2017

Záverečná správa

Ochrana osobných údajov v informačných systémoch vybraných miest

Záverečná správa

Ochrana osobných údajov v informačných systémoch vybraných miest

PREDKLADÁ
Ing. Karol Mitrík, predseda
Najvyšší kontrolný úrad Slovenskej republiky

VEDÚCI KONTROLNEJ AKCIE
Mgr. Roman Furda

Bratislava, apríl 2017

OBSAH

ZOZNAM SKRATIEK A SKRÁTENÝCH POMENOVANÍ

SKRATKA	VÝZNAM
DCOM	Dátové centrum obcí a miest
IKT	Informačno-komunikačné technológie
ISSAI	Medzinárodné štandardy najvyšších kontrolných inštitúcií (International Standards of Supreme Audit Institutions)
ISVS	Informačný systém verejnej správy
KRIS	Koncepcia rozvoja informačných systémov verejnej správy
MetaIS	Centrálny metainformačný systém verejnej správy Slovenskej republiky
NKÚ SR	Najvyšší kontrolný úrad Slovenskej republiky
NR SR	Národná rada Slovenskej republiky
vyhláška o rozsahu a dokumentácii bezpečnostných opatrení	Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení v znení vyhlášky č. 117/2014 Z. z.
výnos MF SR o štandardoch pre ISVS	Výnos Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon o ISVS	Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon o NKÚ SR	Zákon NR SR č. 39/1993 Z. z. o Najvyššom kontrolnom úrade Slovenskej republiky v znení neskorších predpisov
zákon o niektorých súvislostiach s oznamovaním protispoločenskej činnosti	Zákon č. 307/2014 Z. z. o niektorých súvislostiach s oznamovaním protispoločenskej činnosti a o zmene a doplnení niektorých zákonov
zákon o ochrane osobných údajov	Zákon č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 84/2014 Z. z.
zákon o e-Governmente	Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
zákon o obecnom zriadení	Zákon Slovenskej národnej rady č. 369/1990 Zb. o obecnom zriadení v znení neskorších predpisov
zákon o slobodnom prístupe k informáciám	Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov
zákon o účtovníctve	Zákon č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov

ZHRNUTIE

NKÚ SR vykonal v súlade s plánom kontrolnej činnosti na rok 2016 kontrolnú akciu zameranú na zabezpečenie ochrany osobných údajov v informačných systémoch vybraných miest. Kontrolná akcia bola vykonaná na základe získaných poznatkov z vykonaných kontrol ISVS, nakoľko dochádza k porušovaniu najmä v oblasti ochrany osobných údajov a zabezpečenia technických opatrení na zamedzenie prístupu tretích strán k údajom v ISVS. Účelom kontrolnej akcie bolo preverenie stavu dodržiavania všeobecne záväzných právnych predpisov v oblasti ochrany osobných údajov v informačných systémoch vybraných miest. Kontrola bola vykonaná v piatich kontrolovaných subjektoch – Mesto Piešťany, Mesto Hlohovec, Mesto Galanta, Mesto Sládkovičovo a Mesto Holíč, za obdobie rokov 2015 a 2016. V prípade potreby bola kontrolovaná oblasť podľa predmetu kontroly, zdokumentovaná aj za predchádzajúce obdobie.

Kontrolná akcia bola vykonaná v súlade so zákonom o NKÚ SR a so štandardmi, ktoré vychádzajú zo základných princípov ISSAI.

Predmetom kontroly bolo: popis IKT prostredia a vynaložené finančné prostriedky, ochrana osobných údajov a bezpečnosť ISVS, prevádzka ISVS, dodržiavanie všeobecne záväzných právnych predpisov pre oblasť ISVS. Na základe profesionálneho úsudku kontrolóra boli pri kontrole použité neštatistické metódy, porovnávacie a analytické metódy.

Vo všetkých kontrolovaných subjektoch bola vykonaná inventarizácia majetku, záväzkov, aj rozdielu majetku a záväzkov k 31. decembru 2015 v zmysle ustanovení zákona o účtovníctve. V podkladoch inventarizácie majetku kontrolovaného subjektu sa kontrolná skupina zamerala len na majetok súvisiaci s IKT.

V kontrolovaných subjektoch sa pohybovala obstarávacia cena IKT majetku (k 31. decembru 2015), v porovnaní s celkovým majetkom, v rozmedzí od 0,51 % do 1,16 %. Pomer sumy došlých faktúr za IKT majetok, v porovnaní so súhrnnou sumou všetkých došlých faktúr v kontrolovanom období (od 1. januára 2015 do 30. septembra 2016), sa v kontrolovaných subjektoch pohyboval v rozmedzí od 1,72 % do 3,87 %.

V rámci kontroly boli na inventúrnych súpisoch zistené formálne nedostatky (napr. neboli uvedené mená zodpovedných zamestnancov, neboli uvedené podpisy zodpovedných zamestnancov a na jednom kontrolovanom subjekte boli, ako zodpovedné osoby, uvedení zamestnanci, ktorí už nepracovali na Mestskom úrade).

