

MESTO PIEŠŤANY

Materiál na rokovanie Mestského zastupiteľstva mesta Piešťany dňa 12.12.2019

**Názov materiálu: PREROKOVANIE PROTOKOLU O VÝSLEDKU KONTROLY NKÚ
SYSTÉMU OCHRANY A BEZPEČNOSTI ÚDAJOV VO VEREJNOM
SEKTORE**

Materiál obsahuje: dôvodovú správu
Prílohu č. 1 PROTOKOL o výsledku kontroly systému ochrany
a bezpečnosti údajov vo verejnom sektore
Prílohu č. 2 Opatrenia na odstránenie kontrolou zisteného
nedostatku
Prílohu č. 3 Plnenie opatrenia na odstránenie kontrolou zisteného
nedostatku

Návrh na uznesenia: Mestské zastupiteľstvo mesta Piešťany po prerokovaní

Informáciu o výsledku kontroly NKÚ a Protokol o výsledku kontroly systému ochrany
a bezpečnosti údajov vo verejnom sektore

- berie na vedomie

Spracoval: RNDr. Denisa Bartošová, prednostka MsÚ Piešťany

Predkladá: Mgr. Peter Jančovič, primátor Mesta Piešťany

Dôvodová správa

Na základe poverenia predsedu NKÚ SR č. 1737/25 zo dňa 04.07.2019 bola v Meste Piešťany vykonaná kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore za kontrolované obdobie rokov 2016 - 2019, 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 v databázach a informačných systémoch.

Mesto Piešťany malo v internej smernici na ochranu osobných údajov vypracované pravidlá, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Smernica bola aktualizovaná k 01.09.2019, čo nebolo v súlade so zákonom č. 18/2018 Z. z., ktorý nadobudol účinnosť od 25.05.2018, kedy mala byť táto smernica aktualizovaná. Kontrolou bolo zistené, že existovala evidencia sprostredkovateľských zmlúv.

Za Mesto Piešťany boli oboznámení s výsledkom kontroly primátor mesta Mgr. Peter Jančovič, PhD. a prednostka MsÚ RNDr. Bartošová dňa 19.11.2019 a dňa 26.11.2019 bol protokol odovzdaný prednostke MsÚ v sídle Expozitúry NKÚ SR v Trnave.

Na základe požiadavky vedúceho kontrolnej skupiny je povinnosťou mesta oboznámiť mestské zastupiteľstvo s predmetným protokolom a prijatými opatreniami na najbližšom zasadnutí MsZ.

Protokol uvádzame v **prílohe č.1** predkladaného materiálu.

Na základe výsledkov kontroly a zápisnice o prerokovaní protokolu o výsledku kontroly zo dňa 26.11.2019 bolo prijaté dňa 2.12.2019 opatrenie na odstránenie kontrolou zisteného nedostatku, ktoré uvádzame v **prílohe č.2**.

V **prílohe č. 3** uvádzame Plnenie opatrenia na odstránenie kontrolou zisteného nedostatku.

NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo: Z-008736/2019/1130/PIA
Číslo poverenia: 1737/25
Zo dňa: 04.07.2019

Počet výtlačkov: 2
Výtlačok číslo: 2
Počet strán: 11
Počet príloh: -



**Protokol
o výsledku kontroly
systému ochrany a bezpečnosti údajov vo verejnom sektore
KA 015/2019**

Mesto Piešťany

Tmava, október 2019

Obsah

Zoznam použitých skratiek	3
Zhrnutie:	4
1 Harmonizácia vnútroštátneho práva ochrany osobných údajov s Nariadením EÚ 2016/679	5
1.1 Úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR pre prevádzkovateľov	5
2 Zabezpečenie osobných údajov občanov v databázach a informačných systémoch	6
2.1 Interné akty riadenia organizácie	6
2.2 Analýza procesov a povinností vyžadovaných podľa GDPR	6
2.3 Právny základ – pravidlá a postupy	6
2.4 Práva dotknutej osoby – pravidlá, postupy a oznámenia	7
2.5 Základné pravidlá a pokyny pre bezpečné spracúvanie údajov	7
2.6 Bezpečnostné smernice a dokumentácia	8
2.7 Informačná bezpečnosť – bezpečnostné štandardy	9
2.8 Výkon funkcie zodpovednej osoby	9
2.9 Činnosť sprostredkovateľov	10
3 Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa GDPR	11

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 (všeobecné 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 špecifik. 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 čl. 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 Piešťany 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 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).

