NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo: Z-007064/2019/1130/PIA
Číslo poverenia: 1737/24
Zo dňa: 04.07.2019

Počet výtlačkov: 2
Výtlačok číslo: 2
Počet strán: 12
Počet príloh: -

P R O T O K O L
o výsledku kontroly
systému ochrany a bezpečnosti údajov vo verejnom sektore
KA 015/2019

Mesto Leopoldov

Trnava, október 2019

Obsah

Zoznam použitých skratiek

Skrátený názov	Úplné znenie
GDPR	General Data Protection Regulation
IS	informačný systém mesta
IT	Informačné technológie
DCOM	Dátové centrum obcí a miest
nariadenie GDPR nariadenie (EÚ)	Nariadenie európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všemestoné nariadenie o ochrane údajov)
NKÚ SR	Najvyšší kontrolný úrad Slovenskej republiky
OÚ	osobné údaje
SLA	Service Level Agreement
ÚOOÚ SR	Úrad na ochranu osobných údajov Slovenskej republiky
výnos č. 55/2014 Z. z.	výnos Ministerstva Slovenskej republiky o štandardoch pre informačné systémy verejnej správy
zákon č. 18/2018 Z. z.	zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
zákon č. 122/2013 Z. z.	zákon o ochrane osobných údajov a o zmene a doplnení niektorých údajov
zákon č. 395/2002 Z. z.	zákon o archívoch a registratúrach a o doplnení niektorých zákonov
ZO	zodpovedná osoba

Zhrnutie

Dňa 25.01.2012 EK v rámci EÚ predstavila nový právny rámec ochrany osobných údajov, ktorý bol v rokoch 2012 - 2016 pripomienkovaný členskými štátmi EÚ. Finálne znenie Nariadenia (EÚ) nadobudlo platnosť 25.05.2016. Od tohto momentu začalo plynúť dvojročné prechodné obdobie, počas ktorého boli povinné všetky subjekty verejného aj súkromného sektora spracúvajúce osobné údaje v IS (prevádzkovatelia) pripraviť sa na jeho uplatňovanie v plnom rozsahu od 25.05.2018.

Nariadenie (EÚ) má charakter európskeho zákona, ktoré je priamo účinné, vykonateľné a uplatniteľné na území každého členského štátu EÚ bez nutnosti prijatia vnútroštátnych vykonávacích predpisov. Nariadenie dáva členským štátom priestor upraviť len niektoré jeho články v zmysle národných špecifík. Dňom 25.05.2018 teda došlo nielen k zrušeniu dovtedy platnej Smernice 95/46/ES, ale aj k zrušeniu zákona 122/2013, ktorý s účinnosťou od 25.05.2018 nahradil nový zákon 18/2018 a doplnil Nariadenie (EÚ) na národnej úrovni.

V súvislosti s plnením nových povinností zavedených v Nariadení (EÚ) boli prevádzkovatelia nútení viaceré zabehnuté mechanizmy ochrany osobných údajov modifikovať a zaviesť ďalšie opatrenia na zosúladenie spracúvania v IS s Nariadením (EÚ). Do 25.05.2018 bol každý prevádzkovateľ povinný v súlade s či, 24 ods. 1 a 2 Nariadenia (EÚ) prijať vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie vykonáva v súlade s Nariadením (EÚ). Na tento účel bol povinný prijať primerané politiky (smernice) na zabezpečenie ochrany osobných údajov.

NKÚ SR vykonal v meste Leopoldov kontrolu systému ochrany a bezpečnosti údajov vo verejnom sektore, ktorej účelom bolo zistiť objem finančných prostriedkov, ktoré boli alokované na zabezpečenie ochrany údajov; prispieť k správnej implementácii potrebných technických, organizačných a personálnych opatrení vyplývajúcich prevádzkovateľom z nariadenia.

Predmetom kontroly bola harmonizácia vnútroštátneho práva ochrany osobných údajov s Nariadením EÚ 2016/679. Kontrola finančných prostriedkov vyčlenených na implementáciu povinností a opatrení podľa nariadenia a zabezpečenie osobných údajov občanov v databázach a informačných systémoch.

Kontrola bola vykonaná ako kontrola súladu (s prvkami výkonnosti).