Ďalej NKÚ SR zistil, že jeden kontrolovaný subjekt v čase výkonu kontroly nemal v súlade so zákonom o obecnom zriadení schválený, ba ani vypracovaný štatút mesta.

V rámci preverenia ochrany osobných údajov a bezpečnosti ISVS bola kontrola zameraná aj na kvalitu a dodržiavanie interných predpisov kontrolovaných subjektov, ich bezpečnostnej dokumentácie (bezpečnostný projekt, bezpečnostná politika, bezpečnostná smernica, atď.), účinnosť a povinnosti z nich vyplývajúce. Okrem iného bolo zistené:

- štyri kontrolované subjekty v informačnom systéme nemali v politike hesiel nastavené všetky parametre hesla v súlade s bezpečnostnou dokumentáciou
- prideľovanie a rušenie oprávnení do informačného systému nebolo realizované prostredníctvom po formálnej stránke zavedeného procesu v bezpečnostnej dokumentácii
- na jednom kontrolovanom subjekte v privilegovanej skupine používateľských účtov sa nachádzal neblokovaný používateľský účet bývalého zamestnanca s tak nastaveným parametrom hesla, aby nikdy nevypršalo
- na dvoch kontrolovaných subjektoch pri prihlasovaní do informačného systému nebola zabezpečená jedinečná identifikácia, autentifikácia a autorizácia, čo nebolo v súlade s prijatou bezpečnostnou dokumentáciou, ktorá bola vypracovaná v zmysle zákona o ochrane osobných údajov
- na dvoch kontrolovaných subjektoch mali nastavené pracovné stanice používateľov tak, že používateľ mohol vykonať zmenu konfigurácie pracovnej stanice, inštaláciu programov a nelegálneho programového vybavenia, čo nebolo v súlade s prijatou bezpečnostnou dokumentáciou
- na dvoch kontrolovaných subjektoch mali v používateľských skupinách správcov informačného systému s administrátorskými právami zaradených používateľov, ktorí neboli správcami systému.

Ako to vyplýva z uvedených zistení, kontrolované subjekty nemali dostatočne zabezpečenú implementáciu nariadení stanovených v bezpečnostnej dokumentácii, ktorá spresňuje a aplikuje bezpečnostné opatrenia v zmysle zákona o ochrane osobných údajov, a dostatočne nezabezpečovali ani realizáciu schválenej bezpečnostnej politiky v zmysle výnosu MF SR o štandardoch pre ISVS.

Tri kontrolované subjekty mali uzavretú zmluvu s dodávateľom služby o poskytovaní služieb, kde mal kontrolovaný subjekt povinnosť zabezpečiť potrebný vzdialený prístup do svojej siete, avšak ani jedna z nich neobsahovala bezpečnostné požiadavky na tieto služby v súlade s výnosom MF SR o štandardoch pre ISVS.

Ďalej NKÚ SR zistil, že v každom kontrolovanom subjekte sa v priestoroch serverovne nachádzali horľavé materiály, ktoré by mohli (za istých okolností) ohroziť bezpečnosť informačného systému; v dvoch kontrolovaných subjektoch serverovňa nebola dostatočne chránená pred fyzickým prístupom nepovolaných osôb, čo bolo v rozpore s výnosom MF SR o štandardoch pre ISVS.

Kontrolované subjekty mali formálne popísané procesy zálohovania a archivácie v predloženej bezpečnostnej dokumentácii, avšak niektoré nemali vypracované protokoly o obnove dát zo zálohy, nevykonávali test obnovy informačného systému; jeden kontrolovaný subjekt nemal vypracovanú stratégiu zálohovania ani procedúru na zálohovanie a obnovu informačných systémov.

V rámci preverenia dodržiavania všeobecne záväzných právnych predpisov pre oblasť ISVS, bola kontrola zameraná na preverenie vybraných ustanovení zákona o ISVS, výnosu MF SR o štandardoch pre ISVS, zákona o ochrane osobných údajov a zákona o e-Governmente.

Hlavné zistenia v preverovanej oblasti boli tieto:

