



Smernice online

MAREC 2014

ZÁKAZNÍCKY SPRAVODAJ 1

Vážený zákazník / vážená zákazníčka,

ako nášmu vernému čitateľovi on-line knižnice www.smerniceonline.sk som pripravila ďalšiu zákaznickú výhodu. Mesačne od nás dostávate e-mailom prehľad najnovších informácií, ktoré sa stali súčasťou obsahu on-line knižnice, prostredníctvom zákaznického spravodaja priamo do Vašej e-mailovej schránky. Dnes sa Vám do rúk prvýkrát dostáva zákaznický spravodaj on-line knižnice www.smerniceonline.sk v tlačenej verzii. Touto cestou chceme upriamiť pozornosť na dôležité termíny, na ktoré nesmieme zabudnúť a tiež priblížiť témy, s ktorými sa na nás obraciate.

On-line knižnica www.smerniceonline.sk prináša so sebou množstvo výhod, z ktorých je najväčšou práve množstvo odborných informácií, ktoré zjednodušia Vašu každodennú pracovnú činnosť.

Obsahom internetového portálu sú všetky interné smernice potrebné pri odovzdávaní účtovnej agendy, množstvo riešení na problematické situácie z praxe s odbornými odpoveďami našich autorov a tiež veľa vzorov a tlačív potrebných nielen na správnu komunikáciu s finančnou správou.

Dúfam, že zákaznický spravodaj v tejto podobe Vás poteší a prinesie ďalšie obohatené informácie z oblasti účtovníctva, miezd a bezpečnosti práce, čiže z oblastí, ktorým sa on-line knižnica venuje pri spracovaní vzorových interných smerníc.

Za redakciu Verlag Dashöfer želá príjemné čítanie



Nadežda Fuksová
Ing. Nadežda Fuksová,
šéfredaktorka

POVINNOSTI PREVÁDZKOVATEĽOV PRI VYUŽÍVANÍ KAMEROVÝCH SYSTÉMOV INŠTALOVANÝCH ZA ÚČELOM OCHRANY MAJETKU

PhDr. Anna Miklošová, Zdroj: Verlag Dashöfer

Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“), ktorý nadobudol účinnosť 1. júla 2013, priniesol rad zmien.



Z úvodných ustanovení vyplýva, že zákon sa vzťahuje na každého, kto spracúva osobné údaje, určuje účel a prostriedky spracúvania alebo poskytuje osobné údaje na spracúvanie. Aj pri monitorovaní verejne prístupného priestoru dochádza k spracúvaniu osobných údajov (§ 4 ods. 3 písm. a)).

Zákon o ochrane osobných údajov ustanovil, že priestor prístupný verejnosti možno monitorovať len na účely ochrany verejného poriadku a bezpečnosti, odhalovania kriminality, narušenia bezpečnosti štátu, ochrany majetku alebo zdravia, a to len vtedy, ak je priestor zreteľne označený ako monitorovaný. Podľa cit. zákona túto povinnosť má prevádzkovateľ vždy, bez ohľadu na to, či sa snímajú obraz alebo zvuk zaznamenáva na nosič informácií (§ 15 ods. 7).

V zmysle zákona zreteľné označenie monitorovaného priestoru znamená viditeľné umiestnenie informácie o monitorovaní pri vstupe do monitorovaného priestoru z ktorejkoľvek strany. Je dôležité aby zaberaný priestor prístupný verejnosti bol monitorovaný len v rozsahu nevyhnutnom na dosiahnutie účelu spracúvania. To znamená, že napr. v prípade monitorovania parkovacieho miesta pri dome na tento účel nie je možné monitorovať chodník na druhej strane ulice, príp. celú ulicu ap., a teda sklon kamery /kamier je nevyhnutné v tomto zmysle upraviť.

Zákon ustanovuje, že vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch.

Ak takto vyhotovený záznam nie je využitý na účely trestného konania alebo konania o priestupkoch, je ten, kto ho vyhotovil, povinný ho zlikvidovať najneskôr v lehote 15 dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený (§ 17 ods. 7).

Zákon teda striktné stanovuje využitie takéhoto záznamu, čo znamená, že akékoľvek iné použitie (napr. prezentácia susedom, príp. na facebooku) je v rozpore so zákonom.

