

OCHRANA OSOBNÝCH ÚDAJOV V SÚVISLOSTIACH

1. júla 2013 nadobudol účinnosť zákon o ochrane osobných údajov č. 122/2013 Z. z. (ďalej len „zákon“), ktorý nahrádza pôvodný zákon č. 428/2002 Z. z. Spolu s novými vyhláškami a metodickými usmerneniami by mal priniesť do manipulácie s osobnými údajmi a ich ochrany jasné zodpovednosti a požiadavky. Tie v predchádzajúcom zákone chýbali. Prehliadnuť sa nedá ani výška sankcie, ktorá môže byť pre mnohé organizácie likvidačná, keďže siaha až do výšky 300 000 eur.

ZÁKLADNÝ VÝBER POVINNOSTÍ PREVÁDZKOVATEĽA OSOBNÝCH ÚDAJOV

- vypracovať písomnú zmluvu medzi prevádzkovateľom a každým sprostredkovateľom osobných údajov,
- spracúvať osobné údaje len v určenom rozsahu,
- bezpečne likvidovať osobné údaje,
- prijať organizačné, personálne a technické opatrenia na ochranu osobných údajov,
- vypracovať dokumentáciu o prijatých bezpečnostných opatreniach (bezpečnostná smernica / projekt)
- poučiť oprávnené osoby o ich právach, povinnostiach a o zodpovednosti za ich porušenie,
- vyhotoviť písomný záznam o poučení oprávnenej osoby,
- získavať osobné údaje na základe preukázateľného súhlasu dotknutej osoby a v súlade so zákonom,
- poveriť zodpovednú osobu, ktorá musí absolvovať skúšku na úrade,
- registrovať informačný systém, v ktorom sa spracúvajú osobné údaje úplne alebo čiastočne automatickými prostriedkami na úrade, ak nebude určená zodpovedná osoba,
- viesť evidenciu informačných systémov, na ktoré sa nevzťahuje povinnosť registrácie na úrade.

VÁŠ NOVÝ PROJEKT:

Ochrana osobných údajov



Implementáciu požiadaviek ochrany osobných údajov môžete realizovať formou celofiremného projektu, pretože často zasahuje do zaužívaných návykov pracovníkov naprieč celou organizačnou štruktúrou.

Zavádzané zmeny a opatrenia týkajúce sa ochrany osobných údajov vo firme môžu byť zamestnancami vnímané obmedzujúco a bez pochopenia ich podstaty nemajú účinok, rovnako ako všetky zmeny v organizácii. Ako teda začať s implementáciou nového zákona o ochrane osobných údajov?

Hneď v prvom kroku realizácie projektu je potrebné **identifikovať relevantné požiadavky zákona** pre konkrétnu prevádzku. Následne analyzovať **rozsah spracúvaných údajov, identifikovať všetky zainteresované strany a relevantné informačné systémy**. Zistiť a preveriť aktuálny stav manipulácie s osobnými údajmi a bezpečnostných opatrení, ktoré sú už v prevádzke implementované. Až po takejto dôslednej analýze môžu byť navrhnuté efektívne opatrenia na účinnú ochranu osobných údajov, ktoré sú v zmysle zákona potrebné popísať a zdokumentovať. Môže íť o pomerne široký záber informácií, z ktorých vypadne množstvo nezodpovedaných otázok. Preto sa na identifikáciu požiadaviek zákona využívajú konzultačné služby expertov, ktorí zároveň poznajú špecifiká daného odvetvia. Náklady na takéto konzultačné služby sa pohybujú od

150 eur až do 3-tisíc eur. Môže to byť aj viac. Toto široké rozpätie závisí od počtu informačných systémov, zložitosti a rozsahu spracúvania údajov, počtu zainteresovaných strán a pod.

zisk

AKO VÁS MÔŽE PODPORIŤ EXTERNÝ DODÁVATEĽ:

- identifikáciou relevantných požiadaviek, ktoré sa spoločnosti v úlohe prevádzkovateľa či sprostredkovateľa osobných údajov týkajú,
- vypracovaním bezpečnostnej dokumentácie v potrebnom rozsahu,
- prípravou kompletnej administratívnej agendy,
- preškolením a poučením oprávnenej osoby o pravidlách manipulácie s osobnými údajmi,
- výkonom zodpovednej osoby nad dohľadom ochrany osobných údajov, čím predídeme skúškam vlastných zamestnancov.