- jeden kontrolovaný subjekt nemal vypracovanú KRIS, čo nebolo v súlade so zákonom o ISVS
- v čase výkonu kontroly sa v MetaIS nenachádzali žiadne elektronické služby poskytované kontrolovanými subjektmi, ani informácie o informačných systémoch prevádzkovaných kontrolovanými subjektmi, čo nebolo v súlade so zákonom o ISVS, pretože kontrolované subjekty, ako povinné osoby, bezodkladne nesprístupňovali informácie o ISVS prostredníctvom MetaIS, ktoré prevádzkujú
- tri kontrolované subjekty nemali vytvorenú e-mailovú adresu v tvare „info“ pred deliacim znakom @, slúžiacu na poskytovanie informácií osobám podľa zákona o slobodnom prístupe k informáciám, čo nebolo v súlade s výnosom MF SR o štandardoch pre ISVS
- jeden kontrolovaný subjekt nemal schválenú, ba ani vypracovanú bezpečnostnú politiku, čo nebolo v súlade s výnosom MF SR o štandardoch pre ISVS
- vo viacerých prípadoch uvedených v tejto správe, ISVS kontrolovaných subjektov nebol v súlade s výnosom MF SR o štandardoch pre ISVS, čím kontrolované subjekty postupovali v rozpore so zákonom o ISVS
- jeden kontrolovaný subjekt nepostupoval v súlade so zákonom o ochrane osobných údajov, pretože nezabezpečil súlad informačného systému do 9 mesiacov od účinnosti zákona o ochrane osobných údajov, a kontrolnej skupine nepredložil evidenčné listy ku všetkým informačným systémom, identifikovaných bezpečnostným projektom ako informačné systémy, v ktorých sú spracúvané osobné údaje
- niektoré evidenčné listy informačných systémov, v ktorých sú spracúvané osobné údaje, mali formálne nedostatky (napr. chýbal zoznam osobných údajov, právny základ spracúvania osobných údajov, okruh dotknutých osôb), a v jednom prípade nebol názov informačného systému, uvedený v bezpečnostnom projekte, v súlade s názvom uvedeným v evidenčnom liste; čo nebolo v súlade so zákonom o ochrane osobných údajov
- v jednom kontrolovanom subjekte boli predložené poučenia oprávnených osôb, ktoré neobsahovali všetky náležitosti poučenia oprávnenej osoby v súlade so zákonom o ochrane osobných údajov.

NKÚ SR počas kontroly zistil, že všetky kontrolované subjekty mali zriadený prístup a disponovali elektronickou schránkou verejnej moci.

Jeden kontrolovaný subjekt mal v zmysle schválenej KRIS zriadený portál elektronických služieb (portál eGov), avšak občania ku dňu 7. novembru 2016 nevyužívajú žiadne poskytované elektronické služby, zároveň žiaden občan tohto kontrolovaného subjektu nemal zriadený prístup do privátnej časti na portáli eGov. Ďalší kontrolovaný subjekt plánuje poskytovať elektronické služby občanom prostredníctvom portálu elektronických služieb (eGov).

Jeden kontrolovaný subjekt podpísal zmluvu o pripojení k informačnému systému DCOM; jeden kontrolovaný subjekt plánuje využívať iba základné elektronické služby prostredníctvom informačného systému DCOM, ktoré vyplývajú z platnej legislatívy a ktoré sú v súčasnej ponuke DCOM.

1 CIEĽ KONTROLNEJ AKCIE

Účelom kontrolnej akcie bolo preverenie stavu dodržiavania všeobecne záväzných právnych predpisov v oblasti ochrany osobných údajov v informačných systémoch vybraných miest.

Predmet kontroly:
1. Popis IKT prostredia a vynaložené finančné prostriedky.
2. Ochrana osobných údajov a bezpečnosť informačných systémov verejnej správy.
3. Prevádzka informačných systémov verejnej správy.
4. Dodržiavanie všeobecne záväzných právnych predpisov pre oblasť informačných systémov verejnej správy.

2 RÁMEC KONTROLNEJ AKCIE

Kontrolná akcia bola vykonaná v súlade so zákonom o NKÚ SR a so štandardmi, ktoré vychádzajú zo základných princípov ISSAI. Kontrola bola vykonaná v piatich kontrolovaných subjektoch – Mesto Piešťany, Mesto Hlohovec, Mesto Galanta, Mesto Sládkovičovo a Mesto Holíč, a to za kontrolované obdobie rokov 2015 a 2016. V prípade potreby bola kontrolovaná oblasť (podľa predmetu kontroly) zdokumentovaná aj za predchádzajúce obdobie. Pri kontrole boli použité kontrolórske postupy a techniky pre kontrolu súladu a kontrolu informačných systémov, najmä štúdium vnútorných predpisov, kontrola dokladov a dokumentov, nastavenie informačných systémov, rozhovory s manažmentom a zamestnancami kontrolovaného subjektu.

Kontrola preverila správu aktív IKT, správu majetku IKT, vlastníctvo údajov a aplikácie na kontrolovaných subjektoch. V subjektoch bola kontrolovaná inventarizácia majetku, záväzkov, rozdielu majetku a záväzkov, aj súlad so zákonom o účtovníctve. V podkladoch inventarizácie majetku kontrolovaného subjektu sa kontrolná skupina zamerala len na majetok súvisiaci s IKT. V rámci kontroly preverenia ochrany osobných údajov a bezpečnosti ISVS bola vykonaná kontrola podmienok logiky prístupu do informačných systémov, politiky hesiel, správy oprávnení, prístupu tretích strán do informačného systému a fyzická bezpečnosť IKT. Ďalšou oblasťou preverenia prevádzky ISVS bola kontrola nepretržitej prevádzky a obnovy informačných systémov, aj kontrola zálohovania a obnova údajov a programového vybavenia. Do predmetu kontroly patrilo aj preverenie dodržiavania všeobecne záväzných právnych predpisov pre oblasť ISVS; v tejto súvislosti bola kontrola zameraná najmä na preverenie vybraných ustanovení zákona o ISVS, výnosu MF SR o štandardoch pre ISVS, zákona o ochrane osobných údajov a zákona o e-Governmente.