Kontrolou bolo zistené, že mesto uhrádzalo výdavky na ochranu OÚ výlučne z vlastných zdrojov. Oblasť ochrany OÚ nebolo dostatočne finančne zabezpečená.

Mesto nemalo vypracovaný dokument podľa štandardu pre aktualizáciu IKT podľa § 42 výnosu MFSR 55/2014 Z. z ani postupy schvaľovacieho procesu pre zmeny existujúcich a zavedenie nových informačných systémom ISVS a IKT, ktorý zahŕňal bezpečnostné požiadavky podľa § 42 výnosu 55/2014 Z. z.

Podľa poverenia predsedu NKÚ SR č. **1737/24** z 04.07.2019 vykonali:

JUDr. Igor Puobiš, vedúci kontrolnej skupiny
Mgr. Zuzana Luhová, členka kontrolnej skupiny

kontrolu systému ochrany a bezpečnosti údajov vo verejnom sektore, ktorej účelom bolo zistiť objem finančných prostriedkov, ktoré boli alokované na zabezpečenie ochrany údajov; prispieť k správnej implementácii potrebných technických, organizačných a personálnych opatrení vyplývajúcich prevádzkovateľom z nariadenia. Poukázať na možné formálne plnenie povinností v predmetnej politike a vypracovali protokol o výsledku kontroly.

Kontrola bola vykonaná v čase od 25.07.2019 do 13.09.2019 v kontrolovanom subjekte

Mesto Leopoldov, Hlohovská cesta 104/2, 920 41 Leopoldov, IČO 00312703

za kontrolované obdobie rokov 2016 - 2019.

Kontrola bola vykonaná v súlade so zákonom NR SR č. 39/1993 Z. z. o Najvyššom kontrolnom úrade Slovenskej republiky v znení neskorších predpisov a so štandardami, ktoré vychádzajú zo základných princípov medzinárodných štandardov najvyšších kontrolných inštitúcií (ISSAI).

Predmetom kontroly bola harmonizácia vnútroštátneho práva ochrany osobných údajov s Nariadením EÚ 2016/679. Kontrola finančných prostriedkov vyčlenených na implementáciu povinností a opatrení podľa nariadenia a zabezpečenie osobných údajov občanov v databázach a informačných systémoch.

Počas výkonu kontroly bolo zistené:

1. Harmonizácia vnútroštátneho práva ochrany osobných údajov s Nariadením EÚ 2016/679

1.1 Úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR pre prevádzkovateľov

Účelom bolo preveriť, či legislatíva súvisiaca s ochranou osobných údajov a usmernia ÚOOÚ SR boli pre prevádzkovateľa (mesto) primerane zrozumiteľné.

Kontrolou bolo zistené, že mesto Leopoldov využívala webové sídlo ÚOOÚ SR. Zverejnené informácie resp. metodiky považovala ZO za čiastočne zrozumiteľné.

Kontrolovaný subjekt uzatvoril zmluvu o výkone činnosti zodpovednej osoby s obchodnou spoločnosťou Fair Mind s.r.o. dňa 03.06.2016, ktorej predmetom bolo poverenie na výkon kompetencií zodpovednej osoby. Počas výkonu kontroly prišlo k ukončeniu zmluvného vzťahu so spoločnosťou Fair Mind s.r.o. z dôvodu úmrtia zodpovednej osoby (konateľa spoločnosti). Mesto uzatvorilo dňa 27.09.2019 zmluvu o zabezpečení výkonu činnosti zodpovednej osoby pri ochrane osobných údajov dotknutých osôb spracovávaných u prevádzkovateľa so spoločnosťou osobnyudaj.sk, s.r.o.

Mesto v prípade akýchkoľvek problémov v oblasti ochrany OÚ využívala služby externých subjektov (právnik, informatik, zodpovedná osoba). Personálne kapacity mesta je možné považovať za nedostatočné, a to najmä z dôvodu jej obmedzených rozpočtových možností. Mesto deklarovalo, že do času výkonu kontroly ÚOOÚ SR nevykonal v meste žiadnu kontrolu.

Záver k bodu 1

Mesto Leopoldov využívalo webové sídlo ÚOOÚ SR. Zverejnené informácie resp. metodiky považovala ZO za čiastočne zrozumiteľné. Personálne kapacity mesta je možné považovať za nedostatočné, a to najmä z dôvodu jej obmedzených rozpočtových možností.