Prevádzkovateľ

Ten, kto v rámci svojej činnosti monitoruje priestor prístupný verejnosti sa stáva prevádzkovateľom, pretože v zmysle zákona o ochrane osobných údajov **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.**

Aj obyvatelia obytných domov - teda vlastníci bytov a nebytových priestorov - v poslednom období často siahajú po kamerových systémoch ako nástrojoch na ochranu ich majetku, pričom monitorujú napr. vchod do obytného domu vrátane časti chodníka, príp. parkovisko, ktoré k obytnému domu prislúcha, ak takýto priestor pri dome existuje. Povinnosť zreteľne označiť v nevyhnutnom rozsahu monitorovaný priestor prístupný verejnosti a likvidovať takto získaný záznam v pätnásťdňovej lehote platí aj v tomto prípade. Prevádzkovateľom zodpovedajúcim za spracúvanie osobných údajov získaných monitorovaním priestoru prístupného verejnosti však v tomto prípade môže byť:

- spoločenstvo vlastníkov bytov a nebytových priestorov podľa zákona č. 182/1993 Z. z. o vlastníctve bytov a nebytových priestorov v znení neskorších predpisov (ďalej len „zákon o vlastníctve bytov“), ktoré spravuje obytný dom,
- správcovská spoločnosť ak vlastníci bytov a nebytových priestorov uzavreli zmluvu o výkone správy so správcom, ktorý na tomto základe zabezpečuje správu domu, a teda aj jeho ochranu, nakoľko zo zákona o vlastníctve bytov je možná len jedna z týchto dvoch foriem správy.

PRAX!

V praxi niekedy dochádza k tomu, že vlastníci bytov, ktorí uzavreli zmluvu o správe so správcom v zmysle zákona o vlastníctve bytov, sa sami rozhodnú a kamery kúpia, nainštalujú ich a neriešia vec cez správcu. V takom prípade je podľa zákona o ochrane osobných údajov prevádzkovateľom vlastníkom bytu v bytovom dome, ktorý spoločne s inými vlastníkmi určil účel a prostriedky spracúvania osobných údajov.

V poslednom prípade, keď prevádzkovateľom sú sami vlastníci (ktorí nie sú združení do spoločenstva, ale majú správcu, ktorého touto činnosťou nepoverili), problém môže niekedy nastať pri aplikácii ďalších ustanovení zákona o ochrane osobných údajov. Medzi tieto povinnosti patrí vedenie evidencie informačného systému (§ 43), poučenie oprávnených osôb (§ 21 ods. 3) a ochrana spracúvaných osobných údajov formou smernice alebo bezpečnostného projektu (§ 19 ods. 2,3).

Nakoľko **sa zákon o ochrane osobných údajov vzťahuje na každého, kto spracúva osobné údaje**, niektoré povinnosti z neho vyplývajúce sa vzťahujú aj na vlastníkov rodinných domov, ktorí za účelom ochrany majetku nainštalujú na rodinný dom kamerový systém. Pretože pri tejto činnosti dochádza k spracúvaniu osobných údajov z monitorovania verejne prístupného priestoru, povinnosť zreteľne označiť takýto priestor ako monitorovaný (aj keď sa osobné údaje nezaznamenávajú) a povinnosť likvidovať záznam z monitorovania do 15 dní (ak sa záznam vyhotovuje) sa na týchto prevádzkovateľov vzťahuje. Dôležitý je aj rozsah záberu, pretože každý prevádzkovateľ je oprávnený spracúvať len taký rozsah osobných údajov, ktorý je nevyhnutný na dosiahnutie účelu ich spracúvania (§ 6 ods. 2 písm. d)).

Oprávnená osoba

Podľa zákona o ochrane osobných údajov **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 cit. zákona (§ 4 ods. 2 písm. e)).

Ak prevádzkovateľom kamerového informačného systému je správcovská spoločnosť, jej zamestnanec, ktorý bude manipulovať so záznamom je oprávnenou osobou, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru. Oprávnenou osobou prevádzkovateľa je aj zástupca vlastníkov (viď zákon o vlastníctve bytov a nebytových priestorov), ktorý prichádza do styku s osobnými údajmi na základe zvolenia vlastníkmi bytov. Oprávnenými osobami sú aj členovia spoločenstva vlastníkov bytov, príp. „vchodoví dôverníci“, teda fyzické osoby, ktoré prichádzajú do styku s osobnými údajmi na základe zvolenia.