3 ZISTENIA

3.1 POPIS IKT PROSTREDIA A VYNALOŽENÉ FINANČNÉ PROSTRIEDKY

Na základe získaných poznatkov z vykonaných kontrol ISVS dochádza k porušeniam najmä v oblasti ochrany osobných údajov a zabezpečenia technických opatrení na zamedzenie prístupu tretích strán k údajom v ISVS. Ako pilotná kontrolná akcia zameraná na zabezpečenie ochrany osobných údajov v informačným systémoch vybraných miest boli stanovené pre výber vzorky kontrolovaných subjektov kritéria: vzorka piatich miest z jedného kraja s počtom obyvateľov v rozsahu od 5 000 do 28 000 a kontrolované subjekty, ktoré v MetaIS nesprístupňovali informácie o prevádzkovaných ISVS. Na základe uvedených kritérií bola kontrola vykonaná na piatich subjektoch (Mesto Piešťany, Mesto Hlohovec, Mesto Galanta, Mesto Sládkovičovo, Mesto Holíč) v Trnavskom kraji. Kontrolované subjekty sú samostatné územné samosprávne a správne celky Slovenskej republiky, združujúce občanov, ktorí majú na ich území trvalý pobyt. Podľa počtu obyvateľov k 31. decembru 2015 mali tieto mestá od 5 000 do 28 000 obyvateľov. Všetky kontrolované subjekty sú právnickými osobami, ktoré za podmienok ustanovených zákonom o obecnom zriadení samostatne hospodária s vlastným majetkom. Na všetkých kontrolovaných subjektoch bola vykonaná inventarizácia majetku, záväzkov, rozdielu majetku a záväzkov k 31. decembru 2015 v zmysle ustanovení zákona o účtovníctve. Na základe výsledku inventarizácie kontrolovaných subjektov, porovnaním skutočného s účtovným stavom, nebol zistený rozdiel.

Obstarávacia cena IKT majetku k 31. decembru 2015, v porovnaní s celkovým majetkom jednotlivých kontrolovaných subjektov, sa pohybovala v rozmedzí od 0,51 % do 1,16 %. Pomer sumy došlých faktúr za IKT majetok v porovnaní so sumou za všetky došlé faktúry v kontrolovanom období od 1. januára 2015 do 30. septembra 2016, sa pohyboval v kontrolovaných subjektoch v rozmedzí od 1,72 % do 3,87 %. Kontrolou IKT majetku bolo zistené, že v niektorých subjektoch kontrolovaný IKT majetok nemal na inventúrnych súpisoch uvedené mená

zodpovedných zamestnancov (Mesto Piešťany, Mesto Galanta), resp. ich podpisy (Mesto Hlohovec, Mesto Sládkovičovo), čo nebolo v súlade so zákonom o účtovníctve. V Meste Sládkovičovo bolo zistené, že IKT majetok nebol označený inventárnym číslom, čím nebolo možné jednoznačne identifikovať miesto uloženia tohto majetku. Ďalej bolo v Meste Sládkovičovo zistené, že na inventúrnych súpisoch k 31. decembru 2015 boli ako zodpovedné osoby uvedení zamestnanci, ktorí už na Mestskom úrade nepracovali; tento stav nebol v súlade so zákonom o účtovníctve.

Štyri kontrolované subjekty (Mesto Piešťany, Mesto Hlohovec, Mesto Sládkovičovo, Mesto Holíč) mali v súlade so zákonom o obecnom zriadení prijatý štatút mesta. Kontrolovaný subjekt Mesto Galanta na základe písomného vyjadrenia z 12. októbra 2016 v čase výkonu kontroly nemal v súlade so zákonom o obecnom zriadení vypracovaný a schválený štatút Mesta Galanta.

3.2 OCHRANA OSOBNÝCH ÚDAJOV A BEZPEČNOSŤ INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY

V preverovanej oblasti bola kontrola zameraná na kvalitu a dodržiavanie vypracovaných interných predpisov kontrolovaných subjektov bezpečnostnej dokumentácie (bezpečnostný projekt, bezpečnostná politika, bezpečnostná smernica, atď.), ich účinnosť a povinnosti z nich vyplývajúce.

Kontrolované subjekty mali len formálne zavedený proces identifikácie, autentifikácie a politiku hesiel v predloženej bezpečnostnej dokumentácii; kontrolou bolo zistené, že niektoré kontrolované subjekty (Mesto Piešťany, Mesto Hlohovec, Mesto Sládkovičovo, Mesto Holíč) v informačnom systéme nemali v politike hesiel nastavené všetky parametre hesla v súlade s bezpečnostnou dokumentáciou.

Kontrolované subjekty mali formálne zavedený proces na pridelenie a zrušenie prístupových oprávnení do informačných systémov, avšak kontrolou bolo zistené, že prideľovanie a rušenie oprávnení prostredníctvom definovaného procesu nebolo realizované.

V jednom kontrolovanom subjekte (Mesto Piešťany) bolo zistené, že v privilegovanej skupine používateľských účtov sa nachádzal neblokovaný používateľský účet bývalého zamestnanca s tak nastaveným parametrom hesla, aby nikdy nevypršalo.