2. Zabezpečenie osobných údajov občanov v databázach a informačných systémoch

Úroveň prijatých opatrení na zabezpečenie súladu s GDPR

2.1 Interné akty riadenia organizácie

V oblasti interných aktov riadenia organizácie sa NKÚ SR zameral na základné interné riadiace akty mesta (organizačný, pracovný, registratúrny poriadok, zverejňovanie, bezpečnosť a ochrana zdravia pri práci) v súvislosti s nakladaním s OÚ.

Mesto malo vypracovaný registratúrny poriadok, ktorý bol v súlade so zákonom č. 395/2002 Z. z. o archívoch a registratúrach v znení neskorších predpisov.

Kontrolou bolo zistené, že zodpovední zamestnanci v prípade spracúvania majetkových priznaní postupovali tak, že neboli zakladané do osobných spisov zamestnancov.

Kontrolou danej oblasti neboli zistené nedostatky.

2.2 Analýza procesov a povinností vyžadovaných podľa GDPR

Mesto preskúmalo nové povinnosti, ktoré prinášalo nariadenie GDPR oproti zákonu č. 122/2013 Z. z. do 25.05.2018 identifikujúce rozdiely medzi skutočným a požadovaným stavom v oblasti ochrany osobných údajov. Predmetom bolo porovnávanie skutočného stavu so stavom referenčným za účelom identifikácie procesov, IS obsahujúcich osobné údaje, bezpečnostných opatrení a zhody s legislatívou (legislatívne požiadavky EÚ, Slovenskej republiky a technické štandardy týkajúce sa ochrany súkromia a informačnej bezpečnosti.

Kontrolovaný subjekt preskúmal všetky IS, v ktorých spracúval osobné údaje, určil druh spracovateľských činností, ktoré môžu viesť k vysokému riziku pre práva a slobody fyzických osôb a vykonal posúdenie vplyvu na ochranu OÚ.

Mesto preskúmalo zmluvy so sprostredkovateľmi a preverovalo, či sprostredkovateľ spĺňal všetky podmienky aj podľa nariadenia GDPR.

2.3 Právny základ – pravidlá a postupy

Mesto spracúvalo osobné údaje na základe zásady zákonnosti. Tá bola v meste determinovaná najmä z jej pozície ako orgánu verejnej moci, z plnenia zmluvných alebo predzmluvných vzťahov, resp. z plnenia zákonných povinností mesta. V týchto prípadoch nebol vyžadovaný súhlas dotknutej osoby.

Mesto preukázalo že vo vybraných prípadoch spracúvalo OÚ na základe súhlasu dotknutej osoby. Súhlas bol vždy udelený na konkrétny účel a rozsah spracúvania. Dotknutá osoba bola informovaná, že udelený súhlas môže kedykoľvek odvolať a to transparentným spôsobom.

V kontrolovanom období mesto vyhlásilo výberové konanie na voľné pracovné miesto. V oblasti nakladania OÚ pri výberových konania nebolo zistené porušenie.

Interné pravidlá špecifikovali postupy, podľa ktorých oprávnené osoby prevádzkovateľa postupovali pri posudzovaní, či je spracúvanie získaných osobných údajov možné na iný účel, ako na účel, na ktorý boli pôvodne získané. V kontrolovanom subjekte boli zavedené postupy, podľa ktorých oprávnené osoby postupovali pri spracúvaní osobitných kategórií osobných údajov.

Počas kontrolovaného obdobia, na základe preverenia dokladov ani vyjadrenia mesta, mesto nepotrebovala vyžadovať písomný súhlas na spracovanie OÚ fyzickej osoby. OÚ kontrolovaný subjekt spracovával na základe zákonných povinností, ktoré mu vyplývali z príslušných všeobecne záväzných právnych noriem.

Mesto malo vypracované pravidlá, podľa ktorých oprávnené osoby rozhodovali o tom, či prenos OÚ do tretích krajín alebo medzinárodným organizáciám bol možný a pri prenosoch vyžadujúcich primerané záruky, čo bolo v súlade s čl. 6 ods. 1 písm. a) GDPR a čl. 46 GDPR, v ktorom sú určené pravidlá pre zákonnosť spracúvania OÚ a primerané záruky pre prenos údajov do tretích krajín.