POZOR!

V prípade ak kamerový systém využíva vlastník rodinného domu, vymedziť oprávnenú osobu v zmysle zákona o ochrane osobných údajov je problém. Z pohľadu definície zákona o ochrane osobných údajov člena rodiny, ktorý manipuluje s kamerovým záznamom nie je možné označiť za fyzickú osobu podľa uvedenej definície.

Zákon o ochrane osobných údajov presne ustanovuje náležitosti poučenia. Podľa cit. zákona poučenie musí byť písomné a prevádzkovateľ o ňom vyhotovuje písomný záznam. Nakoľko fyzická osoba sa stáva oprávnenou až dňom jej poučenia, tento proces sa musí vykonať pred uskutočnením prvej operácie s osobnými údajmi.

Záznam o poučení obsahuje

- identifikačné údaje prevádzkovateľa,
- titul, meno, priezvisko, pracovné, služobné alebo funkčné zaradenie a podpis oprávnenej osoby,
- titul, meno, priezvisko, pracovné zaradenie alebo funkciu a podpis toho, kto vykonal poučenie,
- rozsah oprávnení, ktoré oprávnená osoba má, povinnosti ustanovené týmto zákonom, ktoré je oprávnená osoba povinná dodržiavať, popis povolených činností, zodpovednosť za ich porušenie,
- deň poučenia a

- deň, odkedy osoba prestala byť oprávnenou osobou (tento údaj doplní prevádzkovateľ po ukončení jej činnosti ako oprávnenej osoby).

Prevádzkovateľ, ktorým je spoločenstvo vlastníkov bytov resp. správcovská spoločnosť, je kapacitne schopný zabezpečiť poučenie oprávnených osôb, ktoré pracujú s kamerovým záznamom. Poučenie môže zabezpečiť napr. predseda predstavenstva, člen predstavenstva alebo konateľ spoločnosti, príp. zodpovedná osoba (týka sa správcovskej spoločnosti, ktorá spracúva osobné údaje prostredníctvom 20 oprávnených osôb). V prípade ak sa vlastníci bytov sami rozhodli zakúpiť a inštalovať kamerový systém, ostáva na ich zvážení, kto z nich bude oprávnenou osobou manipulujúcou so záznamami a kto ju poučí. Poučenie má reflektovať ustanovenia zákona o ochrane osobných údajov týkajúce sa monitorovania verejne prístupného priestoru.

Bezpečnosť spracúvaných osobných údajov

Pretože za bezpečnosť spracúvaných osobných údajov zodpovedá prevádzkovateľ, zákon o ochrane osobných údajov ukladá každému prevádzkovateľovi povinnosť chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmkoľvek inými neprípustnými spôsobmi spracúvania prijatím primeraných bezpečnostných opatrení (§ 19 ods. 1).

Zákon ustanovuje formu akou je prevádzkovateľ povinný tieto opatrenia zdokumentovať. V prípade monitorovania verejne prístupného priestoru kamerovým systémom so záznamom existujú dve možnosti prevádzky takéhoto informačného systému osobných údajov (§ 4 ods. 3 písm. b)), a to:

- záznamy sú zaznamenávané a uchovávané na záznamovej jednotke (rekordér), **ktorá nie je prepojená** s personálnym počítačom (záznamy prehladáme na zobrazovacej jednotke (napr. na televíznej obrazovke)),
- záznamy sú uchovávané na záznamovej jednotke (rekordér), **ktorá je prepojená** na personálny počítač s prístupom na internet (záznamy prehladáme na PC s prístupom na verejnú počítačovú sieť) .

Dnes záznamové zariadenia majú výstup umožňujúci pripojenie k počítaču, nie vždy však musíme túto možnosť využiť.

Nakoľko pri monitorovaní priestoru prístupného verejnosti kamerovým systémom so záznamom dochádza k spracúvaniu osobných údajov a to aj takých, ktoré patria do osobitnej kategórie osobných údajov (osobné údaje odhaľujúce rasový a etnický pôvod a osobné údaje týkajúce sa zdravia - § 13) z pohľadu zákona o ochrane osobných údajov ide o prevádzku informačného systému osobných údajov:

- **neprepojenom** na verejne prístupnú počítačovú sieť, v ktorom sú spracúvané osobitné kategórie osobných údajov a prijaté opatrenia je potrebné preukázať formou bezpečnostnej smernice (§ 19 ods. 2 písm. b)),

alebo

- **prepojenom** na verejne prístupnú počítačovú sieť, v ktorom sú spracúvané osobitné kategórie osobných údajov a prijaté opatrenia je potrebné preukázať formou bezpečnostného projektu (§ 19 ods. 3 písm. a)).