Mesto malo v internej smernici na ochranu osobných údajov vypracované pravidla, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Smernica bola aktualizovaná k 01.09.2019, čo nebolo v súlade so zákonom č. 18/2018 Z. z., ktorý nadobudol účinnosť od 25.05.2018, kedy mala byť táto smernica aktualizovaná. Kontrolou bolo zistené, že existovala evidencia sprostredkovateľských zmlúv.

Podľa poverenia predsedu NKÚ SR č. 1737/25 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 29.07.2019 do 15.10.2019 v kontrolovanom subjekte

mesto Piešťany, Nám. SNP 1475/3, 921 45 Piešťany, IČO: 00612031

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 usmernenia ÚOOÚ SR boli pre prevádzkovateľa (mesto) primerane zrozumiteľné.

Kontrolou bolo zistené, že mesto Piešťany využívalo webové sídlo ÚOOÚ SR. Zverejnené informácie resp. metodiky považovalo mesto zrozumiteľné.

Kontrolovaný subjekt uzatvoril zmluvu o poskytovaní konzultačných služieb pri ochrane osobných údajov s obchodnou spoločnosťou wanet, s.r.o., ktorej predmetom bolo poverenie na výkon kompetencií zodpovednej osoby. Prílohou zmluvy bol menovací dekrét zodpovednej osoby.

Mesto v prípade akýchkoľvek problémov v oblasti ochrany OÚ využívalo hlavne vlastné personálne kapacity vrátane služieb externe zodpovednej osoby.

Mesto deklarovalo, že do času výkonu kontroly ÚOOÚ SR nevykonával v meste žiadnu kontrolu.

Záver k bodu 1

Mesto Piešťany využívalo webové sídlo ÚOOÚ SR. Zverejnené informácie resp. metodiky považovalo mesto zrozumiteľné. Mesto v prípade akýchkoľvek problémov v oblasti ochrany OÚ využívalo hlavne vlastné personálne kapacity vrátane služieb externe zodpovednej osoby.

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 zameriaval 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.

Kontrolovaný subjekt mal vypracovaný interný predpis upravujúci konanie a postup pri sprístupňovaní informácií podľa zákona o slobode informácií.

Preverení 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 spĺňa 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 konaniach nebolo zistené porušenie.

Interné pravidlá špecifikovali postupy, podľa ktorých oprávnené osoby prevádzkovateľa postupovali pri posudzovaní, či je spracúvanie získaných OÚ 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.

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. Platné a účinné boli interné normy:

- a) Smernica pre ochranu osobných údajov,
- b) Smernica pre vybavovanie práv dotknutých osôb k ich osobným údajom,
- c) Smernica pre používanie aktív so zreteľom na ochranu osobných údajov pre zamestnancov.

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

Kontrolou neboli zistené nedostatky.

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 pridelovanie prístupov do IS a určenie rozsahu spracovateľských operácií, ale nevedia 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.

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

Mesto zabezpečilo upratovacie služby vlastnými zamestnancami. Zamestnanci boli poučení v rámci ochrany osobných údajov. Všetci zamestnanci boli preškoľovaní ohľadom ochrany OÚ. Predmetom školenia bola aj informačná bezpečnosť.

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. 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 nepovolánym 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 ukladali povinnosť oprávnenej osobe vyznačiť vytvorenie kópie dokladu obsahujúceho OÚ a zakazovali ponechávať dokumenty (spisy) odložené v opustenom (resp. uzamknutom) dopravnom prostriedku. Osobitne tiež bolo 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 7 dní. Prevádzku kamerového systému zabezpečovalo mesto (Mestská polícia Piešťany). Monitorovaný priestor bol značený 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 – Smernica pre vybavovanie práv dotknutých osôb k smerom k ich osobným údajom.