2.4 Práva dotknutej osoby – pravidlá, postupy a oznámenia

V kontrolovanom období malo mesto vypracované pravidlá, podľa ktorých oprávnené osoby prevádzkovateľa postupovali pri operáciách súvisiacich s OÚ. Platná a účinná bola interná norma č. 29/2015 mesta - Ochrana osobných údajov účinná od 08.07.2015. Dokument pozostával z troch častí:

a) I. časť Organizácia ochrany osobných údajov,
b) II. časť Kompetencie oprávnených osôb,
c) III. časť Popis bezpečnostných opatrení.

Rozsah údajov, ktoré mesto poskytovalo dotknutej osobe, ako aj postup dotknutej osoby v súvislosti so získaním tých údajov bol zverejnený na webovom sídle mesta.

2.5 Základné pravidlá a pokyny pre bezpečné spracúvanie údajov

Oprávnené osoby mesta boli preukázateľne poučené o povinnostiach, vyplývajúcich z ochrany OÚ. NKÚ SR boli predložené záznamy o poučení oprávnených osôb. Poučenie oprávnenej osoby bolo vykonávané pred vykonaním prvej operácie s OÚ (v zmysle interných smerníc) pri nástupe do zamestnania. Mesto malo zadefinované pravidlá pre prideľovanie prístupov do IS a určenie rozsahu spracovateľských operácií, ale neviedla formalizovanú dokumentáciu o týchto prístupoch a rozsahoch.

V prípade ukončenia pracovného pomeru bol zamestnanec povinný vrátiť pridelené úložné médiá a boli mu bezodkladne odobraté prístupové práva do IS. Pracovný poriadok mesta definoval procesy v prípade zastupovania zamestnanca. Interné akty riadenia však neurčovali podmienku, že zastupovanie môže vykonávať len osoba s rovnakými, alebo väčšími prístupovými právami. Boli zadefinované procesy pre prípad opätovného poučenia, ale v kontrolovanom období potreba opätovného poučenia oprávnených osôb nenastala. Oprávnené osoby boli zaviazané povinnosťou dodržiavať mlčanlivosť o OÚ, s ktorými prichádzali do styku. Štatutár mesta bol zodpovedný za prideľovanie prístupov do IS a poučenia oprávnených osôb.

Mesto zabezpečovalo prostredníctvom externej zodpovednej osoby preškolenie oprávnených osôb v oblasti ochrany OÚ.

Mesto zabezpečilo upratovacie služby externým zamestnancom. Externý zamestnanec bol poučený v rámci ochrany osobných údajov. Všetci zamestnanci boli preškoľovaní ohľadom ochrany OÚ. Predmetom školenia bola aj informačná bezpečnosť.Základné pravidlá a pokyny pre bezpečné spracúvanie OÚ oprávnenými osobami boli upravené v internej norme Ochrana osobných údajov.

Interné smernice mesta v oblasti ochrany OÚ zaväzovali oprávnené osoby. Smernica ukladala povinnosť oprávnenej osoby vykonávať spracovateľské operácie s OÚ len vo vybraných IS, ku ktorým malo pridelené prístupové práva a to len v rozsahu operácií, ktoré vyplývali z jej pokynu a výlučne spôsobom, ktorý bol nevyhnutný na dosiahnutie účelu spracúvania. Smernica tiež ukladala možnosť kopírovať, resp. skenovať OÚ alebo zaznamenávať úradné dokumenty len v určených prípadoch. Smernica detailne špecifikovala všeobecné povinnosti oprávnených osôb v oblasti ochrany OÚ. Tieto povinnosti boli primerane aplikované aj pre tretie strany, v prípade mesta najmä dodávateľov a outsourcingového servisu. Bezpečnostné incidenty boli oznamované primátorke mesta. Kontrolovaný subjekt viedol evidenciu

bezpečnostných incidentov. Počas kontrolovaného obdobia nenastal v meste bezpečnostný incident. Interná norma obsahovala podmienku obmedzenia používateľa:

- vyvíjať akúkoľvek komerčnú, podnikateľskú alebo inú zárobkovú činnosť prostredníctvom prostriedkov IT organizácie,
- zneužiť nedbanlivosť iného používateľa na to, aby použil PC, IS alebo počítačovú sieť pod jeho (cudzou) identitou alebo získal údaje z PC alebo zo spracúvaných dokumentov (spisov),
- poskytovať informácie o rozmiestnení prostriedkov IT, ich parametroch, IS a ich technickom a organizačnom zabezpečení nepovolaným osobám.

