16

Mesto Sabinov
Mestský úrad, Námestie slobody 57, 083 01 Sabinov

M a t e r i á l
na zasadnutie Mestského zastupiteľstva
dňa 12. decembra 2019

K bodu:

Informácia o výsledku kontroly NKÚ SR: Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov

Predkladá:

JUDr. Martin Judičák
prednosta MsÚ

Návrh na uznesenie:

Mestské zastupiteľstvo prerokovalo predložený materiál a podľa § 20a ods.1 zákona NR SR č. 39/1993 Zb. o Najvyššom kontrolnom úrade SR v znení neskorších právnych predpisov

berie na vedomie

Informáciu o výsledku kontroly NKÚ SR: Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov

Vypracoval:

JUDr. Martin Judičák
prednosta MsÚ

DÔVODOVÁ SPRÁVA

Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov bola vykonaná na základe plánu kontrolnej činnosti NKÚ SR na rok 2019 podľa poverenia predsedu NKÚ SR č. 1737/56 zo 04.07.2019.

Účelom kontroly bolo zistiť objem finančných prostriedkov ktoré boli alokované na zabezpečenie ochrany údajov, prispieť k správnej implementácii potrebných technických, organizačných a personálnych opatrení vyplývajúcich prevádzkovateľovi z nariadenia GDPR a poukázať na možné formálne plnenie povinností v predmetnej politike.

Predmetom kontroly bola harmonizácia vnútroštátneho práva ochrany osobných údajov s nariadením GDPR, zabezpečenie osobných údajov občanov v databázach a informačných systémoch a finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia GDPR.

Pri kontrole bolo použitých viacero metód a techník: štúdium právnych predpisov EÚ, všeobecne záväzných právnych predpisov, interných predpisov, preskúmanie predložených dokladov a dokumentácie, analýza, syntéza, prepočty, dedukcia, rozhovor, výberové zisťovanie a iné.

Z dôvodu rozsiahlosti nariadenia GDPR a zároveň snahe poskytnúť čo najkomplexnejší pohľad na kvalitatívnu úroveň primeraných technických a organizačných opatrení a ostatných pravidiel a postupov pre používateľov prijatých v súvislosti s ochranou osobných údajov prevádzkovateľom v súlade s nariadením GDPR a ostatnými vnútroštátnymi predpismi, boli pri kontrole na účel hodnotenia použité dve kritériá:

1) štandardný postup preverovania súladu prijatých opatrení prevádzkovateľom podľa platnej legislatívy ustanovenej najmä nariadením GDPR, zákonom č. 18/2018 Z. z. o ochrane osobných údajov a výnosom MF SR o štandardoch pre IS verejnej správy,
2) splnenie kvalitatívnych požiadaviek, postupov a pravidiel dobrej praxe a štandardov bezpečnosti.

Od týchto oblastí sa odlišovala oblasť „Úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ pre prevádzkovateľov", ktorá bola preverovaná v rámci predmetu kontroly „Harmonizácia vnútroštátneho práva ochrany osobných údajov s nariadením GDPR". V tejto oblasti nebol hodnotený prevádzkovateľ, ale na základe vyjadrení prevádzkovateľa bol hodnotený stav harmonizácie prijatého vnútroštátneho práva ochrany osobných údajov s nariadením GDPR a úroveň zrozumiteľnosti zákona č. 18/2018 Z. z. o ochrane osobných údajov a usmernení ÚOOÚ pre prevádzkovateľa. NKU SR vyhodnotil oblasť zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR tak, že legislatíva aj usmernenia boli pre mesto zrozumiteľné.

Kontrola bola vykonaná v čase od 17.07.2019 do 18.10.2019 za kontrolované obdobie rokov 2016 – 2019, v prípade vecných súvislostí aj predchádzajúce a nasledujúce obdobia.

Kontrola bola vykonaná v súlade so zákonom o NKÚ SR a so štandardami, ktoré vychádzajú zo základných princípov medzinárodných štandardov najvyšších kontrolných inštitúcií (ISSAI).

Výsledky sú uvedené v protokole o výsledku kontroly (príloha č. 1) a boli prerokované v súlade s § 15 ods. 1 písm. g) zákona č. 39/1993 Z. z. o Najvyššom kontrolnom úrade SR v znení neskorších predpisov dňa 31.10.2019.