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 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 bola platná interná norma Ochrana osobných údajov. Bezpečnostnú politiku tvorila Bezpečnostný projekt vrátane analýzy rizík a návrhov opatrení 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.

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, podľa vyjadrenia mesta, bezpečnostné incidenty.

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

2.8 Výkon funkcie zodpovednej osoby

Kontrolovaný subjekt uzatvoril 23.05.2018 zmluvu o poskytovaní konzultačných služieb pri ochrane osobných údajov s obchodnou spoločnosťou wanet, s.r.o., ktorej predmetom bolo poverenie na výkon kompetencií zodpovednej osoby. Prílohou zmluvy bol menovací dekrét zodpovednej osoby.

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 financovalo výlučne zo svojho rozpočtu.

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

Úlohou zodpovednej osoby bol dohľad spojený s ochranou OÚ prostredníctvom funkcie zodpovednej osoby 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, konzultácie v oblasti OÚ a školenia a poradenstvo.

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

2.9 Činnosť sprostredkovateľov

Kontrolné zistenie č.1

Mesto malo v internej smernici na ochranu osobných údajov vypracované pravidlá, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Smernica bola aktualizovaná k 01.09.2019, čo nebolo v súlade so zákonom č. 18/2018 Z. z., ktorý nadobudol účinnosť od 25.05.2018, kedy mala byť táto smernica aktualizovaná. Kontrolou bolo zistené, že existovala evidencia sprostredkovateľských zmlúv.

Kontrovaný subjekt mal uzatvorené tieto sprostredkovateľské zmluvy so :

- spprostredkovateľom, právnickou osobou Bytový podnik s.r.o., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ za účelom výkonu bytovej správy,
- spprostredkovateľom, právnickou osobou FT Technologies a.s., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ v rozsahu dojednaným v zmluve. Účelom bolo spracovanie OÚ v IS mestskej polície MP Manager,
- spprostredkovateľom, spoločnosťou Datalan a.s., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ v IS Korvin,
- spprostredkovateľom, Hour spol. s.r.o., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ v IS Human,
- spprostredkovateľom, Galileo corporation s.r.o., ktorej predmetom bolo poverenie sprostredkovateľa prevádzkovateľom spracúvaním OÚ v rámci webového sídla piestany.sk.

Záver k bodu 2

Mesto malo vypracované pravidlá, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Kontrolou bolo zistené, že existovalo päť zmlúv, ktoré boli uzatvorené so sprostredkovateľmi. Mesto malo v internej smernici na ochranu osobných údajov vypracované pravidlá, podľa ktorých postupovalo pri uzatváraní zmlúv so sprostredkovateľmi. Smernica bola aktualizovaná k 01.09.2019, čo nebolo v súlade so zákonom č. 18/2018 Z. z., ktorý nadobudol účinnosť od 25.05.2018, kedy mala byť táto smernica aktualizovaná.

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 financovalo výlučne zo svojho rozpočtu.

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 záznamy o spracovateľských činnostiach v rozsahu čl. 30 ods. 1 nariadenia GDPR. Lehoty uchovávaní údajov v jednotlivých IS boli upravené v registračnom poriadku. V prípade uchovávaní údajov internou smernicou zadefinované, že sa uplatňuje „zásada minimalizácie ich uchovávaní.“

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

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.

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. Podľa vyjadrenia mesta bolo v súvislosti s nariadením GDPR vyčlenených kontrolovaným subjektom v rokoch 2016 – 2017 spolu 27 078,00 eur (dvaja interní zamestnanci, zodpovedná osoba) na plnenie povinností súvisiacich s OÚ.

V súvislosti s ochranou OÚ mesto nakúpilo v rokoch 2016 – 2017 technické prostriedky v celkovej sume 6766,68 eur a vykonalo revíziu bezpečnostného projektu v hodnote 985,00 eur. Mesto zabezpečilo pre oprávnené osoby školenie v roku 2017 v celkovej sume 168,00 eur.