Pri spracúvaní OÚ v listinnej podobe bola uplatňovaná politika „čistého stola" a dodržiavanie interných smerníc zaručovalo, že OÚ budú primerane chránené. Osobitné kategórie OÚ požívali zvýšenú ochranu. Interné normy neukladali povinnosť oprávnenej osobe vyznačiť vytvorenie kópie dokladu obsahujúceho OÚ, ani zákaz ponechávať dokumenty (spisy) odložené v opustenom (resp. uzamknutom) dopravnom prostriedku. Osobitne tiež nebolo riešené oprávnenie poskytnúť alebo sprístupniť OÚ zamestnanca na telefonické (e-mailové, faxové) dožiadanie treťou stranou len vtedy, ak bol preukázateľne udelený písomný súhlas zamestnanca mesta.

V súvislosti s identifikáciou a autentizáciou užívateľa v IS boli zavedené viaceré ochranné mechanizmy. Autentizačné prostriedky boli chránené pred sprístupnením nepovolanej osobe, odcudzením a zneužitím, resp. zdieľaním s inou oprávnenou osobou. Kontrolou bolo zistené, že bola splnená požiadavka na zložitosť hesla určená na aspoň 8 znakov.

Mesto prijalo opatrenia, ktoré boli pre užívateľov záväzné pri práci s pracovnou stanicou a prenosnými zariadeniami. Pri práci bola uplatňovaná politika „čistej obrazovky." Dodávateľ IT zabezpečoval v meste antivírusovú ochranu pracovných staníc a aktualizácie softvérových komponentov. Politika uplatňovania administrátorských, resp. užívateľských práv zamedzovala inštalovaniu nelegálneho, resp. organizáciou a dodávateľom neschváleného softvéru. Kľúčová politika, resp. politika fyzického zabezpečenia pracovného priestoru eliminovala riziká spojené s neoprávneným prístupom k hardvéru.

Detailne boli riešené aj povinnosti súvisiace s prácou s mobilnými prostriedkami, najmä ich ochranou pred stratou, poškodením a neoprávneným prístupom.

Mesto nemonitorovalo zamestnancov v súvislosti s používaním siete Internet, resp. s používaním elektronickej pošty, ale boli určené v internej norme pravidlá ich použitia. Zariadenia a siete však mohli zamestnanci použiť výlučne iba pre pracovné účely. OÚ resp. súbory, ktoré ich obsahovali a ktoré by zodpovedná osoba zasielala prostredníctvom externých sietí (email a internet), museli byť šifrované. Kontrolovaný subjekt zabezpečil antivírusovú ochranu IT prostriedkov.

Mesto bolo prevádzkovateľom kamerového systému. Ten v rámci svojich kompetencií na ochranu verejného poriadku mesto zaviedlo v roku 2009. Predmetom monitoringu boli zverejnené priestranstvá v meste, pričom sa vykonával záznam v trvaní 15 dní. Prevádzku kamerového systému zabezpečovala mesto. Monitorovaný priestor bol označený na vstupoch do mesta informačnými tabuľkami. Pri inštalácii kamerového systému bol vykonaný balančný test

2.6 Bezpečnostné smernice a dokumentácia

Kontrolou bolo zistené, že postupy a opatrenia pre oprávnené osoby boli v oblasti nahlasovania porušenie ochrany OÚ dozornému orgánu a dotknutej osobe boli uvedené v dokumente – Informácia pre dotknuté osoby. Za oznamovanie porušenia ochrany OÚ dozornému orgánu, dotknutým osobám a vedenie dokumentácie zodpovedala zodpovedná osoba.

Mesto analyzovalo dopady spracúvania osobných údajov pre práva a slobody fyzických osôb a vykonalo posúdenie vplyvu na ochranu údajov.