Na odstránenie zistených nedostatkov prijalo mesto Sabinov opatrenia dňa 18.11.2019 (Príloha č. 2).

Stanovisko Mestskej rady:
Mestská rada prerokovala predložený materiál a odporúča mestskému zastupiteľstvu informáciu o výsledku kontroly NKÚ SR: Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov vziať na vedomie.

Pozmeňujúci a doplňujúci návrh poslanca mestského zastupiteľstva:

Rokovanie MsZ konaného dňa .....

k bodu programu: .....

.....

.....

Presne sformulovaný pozmeňujúci a doplňujúci návrh:

.....

.....

.....

.....

.....

.....

Meno a priezvisko poslanca: .....

Mestské zastupiteľstvo v S a b i n o v e

U z n e s e n i e
Mestského zastupiteľstva č. ....

zo dňa 12. decembra 2019

… **k Informácii o výsledku kontroly NKÚ SR: Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov**

Mestské zastupiteľstvo prerokovalo predložený materiál a podľa § 20a ods.1 zákona NR SR č. 39/1993 Zb. o Najvyššom kontrolnom úrade SR v znení neskorších právnych predpisov

berie na vedomie

Informáciu o výsledku kontroly NKÚ SR: Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov.

V Sabinove, dňa 12.12.2019

Ing. Michal Repaský
primátor mesta

NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo poverenia: 1737/56
zo dňa 04.07.2019
Číslo: Z-007942/2019/1110/VLB

Počet výtlačkov: 2
Výtlačok číslo: 2
Počet strán: 16
Počet príloh: 0

PROTOKOL
o výsledku kontroly systému ochrany a bezpečnosti údajov vo verejnom sektore KA-015/2019/1032

Mesto Sabinov

Prešov, október 2019

Obsah

Zoznam použitých skratiek:

Skrátený názov	Úplné znenie
BOZP	Bezpečnosť a ochrana zdravia pri práci
CUBS, s. r. o	CUBS, s. r. o, Masarykova 21, 040 01 Košice
DCOM	Dátové centrum obcí a miest
DEUS	DataCentrum elektronizácie územnej samosprávy Slovenska
EÚ	Európska únia
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IS	Informačný systém
IT	Informačná technológia
ISO	International Organization for Standardization
ISSAI	International Standards of Supreme Audit Institutions
mesto alebo prevádzkovateľ	Mesto Sabinov
MsÚ	Mestský úrad Sabinov
nariadenie GDPR	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
PC	Personal computer
SR	Slovenská republika
ÚOOÚ	Úrad na ochranu osobných údajov Slovenskej republiky
výnos MF SR o štandardoch pre IS verejnej správy	Výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov
Výnos MV SR o štandardoch pre elektronické IS na správu registratúry	Výnos Ministerstva vnútra SR č. 525/2011 Z. z. o štandardoch pre elektronické informačné systémy na správu registratúry v znení neskorších predpisov
zákon č. 122/2013 Z. z. 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 č. 18/2018 Z. z. o ochrane osobných údajov	Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
zákon o archívoch a registratúrach	Zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
zákon o NKÚ SR	Zákon č. 39/1993 Z. z. o Najvyššom kontrolnom úrade Slovenskej republiky 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 slobode informácií	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

Zhrnutie:

Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore v meste Sabinov bola vykonaná na základe plánu kontrolnej činnosti NKÚ SR na rok 2019.

Účelom kontroly bolo zistiť objem finančných prostriedkov ktoré boli alokované na zabezpečenie ochrany údajov, prispieť k správnej implementácii potrebných technických, organizačných a personálnych opatrení vyplývajúcich prevádzkovateľovi z nariadenia GDPR a poukázať na možné formálne plnenie povinností v predmetnej politike.

Predmetom kontroly bola harmonizácia vnútroštátneho práva ochrany osobných údajov s nariadením GDPR, zabezpečenie osobných údajov občanov v databázach a informačných systémoch a finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia GDPR.

Pri kontrole bolo použitých viacero metód a techník: štúdium právnych predpisov EÚ, všeobecne záväzných právnych predpisov, interných predpisov, preskúmanie predložených dokladov a dokumentácie, analýza, syntéza, prepočty, dedukcia, rozhovor, výberové zisťovanie a iné.

