

Správa o výsledku následnej finančnej kontroly

Na základe plánu kontrolnej činnosti útvaru hlavnej kontrolórky na 1.polrok 2010, schváleného uznesením MsZ č.181/2009 z 18.11.2009, vykonali Ing. Ingrid Veverková, hlavná kontrolórka Mesta Brezna a JUDr. Iveta Biela, kontrolórka mesta Brezna

následnú finančnú kontrolu dodržiavania a uplatňovania zákona o ochrane osobných údajov

Predmet následnej finančnej kontroly:

- kontrola dodržiavania a uplatňovania zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov a súvisiacich všeobecne záväzných právnych predpisov upravujúcich kontrolovanú oblasť v podmienkach kontrolovaného subjektu

Cieľ následnej finančnej kontroly:

- overiť objektívny stav kontrolovaných skutočností a ich súlad so všeobecne záväznými právnymi predpismi a vnútornými aktmi riadenia
- overiť, ako je v kontrolovanom subjekte zabezpečená ochrana osobných údajov fyzických osôb pri spracúvaní ich osobných údajov, bezpečnosť osobných údajov, ochrana práv dotknutých osôb
- overiť, ako má kontrolovaný subjekt zabezpečené zásady spracúvania osobných údajov a registráciu a evidenciu informačných systémov.

Kontrola dodržiavania základných povinností pri ochrane osobných údajov

Kontrolou bolo zistené, že mestský úrad (ďalej len „MsÚ“) si pri ochrane osobných údajov neplní svoje zákonné povinnosti alebo ich plnenie nevie kontrolnému orgánu preukázať; kontrolovaný subjekt pri ochrane osobných údajov nepostupuje v súlade s ustanovením § 6 ods. 1 zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „zákon“).

V tejto oblasti bolo konštatované 1 kontrolné zistenie.

Kontrola získavania a spracovania osobných údajov

Kontrolou bolo zistené, že MsÚ si pri získavaní a spracúvaní osobných údajov neplní svoje zákonné povinnosti alebo ich plnenie nevie kontrolnému orgánu preukázať.

Kontrolou bolo zistené, že v niektorých kontrolovaných prípadoch si zamestnanci kontrolovaného subjektu neplnili svoje povinnosti, resp. nepreukázali kontrolnému orgánu plnenie si týchto povinností, vyplývajúcich z ustanovenia § 10 ods.1 zákona, konkrétne:

a) pri získavaní osobných informácií neinformovali vopred dotknutú osobu a bez vyzvania jej vopred neoznámili napr. účel spracúvania osobných údajov príp. ďalšie doplňujúce informácie v takom rozsahu, v akom sú s ohľadom na všetky okolnosti spracúvania osobných údajov potrebné pre dotknutú osobu na zaručenie jej práv a právom chránených záujmov; tieto povinnosti nebolo možné zabezpečiť už z dôvodu, že pre dotknuté činnosti nie je vydaný evidenčný list informačného systému a teda účel a ostatné súvisiace údaje pre získavanie osobných údajov nijakým spôsobom nie sú stanovené;

b) dotknutú osobu nepoučili, že má právo byť informovaná o podmienkach spracúvania svojich osobných údajov a to preukázaním totožnosti oprávnenej osoby, ktorá získava osobné údaje a poučením o dobrovoľnosti alebo povinnosti poskytnúť požadované osobné údaje (prevádzkovateľ má oznámiť dotknutej osobe, na základe akého právneho podkladu mieni spracúvať jej osobné údaje a ak dotknutej osobe povinnosť poskytnúť osobné údaje vyplýva z osobitného zákona, prevádzkovateľ oznámi dotknutej osobe zákon, ktorý jej túto povinnosť ukladá a upovedomí ju o následkoch odmietnutia poskytnúť osobné údaje). Uvedené vyplýva zo zistenia, že v niektorých kontrolovaných prípadoch osobné údaje získavali a spracúvali zamestnanci, u ktorých kontrolovaný subjekt nepreukázal vykonanie poučenia o ich právach a povinnostiach pri získavaní a spracúvaní osobných údajov a o zodpovednosti za ich porušenie v zmysle § 17 zákona.

MsÚ pri získavaní a spracúvaní osobných údajov nepostupuje v súlade s ustanovením § 7 ods. 1, §10 ods.1 zákona o ochrane osobných údajov.