SKUTOČNE SA TO TÝKA AJ VÁS?

Do manipulácie s osobnými údajmi vstupuje viacero zainteresovaných strán. V prvom rade ide o **dotknutú osobu**, ktorej sa osobné údaje týkajú. Dotknutá osoba má svoje práva a povinnosti voči prevádz-

kovateľovi osobných údajov, ktorý získava a inak spracúva jej údaje na výkon svojej činnosti. **Prevádzkovateľ** si nesmie vynucovať získavanie osobných údajov. Poučení pracovníci, ktorí prichádzajú do kontaktu s osobnými údajmi, sú **oprávnené osoby**. Ich povinnosťou je dodržiavať interne stanovené pravidlá. Za výkon kontroly dodržiavania predpisov je stanovená **zodpovedná osoba** alebo štatutár prevádzkovateľa. Ak má firma externého dodávateľa, ktorý spracúva údaje v jeho mene, stáva sa sprostredkovateľom osobných údajov. Vzťah medzi prevádzkovateľom a sprostredkovateľom musí byť definovaný písomnou zmluvou. Najčastejšie ide o externých právnych zástupcov, účtovníčky, správcov informačných systémov s osobnými údajmi a pod. Na prácu s citlivými informáciami sa vytvárajú vhodné podmienky. Oprávnené osoby by mali manipulovať len s takými infor-

máciami a takým spôsobom, ktorý je nutný na výkon ich práce. **Snahou je zabrániť predovšetkým úmyselnému a náhodnému ohrozeniu dôvernosti údajov.** Moderné technické riešenia dnes dokážu oprávnenej osobe znemožniť tlač citlivých informácií, kopírovanie, uloženie na USB kľúče, DVD či zasielanie mailom.

VYTVORENIE KOMPLEXNÉHO PLÁNU (WBS)

Pri plánovaní projektových aktivít je potrebné vychádzať z termínov definovaných zákonom. Ako mílniky v projekte implementácie zákona definujeme nasledovné termíny:

- **do 31. 12. 2013** – zaregistrovať informačné systémy na úrade, ak spĺňajú §34 zákona,
- **do 31. 3. 2014** – zosúladiť bezpečnostnú dokumentáciu,
- **do 30. 6. 2014** – formalizovať vzťah medzi prevádzkovateľom a sprostredkovateľom písomnou zmlu-

vou, písomne poveriť zodpovednú osobu certifikovanú úradom.

Tabuľka 1 (na nasledujúcej strane) je ukážkou toho, ako môžete naplánovať projekt implementácie požiadaviek zákona č. 122/2013 Z. z. o ochrane osobných údajov. Znázorňuje jednotlivé fázy projektu, ich obsah, časové trvanie, plánované náklady a zodpovednosť za ich realizáciu.

PROJEKTOVÉ VÝSTUPY

Po implementácii požiadaviek zákona vzniká sada dokumentov a záznamov:

- **Bezpečnostné opatrenia** vypracované pre všetky identifikované informačné systémy bez pripojenia do verejne prístupných počítačových sietí (internet)
- **Bezpečnostná smernica** vypracovaná pre všetky relevantné informačné systémy s pripojením na internet alebo systémy s osobitnou kategóriou osobitných údajov (rodné číslo, biometria a pod.) bez pripojenia na internet
- **Bezpečnostný projekt** vypracovaný pre všetky informačné systémy s osobitnou kategóriou osobitných údajov s pripojením na internet
- **Záznamy o oboznámení sa s bezpečnostnou dokumentáciou oprávnených osôb**
- **Súhlasy dotknutých osôb** v preddefinovanej štruktúre
- **Zmluvy medzi prevádzkovateľom a jeho sprostredkovateľmi**, čím prevádzkovateľ prenáša zodpovednosť na externý subjekt, ktorý v jeho mene manipuluje s osobnými údajmi
- **Osvedčenie zodpovednej osoby** vydané úradom po úspešnom absolvovaní skúšky
- **Záznam o poverení zodpovednej osoby**
- **Záznamy o poučení oprávnených osôb**
- **Evidencia informačných systémov**
- **Záznamy z kontrolnej činnosti**
- **Záznamy zistených bezpečnostných incidentov a prijatých bezpečnostných opatrení** ▶

3 NAJČASTEJŠIE CHYBY (PROJEKTOVÉ RIZIKÁ)

CHYBA Č. 1:

„Nás sa zákon netýka, lebo osobné údaje nám spravuje iný subjekt.“

Zákon hovorí o povinnostiach všetkých zúčastnených strán pri spracúvaní osobných údajov, či už ste v úlohe prevádzkovateľa, sprostredkovateľa alebo subdodávateľa. Tento vzťah pritom musí byť preukázateľný vo forme písomnej zmluvy. Ak by niektorá strana zmluvu odmietla podpísať, tá druhá strana má povinnosť túto skutočnosť nahlásiť na úrad. Preto každý takýto subjekt podlieha požiadavkám zákona a hrozbe pokuty, ak na to nemá výnimku v osobitnom predpise SR alebo EÚ.