Z dôvodu rozsiahlosti nariadenia GDPR a zároveň snahe poskytnúť čo najkomplexnejší pohľad na kvalitatívnu úroveň primeraných technických a organizačných opatrení a ostatných pravidiel a postupov pre používateľov prijatých v súvislosti s ochranou osobných údajov prevádzkovateľom v súlade s nariadením GDPR a ostatnými vnútroštátnymi predpismi, boli pri kontrole na účel hodnotenia použité dve kritériá:

1) štandardný postup preverovania súladu prijatých opatrení prevádzkovateľom podľa platnej legislatívy ustanovenej najmä nariadením GDPR, zákonom č. 18/2018 Z. z. o ochrane osobných údajov a výnosom MF SR o štandardoch pre IS verejnej správy,
2) splnenie kvalitatívnych požiadaviek, postupov a pravidiel dobrej praxe a štandardov bezpečnosti.

Od týchto oblastí sa odlišovala oblasť „Úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ pre prevádzkovateľov", ktorá bola preverovaná v rámci predmetu kontroly „Harmonizácia vnútroštátneho práva ochrany osobných údajov s nariadením GDPR". V tejto oblasti nebol hodnotený prevádzkovateľ, ale na základe vyjadrení prevádzkovateľa bol hodnotený stav harmonizácie prijatého vnútroštátneho práva ochrany osobných údajov s nariadením GDPR a úroveň zrozumiteľnosti zákona č. 18/2018 Z. z. o ochrane osobných údajov a usmernení ÚOOÚ pre prevádzkovateľa. NKU SR vyhodnotil oblasť zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR tak, že legislatíva aj usmernenia boli pre mesto zrozumiteľné.

Kontrolou bolo zistené, že do účinnosti nariadenia GDPR mesto malo určenú zodpovednú osobu z interných zamestnancov mesta, ktorá vykonávala túto funkciu aj po 25.05.2018. Zodpovedná osoba vykonávala kumulované činnosti vo funkcii referent pre civilnú ochranu, požiarnu ochranu a BOZP a bola odmeňovaná v rámci výkonu svojej pracovnej činnosti z vlastných zdrojov mesta.

Dve organizácie bolo voči kontrolovanému subjektu v postavení sprostredkovateľa. Mesto ako spoločný obecný úrad bolo taktiež v pozícii sprostredkovateľa pre obce pri zabezpečovaní úloh preneseného výkonu štátnej správy.

Mesto ešte pred účinnosťou nariadenia GDPR preskúmalo a identifikovalo IS, v ktorých spracúvalo osobné údaje za účelom ich zosúladenia s novou legislatívou platnou od 25.05.2018. Zároveň transparentným spôsobom na svojom webovom sídle informovalo dotknuté osoby o i právach a všetkých IS prevádzkovateľa, s uvedením ich právneho základu a účele spracovania osobných údajov.

Mesto nemalo vypracované pravidlá a postupy pre oprávnené osoby napríklad pre prípady, keď dochádzalo k získavaniu osobných údajov alebo uplatňovaniu práv dotknutých osôb, ale vychádzalo z jednotlivých ustanovení nariadenia GDPR. Kontrolou bolo ďalej zistené, že mesto vyžadovalo súhlasy dotknutých osôb so spracovaním osobných údajov aj pri výberových konaniach na voľné pracovné miesto v rámci predzmluvných vzťahov.

Pre oprávnené osoby boli určené pravidlá a pokyny v interných smerniciach ako bezpečnostný projekt v znení dodatku č. 1, Smernici o ochrane osobných údajov a Smernici o používaní IS kamerový systém. Uvedené smernice však neboli k 25.05.2018 aktualizované.

V prípade prijatých bezpečnostných opatrení boli zistené niektoré nedostatky, keď interné smernice neupravovali všetky požiadavky na štandardy pre architektúru riadenia a minimálneho technického zabezpečenia podľa výnosu MF SR o štandardoch pre IS verejnej správy. Napriek uvedenému však bola zabezpečená primeraná úroveň ochrany osobných údajov a kľúčových komponentov IS.

Mesto uhrádzalo výdavky na ochranu osobných údajov len z vlastných zdrojov, nežiadalo ďalšie subjekt o poskytnutie finančných zdrojov na ochranu osobných údajov. Finančné prostriedky na oblasť ochrany osobných údajov boli obmedzené.

