Ochrana osobních údajů v podmínkách MÚ

Orgány územní samosprávy jsou, ze zákona a z principu své funkce, správci a zpracovateli osobních údajů ve smyslu Zákona č. 101/2000 Sb., o ochraně osobních údajů. Tato skutečnost jim zakládá povinnosti při ochraně osobních údajů před neoprávněným užitím (§13).

Novelizacemi zákona v posledních letech byly tyto povinnosti zpřísněny, mj. v roce 2004 o povinnost zpracovat a dokumentovat přijetí a provedení technicko-organizačních opatření k zajištění ochrany osobních údajů a v roce 2007 o další povinnosti týkající se oblastí posuzování rizik, řízení přístupů k systémům pro automatizovaná zpracování osobních údajů atd.

Novelizace zákona z roku 2004 nabyla účinnosti 26. 7. 2004, to znamená, že dosavadní správci osobních údajů byli povinni předložit požadovanou dokumentaci do 26. 1. 2005 (§47). Novelizace zákona z roku 2007 nabyla účinnosti 1. 9. 2007.

Chybějící nebo nedostatečná opatření či jejich dokumentace může být postihována vysokými sankcemi ukládanými Úřadem pro ochranu osobních údajů, pokutou až do výše 10.000.000 Kč (§45). § 49 uvádí „Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném, shromážděné v souvislosti s výkonem veřejné správy, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem."

Přes uvedená zpřesnění jsou formulace zákona poměrně vágní, co se týče druhu a způsobu požadovaných technicko-organizačních opatření a jejich dokumentace. ÚOOÚ nevydal a ani nemá v úmyslu vydat metodický pokyn, směrnici, závazný výklad či jiný dokument, který by požadavky přesněji specifikoval. Přiměřenost a účinnost opatření a kvalita jejich dokumentace je posuzována individuálně a subjektivně inspektorem ÚOOÚ.

Zpracování osobních údajů se v podmínkách MÚ provádí zpravidla s pomocí informačních technologií. Po řadě konzultací s pracovníky ÚOOÚ jsme dospěli ke shodě v tom, že s velkou pravděpodobností lze za přiměřená a dostatečná technicko-organizační opatření a jejich dokumentaci považovat řádnou implementaci tzv. Systému řízení bezpečnosti informací (ISMS).

ISMS je souborem opatření, metod, zásad a pravidel, vycházejících z osvědčených praktických postupů. Je popsán a standardizován mezinárodními normami, platnými v ČR, EU i většině rozvinutých zemí světa. Principy jsou definovány dostatečně pružně, aby bylo možné jim rozsah a kvalitu opatření přizpůsobit, jak v různé míře citlivosti zpracovávaných informací, tak i v různé velikosti, charakteru a struktuře organizace.

Systém řízení bezpečnosti informací obsahuje tyto základní části:

- Analýza bezpečnostních rizik - co máme, jakou to má hodnotu, jaká existují rizika.
- Bezpečnostní dokumentace - co a jak máme udělat v jednotlivých oblastech práce s informacemi pro jejich bezpečnost.
- Bezpečnostní plán - kdo, kdy a za kolik to udělá.
- Kontrola účinnosti a účelnosti opatření - audity, monitorování a vyhodnocování, revize dokumentace.

Pro IT

Pracovníci společnosti Pro IT, zkušení řešitelé systémů řízení informační bezpečnosti (mj. Úřad vlády ČR, Statutární město Ostrava), jsou si vědomi složitosti problematiky a obtíží při jejím zvládání, zejména při omezeném počtu pracovníků. Přinášíme proto soubor pomůcek pro řešení informační bezpečnosti v podmínkách menších a středních MÚ:

- Vysvětlení postupu při provádění a vyhodnocení analýzy bezpečnostních rizik podle ČSN ISO/IEC 13335.
- Program RANIT pro provádění rizikových analýz, obsahující předběžně nastavené parametry a katalogy pro potřeby MÚ.
- Vzorovou bezpečnostní dokumentaci, obsahující všechny potřebné kapitoly podle ČSN ISO/IEC 17799, která vás povede při tvorbě dokumentace pro podmínky konkrétního úřadu.
- Vzorový bezpečnostní plán, s návodem pro vyplnění podle skutečných opatření, která musí váš MÚ provést.
- Postup pro provedení vnitřního auditu bezpečnosti informací podle ČSN ISO IEC 27001.

Nejedná se však o pouhý „balík" s nímž byste si museli sami poradit. Součástí dodávky je i práce poradce - specialisty na informační bezpečnost. Ten vám pomůže přizpůsobit dokumentaci vašim potřebám, vytipuje kritické problémy, které je třeba řešit, naučí vás školit zaměstnance v bezpečnosti práce s informacemi.

Na základě zkušeností s implementací ISMS v řadě orgánů územní samosprávy, jsme přesvědčeni, že tyto pomůcky budou účinnou pomocí pro menší a střední MÚ, které jsou nuceny splnit zákonné požadavky v ochraně informací.

Nabízené pomůcky nemohou „udělat bezpečnost" za vás. Ušetří vám však mnoho úsilí při hledání správného postupu, nebo nákladů na služby specializované konzultační firmy.

Soubor pomůcek a služeb k implementaci ISMS		
Položka	**Cena bez DPH**	**Cena s DPH**
Obce do 10.000 obyvatel Soubor pomůcek, konzultační služby na místě v rozsahu 2 člověkodnů, včetně cestovních nákladů	40.000 Kč	47.600 Kč
Obce do 30.000 obyvatel Soubor pomůcek, konzultační služby na místě v rozsahu 4 člověkodnů, včetně cestovních nákladů	60.000 Kč	71.400 Kč
Obce nad 30.000 obyvatel	dle samostatné nabídky	

Pro IT, a.s.

Mírová 166/23, Ostrava-Vítkovice, PSČ 703 00, www.proit.cz

obchod@proit.cz, +420 595 174 250