Mesto obstaralo výlučne so zavedením GDPR v roku 2018 – 2019 technické prostriedky v celkovej hodnote 40 618,63 eur (vlastné zdroje). Kontrolovaný subjekt zabezpečil v súvislosti so zavedením GDPR bezpečnostnú dokumentáciu (interné smernice) z vlastných zdrojov v celkovej sume 11 400,00 eur.

Mesto vynaložilo na činnosť sprostredkovateľov v rokoch 2018 s 2019 spolu 2916,00 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. Bolo preukázané, že financovanie preneseného výkonu štátnej správy nepokrývalo výdavky súvisiace s ochranou OÚ, resp. poskytnuté transfery boli určené výlučne na financovanie týchto kompetencií.

Za kontrolnú skupinu dňa

JUDr. Igor Puobiš
vedúci kontrolnej skupiny

.....

Mgr. Zuzana Luhová
členka kontrolnej skupiny

.....

S obsahom záznamu o výsledku kontroly bol oboznámený dňa

Mgr. Peter Jančovič, PhD.
primátor mesta

.....



MESTO PIEŠŤANY

Námestie SNP č. 3, 921 45 Piešťany

č.j. 47002/KV/2019 - 6964
Vybavuje: RNDr. Bartošová

V Piešťanoch, dňa 2.12.2019

Najvyšší kontrolný úrad SR
Expozitúra NKÚ SR Trnava
Kollárova 8
917 01 Trnava

Vec: Návrh opatrení

Na základe výsledkov kontroly systému ochrany a bezpečnosti údajov vo verejnom sektore KA 015/2019 a zápisnice o prerokovaní protokolu o výsledku kontroly zo dňa 26.11.2019 Vám zasielame opatrenie na odstránenie kontrolou zisteného nedostatku:

KONTROLNÉ ZISTENIE:

Kontrola preukázala, že smernica na ochranu osobných údajov bola aktualizovaná k 01.09.2019, čo nebolo v súlade so zákonom č.18/2018, ktorý nadobudol účinnosť od 25.5.2018, kedy mala byť táto smernica aktualizovaná.

OPATRENIE ku kontrolnému zisteniu:

Aktualizovať smernicu o ochrane osobných údajov.

T: v priebehu kontroly

Z: prednostka MsÚ a zodpovedná osoba

S pozdravom

Mgr. Peter Jančovič, PhD.
primátor mesta Piešťany



MESTO PIEŠŤANY

Námestie SNP č. 3, 921 45 Piešťany

č.j. 47001/WM/2019 - 6964
Vybavuje: RNDr. Bartošová

V Piešťanoch, dňa 4.12.2019

Najvyšší kontrolný úrad SR
Expozitúra NKÚ SR Trnava
Kollárova 8
917 01 Trnava

Vec: Návrh opatrení – plnenie.

Na základe výsledkov kontroly systému ochrany a bezpečnosti údajov vo verejnom sektore KA 015/2019 a zápisnice o prerokovaní protokolu o výsledku kontroly zo dňa 26.11.2019 Vám zasielame plnenie opatrenia na odstránenie kontrolou zisteného nedostatku:

KONTROLNÉ ZISTENIE:

Kontrola preukázala, že smernica na ochranu osobných údajov bola aktualizovaná k 01.09.2019, čo nebolo v súlade so zákonom č.18/2018, ktorý nadobudol účinnosť od 25.5.2018, kedy mala byť táto smernica aktualizovaná.

OPATRENIE ku kontrolnému zisteniu:

Aktualizovať smernicu o ochrane osobných údajov.

T: v priebehu kontroly

Z: prednostka MsÚ a zodpovedná osoba

Stav plnenia:

Opatrenie bolo splnené

Smernica o ochrane osobných údajov bola aktualizovaná v priebehu kontroly.

S pozdravom

Mgr. Peter Jančovič, PhD.
primátor mesta Piešťany