Odporúčania:

- v interných smerniciach upraviť rozsah zverejňovaných osobných údajov fyzických osôb (titul, meno, priezvisko) a bližšie špecifikovať postupy pri nakladaní s osobitnými kategóriami osobných údajov, ktoré by mohli byť zaznamenané napríklad pri kontrole požitia alkoholu alebo iných návykových látok,
- pre účely výberových konaní nevyžadovať súhlasy dotknutých osôb so spracovaním osobných údajov,
- primerane upraviť platné interné predpisy a precizovať aj procesy súvisiace s nakladaním s osobnými údajmi podľa nariadenia GDPR, pri ktorých dochádza zo strany oprávnených osôb k rozhodovaniu, resp., posúdeniu skutočnosti. Tým bude zabezpečená jednotnosť rozhodovania oprávnených osôb v tých istých záležitostiach.
- za účelom preukázateľnosti činnosti zodpovednej osoby vypracúvať priebežné výkazy činnosti a ročnú správu o svojej činnosti, vrátane vypracúvania písomných záznamov z každej komunikácie zodpovednej osoby s najvyšším vedením mesta,
- definovať v interných smerniciach opatrenia ako zákaz ponechávať dokumenty voľne odložené na chodbách, v rokovacích sálach a povinnosť pri práci s citlivými dokumentmi obsahujúcim osobitné kategórie údajov postupovať obozretnejšie,
- definovať v interných smerniciach napríklad konkrétne požiadavky na zložitosť hesla, zákaz používania autentizačných prostriedkov elektronickou poštou alebo faxom vo forme voľne čitateľného textu a zákaz využívať funkcionalitu zapamätať heslo,
- definovať v interných smerniciach povinnosť kontrolovať prenosné média antivírusovým programom pri ich vkladaní alebo výslovnú povinnosť používateľa, ktorý z rôznych dôvodov pracuje na PC pridelenom inému používateľovi, prihlasovať sa do systému výlučne pod svojim užívateľským účtom.

Podľa poverenia predsedu NKÚ SR č. **1737/56** zo 04.07.2019 vykonali:

Mgr. Lucia Vasičková, vedúca kontrolnej skupiny
Mgr. Ivana Petričová, 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 prevádzkovateľovi z nariadenia GDPR a poukázať na možné formálne plnenie povinností v predmetnej politike.

Kontrola bola vykonaná v čase od 17.07.2019 do 18.10.2019 v subjekte:

Mesto Sabinov, Námestie slobody 57, 083 01 Sabinov, IČO 00327735

za kontrolované obdobie rokov 2016 – 2019, v prípade vecných súvislostí aj predchádzajúce a nasledujúce obdobia.

Kontrola bola vykonaná v súlade so zákonom o NKÚ SR 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 GDPR, zabezpečenie osobných údajov občanov v databázach a IS a finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia GDPR.

Počas výkonu kontroly bolo zistené:

1 Harmonizácia vnútroštátneho práva ochrany osobných údajov s nariadením GDPR

1.1 Úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR pre prevádzkovateľov

Účelom kontroly bolo preverenie, či legislatíva súvisiaca s ochranou osobných údajov a usmernenia a metodika ÚOOÚ boli pre prevádzkovateľa zastúpené internou zodpovednou osobou dostatočne prehľadné, jasné a zrozumiteľné.

Kontrolou bolo zistené, že zodpovedná osoba využívala webové sídlo ÚOOU najmä na získavanie metodiky, metodických usmernení pri aplikácií nariadenia GDPR v praxi, ako napríklad Metodické usmernenie č. 2/2018 Zákonnosť spracúvania.

Podľa vyjadrenia zodpovednej osoby usmernenie ÚOOÚ „Kedy Nariadenie a kedy zákon na ochranu osobných údajov" z 20.06.2018 bolo jasné, zrozumiteľné a aplikovateľné a s názorom, že prevádzkovateľ môže postupovať len podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov sa zodpovedná osoba plne stotožňovala. Podľa vyjadrenia zodpovednej osoby bolo možné správne implementovať a aplikovať nariadenie GDPR bez externého právneho poradenstva. ÚOOÚ nevykonal v meste do 25.05.2018 ani po 25.05.2018 žiadnu kontrolu spracúvania osobných údajov.