Pseudonymizácia údajov nebola v žiadnom IS mesta zavedená. Šifrovanie OÚ a dát bolo zabezpečené. Zálohovanie dát bolo zabezpečené dodávateľmi IS.

Mesto malo vypracované záznamy o spracovateľských činnostiach v rozsahu čl. 30 ods. 1 nariadenia GDPR. Lehoty uchovávania údajov v jednotlivých IS boli upravené v registratúrnom poriadku. V prípade uchovávania údajov bolo po formálnej stránke internou smernicou zadefinované, že sa uplatňuje „zásada minimalizácie ich uchovávania."

2.7 Informačná bezpečnosť – bezpečnostné štandardy

Štandardom pre riadenie informačnej bezpečnosti mesta bolo podľa § 29 písm. a) výnosu č. 55/2014 Z. z. vypracovanie bezpečnostnej politiky. Bezpečnostná politika musela byť zadefinovaná aspoň v rozsahu určenom výnosom č. 55/2014 Z. z., schválená vedením mesta a daná na vedomie všetkým zamestnancom ako aj zainteresovaným stranám. V kontrolovanom období bol platná interná norma Ochrana osobných údajov. Bezpečnostnú politiku zahŕňa tretia časť tejto normy vo vzťahu k zákonu 18/2018 Z. z. a viaceré smernice, resp. dokumenty v oblasti informačnej bezpečnosti - Bezpečnostný projekt a ďalšie interné akty riadenia.

Obsahom bezpečnostnej politiky bol aj dokument podľa štandardu pre personálnu bezpečnosť. Kontrolou bolo zistené, že mesto zabezpečovalo poučenie o schválenej bezpečnostnej politike povinnej osoby a o povinnostiach z nej vyplývajúcich pre tretie osoby podľa ustanovenia § 30 písm. a) výnosu č. 55/2014 Z. z. V kontrolovanom období zamestnanci tretích strán fyzicky pristupovali k informačným aktívam mesta v rozsahu sprostredkovateľských zmlúv a primeraného poučenia.

Porušenie bezpečnostnej politiky mesta bolo klasifikované ako závažné porušenie pracovnej disciplíny a oprávnené osoby mali povinnosť ohlasovať bezpečnostné incidenty primátorke.

Mesto malo zadefinované kontrolné mechanizmy v riadení informačnej bezpečnosti.

Kontrolovaný subjekt zabezpečoval v rámci SLA ochranu proti škodlivému kódu vrátane jeho detekcie počas prístupu k externým sieťam a elektronickej pošte. Politika administrátorských práv zabezpečovala, že zamestnanci pri práci používali legálny softvér. Aktualizácia softvéru, vrátane bezpečnostného softvéru bolo zabezpečené dodávateľsky.

Mesto malo zadefinovanú ochranu dát pomocou šifrovania. Ochrana voči prístupu z vonkajšieho prostredia do IS a ochranu vnútorného prostredia mesto zabezpečila (v spolupráci s dodávateľom IS) formou hardvérových a softvérových firewallov.

Interné smernice a Bezpečnostný projekt bližšie špecifikovali postupy fyzickej bezpečnosti a bezpečnosti prostredia podľa ustanovenia § 35 výnosu č. 55/2014 Z. z.

Mesto malo vypracované pravidlá pre monitorovanie, ohlasovanie a evidenciu bezpečnostných incidentov. Počas kontrolovaného obdobia však, podľa vyjadrenia mesta, bezpečnostné incidenty nenastali a preto nevznikla potreba ich evidencie.

Kontrolovaný subjekt zaviedol politiku identifikácie a autentifikácie používateľov pri vstupe do IS. Za prideľovanie prístupových práv bol zodpovedný štatutár mesta.

Kontrolné zistenie č. 1

Mesto nemalo vypracovaný dokument podľa štandardu pre aktualizáciu IKT podľa § 42 výnosu MFSR 55/2014 Z. z ani postupy schvaľovacieho procesu pre zmeny existujúcich a zavedenie nových informačných systémom ISVS a IKT, ktorý zahŕňa bezpečnostné požiadavky podľa § 42 výnosu 55/2014 Z. z.

Kontrolovaný subjekt nemal bližšie špecifikované procesy súvisiace s činnosťou tretej strany v IS. Kontrolou obsahových náležitostí vybraných dodávateľských zmlúv bolo zistené, že tieto obsahovali obmedzenie prístupu tretích strán k údajom, ktoré sú aktívami.