Náležitosti bezpečnostného projektu, ako aj bezpečnostných smerníc ustanovuje vykonávacia vyhláška Úradu na ochranu osobných údajov SR č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení, ktorá je vykonávacou vyhláškou k zákonu o ochrane osobných údajov (ďalej len „vyhláška“).

V zmysle vyhlášky bezpečnostný projekt obsahuje (§5)

- názov informačného systému, na ktorý sa vzťahuje,
- bezpečnostný zámer,
- analýzu bezpečnosti informačného systému,
- bezpečnostnú smernicu.

Bezpečnostný zámer vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu osobných údajov pred ohrozením ich bezpečnosti. Bezpečnostný zámer obsahuje

- formuláciu základných bezpečnostných cieľov a minimálne požadovaných bezpečnostných opatrení,
- špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia,
- vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti informačného systému,
- 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.

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

- identifikáciou rizík založenou na identifikácii aktív a ich vlastníkov, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností zneužitelných hrozbami a na identifikácii dopadov na aktíva v dôsledku straty dôveryhodnosti, integrity a dostupnosti,
- analýzou a ohodnotením rizík založených na určení dopadov, ktoré môžu vyplývať zo zlyhania bezpečnosti,
- 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,
- 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,
- výberom cieľov a opatrení na ošetrovanie rizík a vymedzením súpisu nepokrytých rizík, použitím technických noriem a určením iných metód a prostriedkov ochrany osobných údajov.

Bezpečnostné smernice tvoria:

- popis bezpečnostných opatrení a spôsob ich uplatňovania v konkrétnych podmienkach,
- 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,
- rozsah zodpovednosti oprávnených osôb a zodpovednej osoby,
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení,
- postup 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.

Bezpečnostné smernice musia zodpovedať hore uvedeným podmienkam, či sú vypracované ako súčasť bezpečnostného projektu, alebo samostatne pre informačný systém osobných údajov, ktorý nie je prepojený s verejne prístupnou počítačovou sieťou.

POZOR!

V prípade, ak je prevádzkovateľ povinný vypracovať bezpečnostný projekt len z titulu ochrany osobných údajov získaných monitorovaním verejne prístupného priestoru kamerovým systémom je jednoduchšie zabezpečiť, aby záznamové zariadenie nebolo prepojené s verejne prístupnou počítačovou sieťou.

Registrácia alebo evidencia

O informačnom systéme osobných údajov, v ktorom prevádzkovateľ spracúva osobné údaje získané z monitorovania verejne prístupného priestoru je povinný viesť evidenciu. Tento informačný systém patrí medzi výnimky z registrácie, pretože osobné údaje sa v ňom spracúvajú na základe zákona o ochrane osobných údajov.

Súvisiace vzory:

Vzor záznamu o poučení oprávnenej osoby

Vzor záznamu o oboznámení s internými predpismi prevádzkovateľa

Najčítanejšie na www.smerniceonline.sk

Smernica upravujúca harmonogram prác ročnej účtovnej závierky

Smernica o evidencii, oceňovaní a účtovaní zásob

Smernica o evidovaní, odpisovaní a účtovaní majetku

Prax mzdovej účtovníčky: ročné zúčtovanie predávkov na daň

Kontrolný výkaz pri DPH od 1.1. 2014



BEZPEČNOSŤ SPRACÚVANIA OSOBNÝCH ÚDAJOV Z POHĽADU ZÁKONA Č. 122/2013 Z. Z. O OCHRANE OSOBNÝCH ÚDAJOV A O ZMENE A DOPLNENÍ NIEKTORÝCH ZÁKONOV

PhDr. Anna Miklošová, Zdroj: Verlag Dashöfer

Podmienky pre preukazovanie prijatia bezpečnostných opatrení na ochranu osobných údajov



Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (zákon o ochrane osobných údajov) priniesol zmeny aj do požiadaviek na bezpečnosť spracúvaných osobných údajov.