Záver

Oblasť zrozumiteľnosti práva a usmernení ÚOOÚ bola vyhodnotená ako zrozumiteľná.

2 Zabezpečenie osobných údajov občanov v databázach a informačných systémoch

V súvislosti s plnením nových povinností zavedených v nariadení GDPR boli prevádzkovatelia nútení viaceré zabehnuté mechanizmy ochrany osobných údajov modifikovať a zaviesť ďalšie opatrenia na zosúladenie spracúvania v IS. To im mohlo spôsobiť nárast investícií a nákladov na zabezpečenie ľudských zdrojov.

Do 25.05.2018 bol každý prevádzkovateľ povinný podľa nariadenia GDPR prijať vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie vykonáva v súlade s nariadením GDPR. Zároveň mal prijať vhodné opatrenia s cieľom poskytnúť dotknutej osobe v súvislosti so získavaním osobných údajov všetky informácie uvedené v čl. 13 a 14 a v súvislosti s uplatňovaním jej práv všetky oznámenia podľa čl. 15 až 22 a čl. 34 nariadenia GDPR

a to v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho, a uplatňovanie práv jej uľahčovať.

Súčasne bol prevádzkovateľ povinný zabezpečiť, aby každá fyzická osoba, ktorú poveril spracúvaním a tá získala prístup k osobným údajom, spracúvala tieto údaje len na základe pokynov prevádzkovateľa s výnimkou prípadov, keď sa to vyžaduje podľa práva EÚ alebo SR. Taktiež sprostredkovateľ a každá poverená osoba by ich mala môcť spracúvať len na základe pokynov prevádzkovateľa.

Každý orgán verejnej moci a verejnoprávny subjekt bol povinný s súčinnosťou od 25.05.2018 určiť zodpovednú osobu.

Podľa § 78 ods. 11 zákona č. 18/2018 Z. z. o ochrane osobných údajov prevádzkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov bol zaviazaný primerane postupovať podľa medzinárodných noriem a štandardov bezpečnosti.

2.1 Úroveň prijatých opatrení na zabezpečenie súladu s nariadením GDPR

2.1.1 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, BOZP) v súvislosti s nakladaním s osobnými údajmi.

Kontrolou bolo zistené, že mesto malo vypracovaný Organizačný poriadok Mestského úradu v Sabinove s účinnosťou od 01.07.2007, ktorý bol vydaný primátorom mesta v súlade s ustanovením § 13 ods. 4 písm. d) zákona o obecnom zriadení.

Pracovný poriadok pre zamestnancov Mesta Sabinov účinný od 01.02.2016 bol prerokovaný s odborovou organizáciou pri MsÚ uznesením č. 1/2016 dňa 14.01.2016. Pracovný poriadok neobsahoval informáciu, že majetkové priznania zamestnancov sa spracúvajú v osobitnom IS a nezakladajú sa do osobného spisu zamestnanca. Kontrolou bolo zistené, že zodpovední zamestnanci v prípade spracúvania majetkových priznaní postupovali tak, že tieto neboli zakladané do osobných spisov zamestnancov.

Usmernenie č. 1/2019 Mestského úradu v Sabinove zo 04.06.2019 o registratúrnom poriadku, ktoré nadobudlo účinnosť 01.07.2019 zrušilo Registratúrny poriadok a Registratúrny plán platný od 01.07.2016. Registratúrny poriadok obsahoval podrobnosti o postupe pri spracovaní elektronických registratúrnych záznamov v súlade s § 16a zákona o archívoch a registratúrach. Mesto využívalo elektronický systém správy registratúry od firmy DATALAN, a. s., ktorý je v zhode so štandardmi ustanovenými podľa výnosu MV SR o štandardoch pre elektronické IS na správu registratúry.

Mesto malo vypracovanú aj Smernicu o slobodnom prístupe k informáciám, ktorá nadobudla účinnosť 01.11.2008, pričom neupravovala postup určený pre oprávnené osoby, ako aplikovať v praxi ustanovenie § 9 ods. 1 až 3 zákona o slobode informácií – ochrana osobnosti a osobných údajov a za akých podmienok by mali poskytnúť informáciu, ak obsahuje údaje fyzickej osoby.

Smernica o povinnom zverejňovaní zmlúv, objednávok a faktúr v podmienkach mesta Sabinov, ktorá nadobudla účinnosť 01.03.2017 neobsahovala postup oprávnených osôb pri zverejňovaní osobných údajov fyzických osôb v zmluvách.