V tejto oblasti bolo konštatovaných 16 kontrolných zistení.

Kontrola zabezpečenia zodpovednosti za ochranu osobných údajov

MsÚ má pre zabezpečenie zodpovednosti za ochranu osobných údajov spracovaný „Bezpečnostný projekt informačného systému na Mestskom úrade v Brezne“ (ďalej len „bezpečnostný projekt“); problém je, že tento bezpečnostný projekt bol vydaný v roku 2003 a do dňa začatia kontroly v roku 2010 platí v znení z tohto roku (k zmenám a doplnkom v jeho obsahu nedošlo). Po jeho vydaní bol zákon niekoľkokrát novelizovaný, teda zmeny legislatívy sa do obsahu projektu nepremietli, rovnako ako ani zmeny obsahu súvisiacich vnútorných noriem kontrolovaného subjektu, napr. organizačného poriadku. Z toho dôvodu kontrolný orgán považuje tento bezpečnostný projekt za neaktuálny.

Kontrolou obsahu bezpečnostného projektu bolo zistené, že bezpečnostný projekt: obsahuje predovšetkým úpravu zameranú na oblasť automatizovaného (počítačového) informačného systému; ostatným súčasťami informačného systému, v rámci ktorých sa taktiež získavajú a spracúvajú osobné údaje, je v projekte venovaná len okrajová, resp. nedostatočná pozornosť.

Kontrolou bolo zistené, že MsÚ v rámci zabezpečenia zodpovednosti za ochranu osobných údajov:

- nemá spracovaný bezpečnostný projekt v súlade s príslušnými ustanoveniami zákona o ochrane osobných údajov;
- nemá zabezpečenú ochranu osobných údajov v tom slova zmysle, že nemá stanovený rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému a rovnako nemá stanovený rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov;
- nemá zabezpečený systém výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému (kontrolovaný subjekt nepreukázal kontrolnému orgánu vykonanie ani jednej kontroly od roku 2002).

MsÚ pri zabezpečení zodpovednosti za ochranu osobných údajov nekonal v súlade s § 16 ods. 2, 4 až 6 zákona o ochrane osobných údajov.

V tejto oblasti boli konštatované 3 kontrolné zistenia.

Kontrola realizácie dohľadu nad ochranou osobných údajov

MsÚ v rámci výkonu dohľadu nad ochranou osobných údajov mal povinnosť písomne poveriť zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov.

Kontrolou boli zistené vážne pochybenia pri plnení si tejto povinnosti zo strany MsÚ:

- chýbali a chýbajú poverenia zodpovedných osôb na výkon dohľadu nad ochranou osobných údajov,
- existujúce poverenia nie sú spracované dostatočne a dôsledne podľa § 19 ods.2 zákona,
- chýbajú potvrdenia o vykonaní odborného vyškolenia zodpovedných osôb a rozsahu v akom bolo školenie vykonané a výpisov z registra trestov zodpovedných osôb podľa § 19 ods.2 zákona

Kontrolný orgán uvedené skutočnosti hodnotí ako zistenie s obzvlášť závažným dôsledkom; keďže kontrolovaný subjekt nevie relevantne preukázať splnenie podmienok, ktoré zákon určuje, resp. spája s výkonom činnosti zodpovedných osôb podľa § 19 ods.2 zákona, je tým spochybnená legálnosť písomných poverení týchto osôb a následne ich oprávnenosť pre výkon činnosti na základe poverení.

MsÚ si nesplnil povinnosti prevádzkovateľa vyplývajúce z ustanovenia § 55 ods.2 v spojení s ustanovením § 19 ods.5 zákona o ochrane osobných údajov a nepreukázal splnenie podmienok určených v ustanovení § 19 ods. 2, 3,5 a 12 zákona o ochrane osobných údajov pre výkon činnosti osôb zodpovedných za výkon dohľadu nad ochranou osobných údajov.

V tejto oblasti bolo konštatovaných 5 kontrolných zistení.