V dvoch kontrolovaných subjektoch (Mesto Galanta, Mesto Sládkovičovo) bolo zistené, že pri prihlasovaní do informačného systému nebola zabezpečená jedinečná identifikácia, autentifikácia a autorizácia, čo nebolo v súlade s prijatou bezpečnostnou dokumentáciou, ktorá bola vypracovaná v zmysle zákona o ochrane osobných údajov.

V niektorých kontrolovaných subjektoch (Mesto Sládkovičovo, Mesto Holíč) mali nastavené pracovné stanice používateľov tak, že používateľ mohol vykonať zmenu konfigurácie pracovnej stanice, inštaláciu programov a nelegálneho programového vybavenia, čo nebolo v súlade s prijatou bezpečnostnou dokumentáciou, účinnou v kontrolovanom subjekte.

V niektorých kontrolovaných subjektoch (Mesto Piešťany, Mesto Galanta) mali v používateľských skupinách správcov informačného systému s administrátorskými právami zaradených používateľov, ktorí neboli správcami systému.

V súlade s uvedenými skutočnosťami treba konštatovať, že v kontrolovaných subjektoch nebola dostatočne zabezpečená implementácia príkazov stanovených v bezpečnostnej dokumentácii, ktorá spresňuje a aplikuje bezpečnostné opatrenia v zmysle zákona o ochrane osobných údajov, a nebola dostatočne zabezpečená ani realizácia a dodržiavanie schválenej bezpečnostnej politiky v zmysle výnosu MF SR o štandardoch pre ISVS.

NKÚ SR ďalej zistil, že niektoré kontrolované subjekty (Mesto Piešťany, Mesto Galanta, Mesto Sládkovičovo) mali uzavretú zmluvu o poskytovaní služieb, ktorú im poskytoval dodávateľ služby, kde kontrolovaný subjekt mal povinnosť zabezpečiť potrebný vzdialený prístup do svojej siete na účely riadneho plnenia služieb zo strany poskytovateľa, avšak ani jedna z predmetných zmlúv neobsahovala bezpečnostné požiadavky na tieto služby v súlade s výnosom MF SR o štandardoch pre ISVS.

Ohliadkou priestorov s aktívnymi prvkami sieťovej infraštruktúry, umiestnenie serverov a hlavnej technologickej miestnosti (serverovňa) bolo zistené, že v každom kontrolovanom subjekte sa v priestore serverovne nachádzali horľavé materiály, ktoré by mohli za istých okolností ohroziť bezpečnosť informačného systému, čo nebolo v súlade s výnosom MF SR o štandardoch pre ISVS.

Kontrolované subjekty nemali vypracované pravidlá pre prácu v zabezpečenom priestore.

V dvoch prípadoch kontrolovaných subjektov (Mesto Holíč, Mesto Sládkovičovo) bolo možné konštatovať, že serverovňa nebola dostatočne chránená ani pred fyzickým prístupom nepovolaných osôb, čo nebolo v súlade s výnosom MF SR o štandardoch pre ISVS.

3.3 PREVÁDZKA INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY

V preverovanej oblasti bola kontrola zameraná na preverenie nepretržitej prevádzky a obnovy informačných systémov, na overovanie zálohovania, na obnovu údajov a programov, na oblasť riadenia procesov IT a vnútorného kontrolného systému.

Kontrolované subjekty mali formálne popísané procesy zálohovania a archivácie v predloženej bezpečnostnej dokumentácii. Avšak, Mesto Galanta nemalo protokoly o obnove dát zo zálohy a nevykonávalo test obnovy informačného systému; Mesto Sládkovičovo nemalo vypracované protokoly o obnove dát zo zálohy; Mesto Holíč nemalo vypracovanú stratégiu zálohovania a ani procedúru na zálohovanie a obnovu informačných systémov, a nemalo vypracované ani protokoly o obnove dát zo zálohy. Mesto Hlohovec vykonávalo obnovu dát zo zálohy dodávateľsky, prostredníctvom servisnej zmluvy, a Mesto Piešťany vykonávalo archivačné zálohy v mesačných intervaloch, ale nevykonávalo test komplexnej obnovy informačného systému, len obnovu databáz informačného systému.

3.4 DODRŽIAVANIE VŠEOBECNE ZÁVÄZNÝCH PRÁVNYCH PREDPISOV PRE OBLASŤ INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY.

V preverovanej oblasti bola kontrola zameraná na kontrolu dodržiavania všeobecne záväzných právnych predpisov, a to konkrétne vybraných ustanovení zákona o ISVS, výnosu MF SR o štandardoch pre ISVS, zákona o ochrane osobných údajov a zákona o e-Governmente.

3.4.1 Preverenie vybraných ustanovení zákona o ISVS

V zmysle zákona o ISVS sú kontrolované subjekty povinné osoby, ktoré sú aj správcami ISVS, a teda sú povinné vypracovať KRIS. Jeden kontrolovaný subjekt (Mesto Holíč) predložil KRIS z roku 2016 v súlade so zákonom o ISVS; jeden kontrolovaný subjekt (Mesto Piešťany) predložil KRIS z roku 2013 v súlade so zákonom o ISVS; dva kontrolované subjekty (Mesto Hlohovec, Mesto Galanta) predložili KRIS z roku 2010; jeden kontrolovaný subjekt (Mesto Sládkovičovo) nemal vypracovanú KRIS, čo nebolo v súlade so zákonom o ISVS.