Zákaznícky spravodaj online knižnice Smernice

Vydáva vydavateľstvo VERLAG DASHÖFER, s. r. o., Železničarska 13, 814 99 Bratislava. IČO 35 730 129. Tel.: 02/33 00 55 55, Fax: 02/33 00 55 50, e-mail: info@dashofer.sk / Redakcia: Ing. Marianna Hučková/ Sadzba: VERLAG DASHÖFER, s. r. o., Tlač: IM print, s. r. o. / Vychádza: mesačne/ Samostatne nepredajné. Súčasťou zákaznického servisu online knižnice Smernice www.smerniceonline.sk Ročné predplatné: 144 € bez DPH; 172,80 € s DPH/ Predplatné online knižnice je na obdobie 12 mesiacov od dátumu vašej objednávky. Objednávku na ďalšie obdobie nie je treba obnovovať, je predĺžená automaticky na ďalších 12 mesiacov. Objednávku môžete zrušiť len písomne, a to najneskôr 6 týždňov pred koncom vášho ročného predplatného obdobia. / Objednať možno na adrese vydavateľstva / ISSN 1339-5084, aktualizovaný denne/ Zákaznícky spravodaj a všetky v ňom obsiahnuté príspevky a ilustrácie sú chránené autorským právom. Ich používanie je bez schválenia vydavateľstva – s výnimkou zákonom povolených prípadov – nepripustné. Žiadna časť nesmie byť akoukoľvek formou bez písomného súhlasu vydavateľstva reprodukováaná alebo s použitím elektronických off-line alebo on-line systémov ukladaná do pamäti, či šírená. Za správnosť obsahu príspevku ručia autori. Informácie boli spracované na základe najlepších poznatkov v okamžiku zverejnenia.

ZÁKAZNÍCKY SPRAVODAJ

Podľa tohto zákona, ako aj podľa predtým platného zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „zákon č. 428/2002 Z. z.“) sú **prevádzkovateľ, ako aj sprostredkovateľ povinní prijatie primeraných technických, organizačných a personálnych opatrení preukázať bezpečnostnými smernicami alebo bezpečnostným projektom s bezpečnostnými smernicami** (§ 19).

Kým podľa zákona č. 428/2002 Z. z. spracúvanie osobitnej kategórie osobných údajov bolo jedinou podmienkou, kedy prevádzkovateľ alebo sprostredkovateľ mali povinnosť preukázať, že prijali bezpečnostné opatrenia na ochranu osobných údajov formou bezpečnostného projektu alebo bezpečnostnými smernicami, zákon o ochrane osobných údajov podmienky pre zdokumentovanie prijatých opatrení rozšíril.

Podľa zákona o ochrane osobných údajov sú prevádzkovateľ, ako aj sprostredkovateľ povinní preukázať prijaté bezpečnostné opatrenia aj v prípade ak sa v informačnom systéme nespracúvajú osobné údaje patriace do osobitnej kategórie osobných údajov ale informačný systém je prepojený s verejne prístupnou počítačovou sieťou (§ 19 ods. 2). Zjednodušene povedané povinnosť preukázať primerané opatrenia na ochranu osobných údajov má aj subjekt spracúvajúci osobné údaje v adresári vytvorenom pomocou tabuľkového procesoru Excel, ak je takýto informačný systém prepojený na verejnú počítačovú sieť. V takom prípade prevádzkovateľ alebo sprostredkovateľ preukážu prijatie primeraných bezpečnostných opatrení bezpečnostnými smernicami.

Zákon o ochrane osobných údajov nezmenil podmienky, za ktorých sú prevádzkovateľ alebo sprostredkovateľ povinní prijať primerané opatrenia na ochranu osobných údajov formou bezpečnostného projektu informačného systému a z neho vyplývajúcich bezpečnostných smerníc. Je to vtedy, ak sa v informačnom systéme prepojenom na verejnú počítačovú sieť spracúvajú osobitné kategórie osobných údajov (§ 19 ods. 3).

Bezpečnostný projekt

Zákon o ochrane osobných údajov splnomocňovacím ustanovením určil (§ 20), že náležitosti dokumentácie na ochranu osobných údajov ustanoví vykonávacia vyhláška Úradu na ochranu osobných údajov SR č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení, ktorá je vykonávacou vyhláškou k zákonu o ochrane osobných údajov (ďalej len „vyhláška“).