Kontrola vykonania poučenia oprávnených osôb o právach a povinnostiach vyplývajúcich zo zákona

Z ustanovenia § 4 ods.4 zákona vyplýva, že oprávnenou osobou je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu....., na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie podľa § 17 zákona je prevádzkovateľ povinný poučiť oprávnené osoby o právach a povinnostiach ustanovených týmto zákonom a o zodpovednosti za ich porušenie

Kontrolný orgán požiadal MsÚ o predloženie úplného a kompletného zoznamu oprávnených osôb, aktuálny ku dňa začatia kontroly. MsÚ predložil kontrolnému orgánu písomné vyjadrenie, podľa ktorého tento doklad *Mestský úrad nemá a nemôže ho ku kontrole predložiť*. Na základe tejto skutočnosti kontrolný orgán nemá možnosť skontrolovať, či všetky oprávnené osoby, resp. osoby ktoré pri výkone svojej funkcie prichádzajú do styku s osobnými údajmi, majú spracované poučenie oprávnených osôb podľa § 17 zákona. V tejto súvislosti môže len konštatovať, že medzi predloženými poučeniami sa nenachádzajú poučenia oprávnených osôb podľa § 17 zákona zamestnancov, ktorí nepochybne prichádzajú pri výkone svojej činnosti do styku s osobnými údajmi.

MsÚ kontrolnému orgánu nepreukázal zabezpečenie účinného systému ochrany osobných údajov - kontrolovaný subjekt nemá spracovanú bezpečnostnú smernicu, v ktorej by bol vymedzený rozsah zodpovednosti ako aj rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému podľa ustanovenia § 19 ods. 6 písm. b) a c) zákona o ochrane osobných údajov.

MsÚ kontrolnému orgánu nepreukázal splnenie podmienok určených v ustanovení § 17 zákona o ochrane osobných údajov - povinnosť poučiť o právach a povinnostiach pre výkon činnosti všetkých oprávnených osôb podľa § 4 ods. 4 zákona o ochrane osobných údajov.

V tejto oblasti bolo konštatovaných 6 kontrolných zistení.

Kontrola registrácie a evidencie informačných systémov

Kontrolný orgán požiadal MsÚ o predloženie úplnej a kompletnej evidencie informačných systémov u prevádzkovateľa, t.j. úplného a kompletného zoznamu evidenčných listov informačných systémov odo dňa účinnosti zákona až do dňa začatia kontroly. MsÚ predložil kontrolnému orgánu písomné vyjadrenie, podľa ktorého túto evidenciu, resp. zoznam evidenčných listov informačných systémov *Mestský úrad nemá a nemôže ho ku kontrole predložiť*. Ako dokumentáciu z evidencie informačných systémov predložených ku kontrole kontrolovaný subjekt predložil len 13 dokumentov s označením „Evidenčný list informačného systému“.

Na základe uvedeného stavu nie je možné zo strany kontrolného orgánu vyhodnotiť, či predložené dokumenty s označením „Evidenčný list informačného systému“ (ďalej len „evidenčné listy“) sú splnením povinnosti kontrolovaného subjektu podľa § 25 ods. 2 zákona (povinnosť registrácie sa vzťahuje na všetky informačné systémy, v ktorých sa spracúvajú osobné údaje úplne alebo čiastočne automatizovanými prostriedkami spracúvania s výnimkou zákonom vymedzených informačných systémov) v spojitosti s § 29 ods. 1 zákona (o informačných systémoch, ktoré nepodliehajú registrácii, prevádzkovateľ vedie evidenciu, a to najneskôr odo dňa začatia spracúvania údajov v týchto informačných systémoch).

MsÚ kontrolnému orgánu nepreukázal splnenie svojej zákonnej povinnosti vyplývajúcej z § 25 ods. 2 zákona o ochrane osobných údajov v spojitosti s § 29 zákona o ochrane osobných údajov.

Kontrolou predložených evidenčných listov bolo zistené, že tieto nie sú evidenciou podľa § 29 zákona o informačných systémoch, rovnako v ich obsahu boli zistené vážne nedostatky.

MsÚ pri evidencii informačných systémov nekonal v súlade s § 29 a § 30 ods.3 zákona o ochrane osobných údajov.

V tejto oblasti boli konštatované 4 kontrolné zistenia.

Na základe výsledkov kontroly, uvedených v správe o výsledku následnej finančnej kontroly, kontrolný orgán uložil vedúcemu kontrolovaného subjektu v termíne do 9.8.2010 prijať konkrétne opatrenia na odstránenie zistených nedostatkov a ich príčin a určiť osoby zodpovedné