Kontrolované subjekty zabezpečovali technickými a softvérovými prostriedkami (firewall, antivírusová ochrana) ISVS proti zneužitiu.

Preverením MetaIS bolo zistené, že v čase výkonu kontroly sa v MetaIS nenachádzali žiadne elektronické služby poskytované kontrolovanými subjektmi, ani informácie o informačných systémoch prevádzkovaných kontrolovanými subjektmi, čo nebolo v súlade so zákonom o ISVS, keďže kontrolované subjekty, ako povinné osoby, bezodkladne nesprístupňovali informácie o ISVS prostredníctvom MetaIS, ktoré prevádzkujú.

Kontrolou bolo zistené, že vo viacerých prípadoch, uvedených v predchádzajúcich bodoch tejto správy, ISVS kontrolovaných subjektov nebol v súlade s výnosom MF SR o štandardoch pre ISVS, čím kontrolované subjekty postupovali v rozpore so zákonom o ISVS.

3.4.2 Preverenie súladu s vybranými ustanoveniami výnosu MF SR o štandardoch pre ISVS

Okrem porušení výnosu MF SR o štandardoch pre ISVS, uvedených v predchádzajúcich bodoch tejto správy, bolo ďalej zistené, že

– tri kontrolované subjekty (Mesto Sládkovičovo, Mesto Piešťany, Mesto Holíč) nemali vytvorenú e-mailovú adresu v tvare „info“ pred deliacim znakom @, slúžiacu na poskytovanie informácií osobám podľa zákona o slobodnom prístupe k informáciám, čo nebolo v súlade s výnosom MF SR o štandardoch pre ISVS

– pre riadenie informačnej bezpečnosti má byť vypracovaná a schválená bezpečnostná politika v zmysle výnosu o štandardoch pre ISVS. Kontrolovaný subjekt, Mesto Sládkovičovo, nemal vypracovanú a schválenú bezpečnostnú politiku; kontrolovaný subjekt, Mesto Holíč, mal vypracovanú a schválenú bezpečnostnú politiku, avšak manažér informačnej bezpečnosti bol menovaný až v priebehu výkonu kontroly; dva kontrolované subjekty (Mesto Piešťany, Mesto Galanta) predložili Vyhlásenie o zavedení bezpečnostnej politiky; kontrolovaný subjekt, Mesto Hlohovec, mal vypracovanú a schválenú bezpečnostnú politiku ako samostatný formalizovaný dokument.

Kontrolovaný subjekt Mesto Holíč mal v bezpečnostnej politike ustanovené, že na účely zaistenia efektivity ochranných opatrení a adekvátneho zabezpečenia IKT musí byť vykonané nezávislé hodnotenie formou bezpečnostného auditu najmenej každé dva roky alebo pri významných zmenách IKT Mesta Holíč. Ku dňu výkonu

kontroly bezpečnostný audit nebol vykonaný, čo nebolo v súlade s výnosom MF SR o štandardoch pre ISVS. Kontrolovaný subjekt, Mesto Hlohovec, prevádzkoval elektronickú podateľňu a mal v súlade s výnosom MF SR o štandardoch pre ISVS vytvorenú e-mailovú adresu, ktorá mala pred deliacim znakom @ tvar „podatelna".

3.4.3 Preverenie vybraných ustanovení zákona o ochrane osobných údajov

V preverovanej oblasti bola kontrola zameraná aj na preverenie súladu s vybranými ustanoveniami zákona o ochrane osobných údajov, na kontrolu bezpečnostnej dokumentácie (bezpečnostný projekt, bezpečnostná smernica, atď.) a povinnosti z toho vyplývajúce. V zmysle zákona o ochrane osobných údajov je prevádzkovateľ povinný viesť evidenciu o informačných systémoch, v ktorých spracúva osobné údaje, ktoré nepodliehajú oznamovacej povinnosti alebo osobitnej registrácii.

Všetky kontrolované subjekty predložili bezpečnostný projekt, avšak kontrolou bolo zistené, že kontrolovaný subjekt, Mesto Holíč, nepostupoval v súlade so zákonom o ochrane osobných údajov, keďže nezabezpečil súlad informačného systému Mesta Holíč do 9 mesiacov od účinnosti zákona o ochrane osobných údajov; kontrolnej skupine neboli predložené ani evidenčné listy ku všetkým informačným systémom identifikovaných bezpečnostným projektom ako informačné systémy, v ktorých sú spracúvané osobné údaje. Ďalej kontrolovaný subjekt, Mesto Holíč, mal vypracovanú smernicu na dodržiavanie zákonných ustanovení v zmysle zákona o ochrane osobných údajov – o bezpečnom používaní kamerového systému, avšak evidenčný list kamerového systému kontrolnej skupine nebol predložený, čo nebolo v súlade so zákonom o ochrane osobných údajov. Taktiež kontrolnej skupine neboli predložené záznamy o poučení oprávnených osôb na používanie a nakladanie s kamerovým systémom. Ďalej kontrolovaný subjekt, Mesto Holíč, nepostupoval v súlade so zákonom o ochrane osobných údajov, pretože predložené poučenia oprávnených osôb neobsahovali všetky náležitosti poučenia oprávnenej osoby v súlade so zákonom o ochrane osobných údajov.