2.8 Výkon funkcie zodpovednej osoby

Kontrolovaný subjekt uzatvoril zmluvu o výkone činnosti zodpovednej osoby s obchodnou spoločnosťou Fair Mind s.r.o. dňa 03.06.2016, ktorej predmetom bolo poverenie na výkon kompetencií zodpovednej osoby. Počas výkonu kontroly prišlo k ukončeniu zmluvného vzťahu so spoločnosťou Fair Mind s.r.o. z dôvodu úmrtia zodpovednej osoby (konateľa spoločnosti). Mesto uzatvorilo dňa 27.09.2019 zmluvu o zabezpečení výkonu činnosti zodpovednej osoby pri ochrane osobných údajov dotknutých osôb spracovávaných u prevádzkovateľa so spoločnosťou osobnyudaj.sk, s.r.o.

Mesto deklarovalo, že do 25.5.2018 a ani po 25.05.2018 neboli poskytované finančné prostriedky štátom na činnosť zodpovednej osoby, ani priamo na oblasť ochrany OÚ. Prostriedky poskytované od štátu mali charakter transferov na prenesený výkon štátnej správy bez väzby na ochranu OÚ. Z finančných prostriedkov poskytovaných na prenesený výkon štátnej správy nebolo možné odčleniť výlučne prostriedky na ochranu OÚ. Vzhľadom na charakter transferov mesto nežiadalo prostriedky výlučne na ochranu osobných údajov a túto oblasť financovalao výlučne zo svojho rozpočtu.

Kontrolou bolo zistené, že mesto zverejnilo informácie o zodpovednej osobe.

Úlohou zodpovednej osoby bolo vybavovať celú agendu týkajúcu sa spracúvania OÚ dotknutých osôb a uplatňovania ich práv. Úlohou zodpovednej osoby bolo ďalej monitorovať zavedené pravidlá ochrany OÚ v meste vrátane rozdeľovania povinností osobám oprávneným spracúvať OÚ a posudzovať ich súlad, dávať odporúčania, konzultácie v oblasti OÚ a školenia.

Za výkon práce poberala ZO zmluvne dohodnutú odmenu. Preverením zmluvných podmienok neboli zistené nedostatky.

2.9 Činnosť sprostredkovateľov

Mesto malo vypracované pravidlá, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Kontrolou bolo zistené, že existovala evidencia sprostredkovateľských zmlúv.

Kontrovaný subjekt mal uzatvorené tieto sprostredkovateľské zmluvy so :

a) sprostredkovateľom, právnickou osobou MAPA Slovakia Digital s.r.o., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ za účelom spracovania katastrálneho operátu,
b) sprostredkovateľom, právnickou osobou LEOPARD, s.r.o., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ v rozsahu dojednaným v zmluve. Účelom bola správa bytov vo vlastníctve prevádzkovteľa,
c) sprostredkovateľom, zodpovednou osobou, ktorej predmetom bol dohľad nad ochranou OÚ a o spracúvaní OÚ prostredníctvom sprostredkovateľa,
d) sprostredkovateľom, fyzickou osobou, ktorej účelom bol lektoring bezpečnosti a ochrany zdravia pri práci a výkon pracovnej zdravotnej služby,
e) sprostredkovateľom, právnickou osobou Wolf & Linden s. r. o., ktorej účelom bol poskytovanie právneho servisu,
f) sprostredkovateľom, právnickou osobou Prosman a Pavlovič advokátska kancelária, s.r.o., ktorej účelom bolo poskytovanie právneho servisu,
g) sprostredkovateľom, s obchodnou spoločnosťou TOPSET Solutioun, s. r. o., ktorej účelom bolo spracúvanie OÚ v počítačovom systéme hrobové miesta systémoch,

Záver k bodu 2

Mesto malo vypracované pravidlá, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Kontrolou bolo zistené, že existovala evidencia zmlúv, ktoré boli uzatvorené so sprostredkovateľmi.