Vyhláška v prílohe ustanovuje aj zoznam možných technických a organizačných opatrení, ktoré je prevádzkovateľ povinný prijať v závislosti od spôsobu spracúvania osobných údajov. Pri vypracovávaní bezpečnostného projektu je možné vychádzať z niektorej z nasledovných technických noriem:

- STN ISO/IEC 27001:2005 Manažment bezpečnosti informačných systémov,
- STN ISO/IEC 27002:2005 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažerstva informačnej bezpečnosti alebo
- STN ISO/IEC 27005:2011 Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti.

Štruktúra bezpečnostného projektu, ako aj zoznam možných bezpečnostných opatrení sú vyhláškou vymedzené všeobecne. Každý prevádzkovateľ alebo sprostredkovateľ musí ako východisko k vypracovaniu a aplikácii bezpečnostných opatrení najskôr spracovať analýzu rizík. Tá mapuje skutočný spôsob spracúvania osobných údajov, jeho aktuálny stav a vymedzuje riziká, ktoré sú vzhľadom na aktíva informačného systému spôsobilé narušiť dôvernosť, integritu a dostupnosť spracúvaných osobných údajov. Analýzou vymedzené riziká vyúsťujú do bezpečnostných opatrení, ktoré majú zabrániť alebo na stanovenú mieru tieto riziká eliminovať. Analýza rizík nadväzuje na

bezpečnostný zámer, teda cieľ, ktorý sa má aplikáciou opatrení dosiahnuť.


Nakoľko každý prevádzkovateľ spracúva osobné údaje v špecifických podmienkach (objekt, v ktorom prevádzkovateľ sídli, zariadenia na ktorých informačný systém osobných údajov prevádzkuje, vrátane siete, nosiče, na ktorých sú osobné údaje evidované a uchovávané, oprávnené osoby, ktoré operácie s osobnými údajmi vykonávajú pri nastavení podmienok prístupu k nim atď.), **je potrebné sa pri vypracovaní bezpečnostného projektu riadiť požiadavkami**, ktoré z týchto podmienok vyplývajú.

Každý bezpečnostný projekt bude osobitý

Aj keď každý prevádzkovateľ, ktorý je zamestnávateľom, spracúva osobné údaje v informačnom systéme osobných údajov na účel zabezpečenia pracovno-právneho vzťahu so zamestnancami a vykonáva s osobnými údajmi operácie porovnateľné s iným zamestnávateľom, k spracúvaným osobným údajom môže mať prístup iný počet oprávnených osôb a to tak v listinnej, ako aj v automatizovanej forme. Prevádzkovateľ môže spracúvať osobné údaje v personálnom a mzdovom informačnom systéme osobných údajov na jednom počítači alebo na viacerých pracovných staniciach zapojených do počítačovej siete. Osobné údaje môžu byť spracúvané centralizovane alebo decentralizovane, príp. môžu byť predmetom cezhraničného toku. Všetky tieto podmienky spracúvania osobných údajov vyžadujú relevantné nastavenie bezpečnostných opatrení.

Z vyhlášky vyplýva, že 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. Takže aj takáto skutočnosť má vplyv na odlišnosť bezpečnostnej dokumentácie ochrany osobných údajov.

Nie je možné stanoviť univerzálny vzor bezpečnostného projektu, ktorý by jednotlivý prevádzkovateľ alebo sprostredkovateľ „naplnil“, ale každý takýto dokument je „originálom“ odrážajúcim osobité podmienky prevádzkovateľa príp. sprostredkovateľa spracúvajúceho osobné údaje vo svojich informačných systémoch.



Smernica o ochrane osobných údajov

Jedna z najhorúcejších tém dnešných dní!

Doplňte si vlastné údaje. Vytlačte. Používajte v praxi.

www.smerniceonline.sk Smernicu nájdete tu

Interné smernice potrebné pri účtovnej a daňovej kontrole sú súčasťou obsahu www.smerniceonline.sk

Smernica o pláne inventarizácie majetku a záväzkov

Smernica o oceňovaní majetku a záväzkov v účtovníctve

Smernica o zásadách tvorby a čerpania rezerv

Smernica o evidencii, oceňovaní a účtovaní zásob a iné.

Všetky vzorové smernice si môžete stiahnuť, prispôsobiť vašim požiadavkám v externom editore, vytlačiť a doložiť k účtovnej evidencii.