Kontrolovaný subjekt, Mesto Sládkovičovo, nepredložil evidenčné listy ku všetkým informačným systémom identifikovaných v bezpečnostnom projekte ako informačné systémy, v ktorých sú spracúvané osobné údaje, čo nebolo v súlade so zákonom o ochrane osobných údajov. Kontrolou bolo zistené, že kontrolovaný subjekt, Mesto Sládkovičovo, nemal vypracovaný evidenčný list k informačnému systému, v ktorom sú spracúvané osobné údaje, ktorého právnym základom spracúvania osobných údajov je zákon o niektorých súvislostiach s oznamovaním protispoločenskej činnosti. Niektoré evidenčné listy kontrolovaného subjektu, Mesto Sládkovičovo, mali formálne nedostatky; napr. v evidenčných listoch chýbal zoznam osobných údajov, právny základ spracúvania osobných údajov a okruh dotknutých osôb, čo nebolo v súlade so zákonom o ochrane osobných údajov. Predložené záznamy o poučení oprávnených osôb neobsahovali všetky náležitosti poučenia v zmysle zákona o ochrane osobných údajov.

Kontrolovaný subjekt, Mesto Galanta, predložil bezpečnostný projekt schválený dňa 27. novembra 2014, analýzu bezpečnosti I, II a návrhy opatrení z 21. novembra 2014. Kontrolnej skupine bola predložená bezpečnostná smernica Mesta Galanta, ktorá nadobudla platnosť a účinnosť od 3. novembra 2014, čo znamená – ešte pred dňom schválenia bezpečnostného projektu a pred vykonaním analýzy a návrhmi opatrení. V zmysle vyhlášky o rozsahu a dokumentácii bezpečnostných opatrení má bezpečnostná smernica obsahovať závery vyplývajúce z bezpečnostného zámeru a analýzy bezpečnosti informačného systému na konkrétne podmienky prevádzkovaného informačného systému. Predložené evidenčné listy informačných systémov, v ktorých sú spracúvané osobné údaje kontrolovaného subjektu, Mesto Galanta, neboli síce vypracované v zmysle vzoru evidencie zverejneného Úradom na ochranu osobných údajov SR, ktoré zverejnil na svojom webovom sídle v zmysle zákona o ochrane osobných údajov, ale spĺňali náležitosti v rozsahu zákona o ochrane osobných údajov, pričom sa v evidenčných listoch vyskytli len formálne nedostatky. V jednom prípade na vybranej vzorke predložených evidenčných listov bol zistený nesúlad názvu informačného systému uvedeného v bezpečnostnom projekte s názvom uvedeným na evidenčnom liste, ku ktorému sa viazal. Na vybranej vzorke poučení oprávnených osôb boli formálne nedostatky.

Pri dvoch subjektoch (Mesto Hlohovec, Mesto Piešťany), na základe kontroly náhodne vybranej vzorky z predložených evidenčných listov informačných systémov, v ktorých boli spracúvané osobné údaje, kontrolná skupina konštatovala, že kontrolované subjekty (Mesto Hlohovec, Mesto Piešťany) viedli evidenciu informačných systémoch, v ktorých spracúvali osobné údaje, v súlade so zákonom o ochrane osobných údajov. Ďalej kontrolná skupina na základe kontroly náhodne vybranej vzorky z predložených záznamov o poučení oprávnených osôb konštatovala, že záznamy o poučení oprávnených osôb dvoch kontrolovaných subjektov (Mesto Hlohovec, Mesto Piešťany) boli v súlade so zákonom o ochrane osobných údajov.

V zmysle zákona o ochrane osobných údajov prevádzkovateľ, ktorý spracúva osobné údaje prostredníctvom oprávnených osôb, môže výkonom dohľadu písomne poveriť zodpovednú osobu alebo viaceré zodpovedné osoby, ktoré dozerajú na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov. Dva kontrolované subjekty (Mesto Sládkovičovo, Mesto Galanta) nemali poverené zodpovedné osoby. Tri kontrolované subjekty (Mesto Piešťany, Mesto Hlohovec, Mesto Holíč) mali poverené zodpovedné osoby výkonom dohľadu nad ochranou osobných údajov v zmysle zákona o ochrane osobných údajov, ktoré spĺňali podmienky na výkon funkcie zodpovednej osoby v súlade so zákonom o ochrane osobných údajov.

3.4.4 Preverenie vybraných ustanovení zákona o e-Governmente

V zmysle zákona o e-Governmente boli orgány verejnej moci povinné od 1. augusta 2016 komunikovať s právnickými osobami prostredníctvom využitia elektronických schránok. Od 1. novembra 2016 mal mať každý orgán verejnej moci zákonnú povinnosť uplatňovať výkon verejnej moci elektronicky, t. j. povinne komunikovať prostredníctvom elektronických schránok. Počas výkonu kontroly bolo zistené, že všetky kontrolované subjekty mali zriadený prístup a disponovali elektronickou schránkou verejnej moci.