Mesto deklarovalo, že do 25.5.2018 a ani po 25.05.2018 neboli poskytované finančné prostriedky štátom na činnosť zodpovednej osoby, ani priamo na oblasť ochrany OÚ. Úlohou zodpovednej osoby bolo vybavovať celú agendu týkajúcu sa spracúvania OÚ dotknutých osôb a uplatňovania ich práv. Za výkon práce poberala ZO zmluvne dohodnutú odmenu.

Mesto nemalo vypracovaný dokument podľa štandardu pre aktualizáciu IKT podľa § 42 výnosu MFSR 55/2014 Z. z ani postupy schvaľovacieho procesu pre zmeny existujúcich a zavedenie nových informačných systémom ISVS a IKT, ktorý zahŕňal bezpečnostné požiadavky podľa § 42 výnosu 55/2014 Z. z.

3 Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia

Mesto ako prevádzkovateľ zabezpečovalo oblasť ochrany OÚ pomocou zodpovednej osoby a vlastnými zamestnancami.

Všetci zamestnanci vrátane štatutára mesta boli v postavení oprávnených osôb. V súvislosti s nariadením GDPR nedošlo k zmene a bola zachovaná kontinuita v personálnom zabezpečení ochrany OÚ.

V rokoch 2016 až 2018 mesto neobstaralo žiadne zariadenia, súvisiace priamo s ochranou OÚ. V roku 2009 mesto obstaralo kamerový systém, ktorý bol postupne rozširovaný. Jeho úlohou bolo monitorovať verejne prístupné miesta. Kontrolovaný subjekt vynaložil celkovo na kamerový systém 66 582,00- eur.

Kontrolovaný subjekt uhradil externe zodpovednej osobe v roku 2016 300,00 eur v roku 2017 900,00eur, v roku 2018 307,50 eur a v roku 2019 225,00 eur. Mesto uhradilo externej zodpovednej osobe spolu 1732,50 eur.

Mesto preukázateľne zabezpečilo aj vzdelávanie oprávnených osôb v oblasti ochranu OÚ aj nariadenia GDPR. Kvantifikácia výdavkov na vzdelávanie výlučne na ochranu OÚ nebolo možná, pretože vzdelávanie bolo poskytnuté zodpovednou osobou v rámci zmluvného vzťahu.

Všetky výdavky súvisiace s ochranou osobných údajov boli realizované iba z vlastných zdrojov mesta. Tie boli rozpočtované na príslušný rozpočtový rok, ale neboli rozpočtované výlučne za oblasť ochrany OÚ. Výdavky na ochranu OÚ boli rozpočtované v rámci rôznych programov v rôznych položkách (služby - plnenie SLA, školenia). Bolo preukázané, že financovanie preneseného výkonu štátnej správy nepokrývalo výdavky súvisiace s ochranou OÚ, resp. poskytnuté transfery boli určené výlučne na financovanie týchto kompetencií.

Záver k bodu 3

Mesto ako prevádzkovateľ zabezpečovalo oblasť ochrany OÚ pomocou zodpovednej osoby a vlastnými zamestnancami. Kontrolovaný subjekt uhradil externe zodpovednej osobe v rokoch roku 2016 uhradil 300,00 eur, v roku 2017 900,00 eur, v roku 2018 307,50 eur a v roku 2019 225,00 eur. Mesto uhradilo externej zodpovednej osobe spolu 1732,50 eur.

Všetky výdavky súvisiace s ochranou osobných údajov boli realizované iba z vlastných zdrojov mesta. Tie boli rozpočtované na príslušný rozpočtový rok, ale neboli rozpočtované výlučne za oblasť ochrany OÚ. Výdavky na ochranu OÚ boli rozpočtované v rámci rôznych programov v rôznych položkách (služby - plnenie SLA, školenia). Bolo preukázané, že financovanie preneseného výkonu štátnej správy nepokrývalo výdavky súvisiace s ochranou OÚ, resp. poskytnuté transfery boli určené výlučne na financovanie týchto kompetencií. Vynakladané financie na danú oblasť nie sú dostatočné.

Za kontrolnú skupinu dňa: 21.10.2019

JUDr. Igor Puobiš .....
vedúci kontrolnej skupiny

Mgr. Zuzana Luhová .....
členka kontrolnej skupiny

S obsahom protokolu o výsledku kontroly bol oboznámený dňa: 28. 10. 2019

Mgr. Terézia Kavuliaková .....
primátorka mesta

NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY 20