajov,
- opis opatrení, ktoré sprostredkovateľ preukázal prevádzkovateľovi,
- vyhlásenie sprostredkovateľa o tom, že spracúvanie osobných údajov vykoná osobne, inak do zmluvy uvedie identifikačné údaje osoby, prostredníctvom ktorej spracúvanie osobných údajov vykoná (ďalej len „subdodávateľ“),
- trvanie zmluvy a spôsob ukončenia zmluvy,
- dátum vyhotovenia zmluvy a podpisy zmluvných strán.



Ďakujem za pozornosť

viera.gubkova@lynx.sk