Kontrolovaný subjekt, Mesto Holíč, mal v zmysle schválenej KRIS zriadený portál elektronických služieb (portál eGov). Na základe písomného vyjadrenia kontrolovaného subjektu občania Mesta Holíč nevyužívali do 7. novembra 2016 žiadne elektronické služby poskytované Mestom Holíč, zároveň žiaden občan Mesta Holíč nemal zriadený prístup do privátnej časti na portáli eGov.

Kontrolovaný subjekt, Mesto Sládkovičovo, podpísalo zmluvu o pripojení k informačnému systému DCOM. Informačný systém DCOM sprístupní poskytovanie elektronických služieb občanom na úrovni regionálnej a miestnej samosprávy. V čase výkonu kontroly Mesto Sládkovičovo prostredníctvom svojej webovej stránky poskytovalo celkom 37 elektronických služieb (informatívny charakter) a 15 tlačív na podania.

Kontrolovaný subjekt, Mesto Hlohovec, plánuje poskytovať elektronické služby občanom prostredníctvom portálu elektronických služieb (eGov). Na základe písomného vyjadrenia kontrolovaného subjektu, Mesto Hlohovec, občania Mesta Hlohovec do 29. novembra 2016 nevyužívali žiadne elektronické služby poskytované Mestom Hlohovec.

Kontrolovaný subjekt, Mesto Galanta, na základe písomného vyjadrenia z 30. novembra 2016, plánuje využívať len základné elektronické služby prostredníctvom informačného systému DCOM, ktoré vyplývajú z platnej legislatívy a ktoré sú v súčasnej ponuke DCOM.

Na základe vyjadrenia kontrolovaného subjektu, Mesto Piešťany, bola k 30. novembru 2016 v podpisovom konaní medzi Mestom Piešťany a DataCentrom elektronizácie územnej samosprávy Slovenska zmluva na zavedenie poskytovania elektronických služieb občanom a podnikateľom mesta.

4 REAKCIE KONTROLOVANÝCH SUBJEKTOV

Ku kontrolným zisteniam, uvedeným v protokoloch o výsledku kontroly, neboli zo strany kontrolovaných subjektov – Mesto Piešťany, Mesto Hlohovec, Mesto Galanta a Mesto Sládkovičovo, vznesené námietky proti ich pravdivosti, úplnosti a preukázateľnosti. Kontrolovaný subjekt, Mesto Holíč, vzniesol jednu námietku, ktorá bola kontrolnou skupinou preverená, no výsledok preverenia námietky nepotvrdil jej opodstatnenosť; oznámenie výsledku preverenia námietky bolo zaslané kontrolovanému subjektu, Mesto Holíč.

Protokoly o výsledku kontroly boli prerokované s písomne poverenými zamestnancami kontrolovaných subjektov. Kontrolované subjekty prijali spolu 84 opatrení na odstránenie kontrolou zistených nedostatkov.

Plnenie prijatých opatrení NKÚ SR vyhodnotí po predložení správ o splnení, resp. bude monitorovať plnenie opatrení. V odôvodnených prípadoch bude plnenie preverené samostatnou kontrolou k plneniu opatrení, prípadne v rámci inej kontroly/iných kontrol, ktorú/é NKÚ SR vykoná v príslušnom kontrolovanom subjekte.

ZÁVER

Kontrolou boli naplnené ciele kontroly. Kontrolná skupina preverila správu aktív IKT a správu majetku IKT, prevádzku a bezpečnosť informačných systémov verejnej správy, preverila aj dodržiavanie všeobecne záväzných právnych predpisov v oblasti informačných systémov verejnej správy a ochrany osobných údajov. Kontrola poukázala najmä na nedostatočnú implementáciu bezpečnostných opatrení a nedostatočné aplikovanie formalizovaných zásad, uvedených v bezpečnostnej dokumentácii (bezpečnostný projekt, bezpečnostná smernica, bezpečnostná politika). Kontrolou bol zistený nesúlad informačných systémov s výnosom MF SR o štandardoch pre ISVS, zákonom o ISVS a zákonom o ochrane osobných údajov. Výsledky kontroly boli prerokované s písomne poverenými zamestnancami kontrolovaných subjektov. V zmysle zápisnice o prerokovaní protokolu sa kontrolované subjekty zaviazali prijať do stanoveného termínu opatrenia a do stanoveného následného termínu zaslať správu o splnení, resp. plnení opatrení. Kontrolované subjekty prijali spolu 84 opatrení na odstránenie kontrolou zistených nedostatkov. NKÚ SR požiadal kontrolované subjekty, aby na v časovom slede najbližších zasadaniach mestských zastupiteľstiev informovali o výsledku kontroly a o prijatých opatreniach Mestské zastupiteľstvá kontrolovaných subjektov.

KONTAKT

Najvyšší kontrolný úrad Slovenskej republiky
Priemyselná 2
824 73 Bratislava

e-mail: info@nku.gov.sk
web: www.nku.gov.sk
telefón: 02/501 14 911 – podateľňa