CHYBA Č. 2:

„Nepracujeme s rodnými číslami, teda ani s osobnými údajmi.“

Za osobné údaje treba považovať akékoľvek informácie o konkrétnej fyzickej osobe, na základe ktorých je možné túto osobu priamo alebo nepriamo identifi-

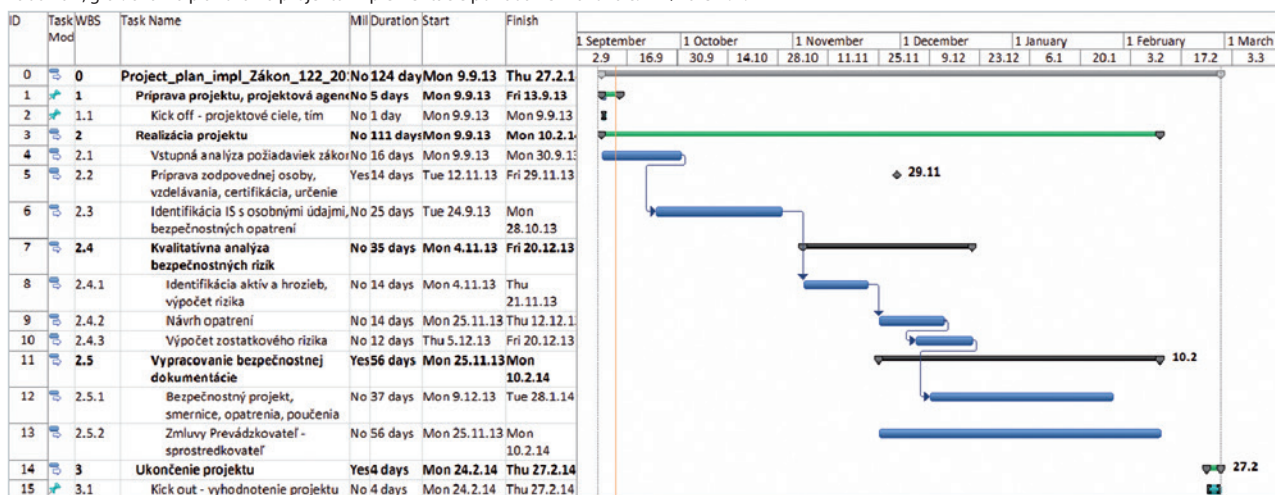
kovat. Len samotné meno a priezvisko nemusí spadať do kategórie osobných údajov, ak nie je jasné, o ktorú osobu ide. Ak k týmto informáciám pribudnú ďalšie údaje, napr. názov zamestnávateľa, potom sa okruh dotknutých osôb výrazne zníži. Takáto informácia sa môže považovať za osobný údaj. Získaním ďalších informácií o osobe (adresa, telefónne číslo, dátum narodenia, rodné číslo dotknutej osoby, biometrické údaje a pod.) rastie riziko ich úniku a negatívny dosah.

CHYBA Č. 3:

„Použijeme univerzálnu bezpečnostnú dokumentáciu.“

Univerzálna bezpečnostná dokumentácia neexistuje. Neodrzakladuje skutočnú prevádzku spracúvania osobných údajov. *Príklad z praxe:* Prevádzkovateľ mal v bezpečnostnom projekte uvedené, že osobné údaje ukladá v tlačenej forme do kovových uzamykateľných skriní. Skrine neexistovali. Porušenie interných predpisov bolo jednoznačné.

Tabuľka 1, graf: Ukážka plánovania projektu implementácie požiadaviek zákona č. 122/2013 Z. z.



ELEKTRONIZÁCIA DOKUMENTOV – PRIDANÁ HODNOTA PRE BIZNIS

Ako je možné pracovať s osobnými údajmi bez generovania veľkého množstva papierových dokumentov? A súčasne dodržiavať zákon? Pripravovaná elektronizácia štátnej správy a trendy v moderných technológiách menia myslenie. Inovujú sa zaužívané činnosti ľudí v práci i v súkromí. Spoločnostiam urýchľujú biznis, znižujú prevádzkové náklady, priťahujú nových zákazníkov, ale aj nadšených mladých zamestnancov. Získavanie súhlasov na spracúvanie osobných údajov, ich uchovávanie a predkladanie nemusí byť s využitím moderných technológií obťažujúce a zdĺhavé.

Praktická aplikácia procesu získavania súhlasov dotknutých osôb s využitím mobilných zariadení:

- použitie tabletov na pracovných stretnutiach,
- atraktívna prezentácia marketingových materiálov, videí, referencií,

- jednoduché získanie osobných údajov aj so súhlasom dotknutých osôb vizuálnym elektronickým podpisom na tablete do zobrazeného formulára,
- odoslanie zašifrovaných údajov vo formáte PDF mailom,
- presun zašifrovaných údajov do centrálneho firemného úložiska alebo informačného systému,
- zabudované bezpečnostné prvky ochrany údajov priamo v tablete,
- centrálna správa tabletov v prípade ich krádeže alebo poruchy.

Prínos inovatívneho prístupu:

- úspora času pracovníkov operatívny,
- získanie transparentného procesu tvorby dokumentov, riadenia prístupov a monitorovania práce s citlivými údajmi,
- zefektívnenie vyhľadávania informácií,
- ľahšie zabezpečenie povinnosti získavania súhlasov dotknutých osôb pri využití mobilných zariadení,

- dostupnosť súhlasov priamo v databázach s osobnými údajmi,
- odbúranie nadbytočnej byrokracie,
- konkurenčná výhoda,
- výrazné zníženie nákladov na tlač dokumentov, prenájom priestorov, fyzické uchovávanie a archiváciu,
- eliminácia nákladov na služobné výjazdy do centrálnych archívov,
- nie je fikcia budúcnosti, ale efektívne využívanie informačných technológií.

Ďalšie príležitosti:

- dôsledný prístup = príležitosť na certifikáciu podľa ISO 27001,
- zmena firemnej kultúry,
- manažment získava prehľad o forme spracúvania citlivých údajov,
- predvídanie potenciálnych rizík a včasná reakcia na elimináciu ich dosahu.



Inšpirujte sa príbehmi v projektovom manažmente.

www.bpug.sk

zisk PREČO OCHRANU OSOBNÝCH ÚDAJOV RIEŠIŤ PROJEKTOVO?

- týka sa to všetkých, náročný a dynamický projekt,
- nový pohľad a dosah,
- komplexná problematika celej firmy,
- jasne stanovené termíny a zodpovednosti,
- vyššia prehľadnosť v procese implementácie a následné dodržiavanie povinností. ■

Autori:

Erika Slivová, ANASOFT APR,
Peter Minárik, COMM-PASS

MESAČNÍK PRE OSOBNÝ A PROFESIONÁLNY RAST



Zisk
manažment
si môžete objednať
telefonicky na:
041 70 53 222
alebo e-mailom na:
služby@ezisk.sk
www.ezisk.sk

Zisk manažment je mesačník, ktorý čitateľom prináša praktické informácie a návody na to:

- ako viesť a riadiť firmu,
- ako úspešne podnikať,
- ako nájsť správnych zamestnancov,
- ako ich motivovať inou ako finančnou formou,
- ako odhaliť povalačov,
- ako hodnotiť a odmeňovať,
- ako vybudovať dobré meno firmy,
- ako na trhu preraziť a ochromiť konkurenciu,
- ako pri podnikaní ušetriť,
- ako sa úspešní stali úspešnými,
- ako byť spoločensky zodpovedný,
- ako si získať a udržať zákazníka,
- ako zákazníka nestraťiť,
- ako robiť marketing (nielen) na internete,
- ako na sociálne siete,
- ako riadiť seba a svoj profesionálny rast,
- ako sa stať lídrom,
- ako profesionálne „nevyhorieť“.

Manažérom, personalistom, marketérom a podnikateľom poskytuje praxou overené rady a nápady, ktoré smerujú k zvyšovaniu zisku v podniku. Viac o mesačníku Zisk manažment nájdete na www.ezisk.sk.

**VŽDY
SA NÁJDE
DIERA NA TRHU,
KDE UVIDÍTE
ZISK**