Mesto malo vypracovanú smernicu na zaistenie bezpečnosti a ochrany zdravia pri práci z 05.02.2019. Kontrola používania alkoholických nápojov a iných omamných a psychotropných látok bola upravená v samostatnej smernici z 01.02.2008. Nakladanie s osobitnými kategóriami osobných údajov, ktoré by boli zaznamenané napríklad pri zistení prítomnosti omamných látok alebo psychotropných látok, resp. alkoholu, neboli bližšie špecifikované. Tieto osobné údaje si vyžadovali zvýšenú ochranu a povinnosť mlčanlivosti.

Odporúčanie:

NKU SR odporúča v interných smerniciach upraviť rozsah zverejňovaných osobných údajov fyzických osôb (titul, meno, priezvisko) a bližšie špecifikovať postupy pri nakladaní s osobitnými kategóriami osobných údajov, ktoré by mohli byť zaznamenané napríklad pri kontrole požitia alkoholu alebo iných návykových látok.

2.1.2 Analýza procesov a povinností vyžadovaných podľa nariadenia GDPR

V rámci všeobecnej povinnosti prevádzkovateľa vypracovalo mesto prostredníctvom firmy CUBS, s. r. o. dokument „Posúdenie vplyvu na ochranu osobných údajov (personálne, organizačné a technické opatrenia) prevádzkovateľa" za účelom identifikovania, či určitý druh spracúvania osobných údajov nepovedie k vysokému riziku pre práva a slobody fyzických osôb. Súčasťou dokumentu bola aj analýza procesov, priestorov, IS a posúdenie úrovne bezpečnosti ochrany osobných údajov vrátane navrhnutých opatrení, ktoré mal prevádzkovateľ zaviesť v súvislosti s nariadením GDPR. Uvedená analýza neidentifikovala pri spracovateľských operáciách vysoké riziká pre práva a slobody fyzických osôb.

Súčasťou dokumentu boli aj vypracované nové záznamy o spracovateľských činnostiach (Príloha č. 1), ktoré obsahovali všetky náležitosti v zmysle čl. 30 ods. 1 nariadenia GDPR a tieto boli zverejnené aj na webovom sídle mesta v časti Ochrana osobných údajov. Prenos osobných údajov v jednotlivých IS sa u prevádzkovateľa neuskutočňoval.

Na základe vykonanej analýzy zmlúv s externými subjektami boli identifikovaní dvaja sprostredkovatelia, ktorí spracúvali osobné údaje v mene prevádzkovateľa.

2.1.3 Právny základ spracúvania osobných údajov – pravidlá a postupy

Mesto spracúvalo osobné údaje na základe zásady zákonnosti, z dôvodu pozície mesta ako orgánu verejnej moci, z plnenia zmluvných vzťahov alebo predzmluvných vzťahov, resp. z plnenia zákonných povinností mesta. V takýchto prípadoch nebol vyžadovaný súhlas dotknutej osoby.

V rámci interných pravidiel mesto bližšie nešpecifikovalo všeobecné postupy pre oprávnené osoby, akým spôsobom postupovať, ak je právnym základom spracúvania osobných údajov súhlas dotknutej osoby.

V niektorých prípadoch mesto spracúvalo osobné údaje, kedy bol právnym základom ich spracúvania súhlas dotknutej osoby (napríklad: pre účel vedenia evidencie členov rady školy, propagácie prevádzkovateľa, zverejňovania informácií o organizovaných podujatiach, resp. aktivitách, uvítania novorodencov do života, evidencie jubilantov). Uvedené súhlasy obsahovali informácie o účele použitia osobných údajov, rozsahu ich spracúvania a možnosti a spôsobe odvolania súhlasu.

Kontrolou bolo zistené, že prevádzkovateľ vyžadoval súhlas dotknutej osoby aj pri výberových konaniach na pracovné pozície mesta aj napriek tomu, že na ich spracúvanie nebol potrebný súhlas v zmysle článku 6 ods. 1 písm. b/ nariadenia GDPR (predzmluvný vzťah).

Odporúčanie:
NKÚ SR odporúča, aby na účely výberových konaní neboli vyžadované súhlasy dotknutých osôb so spracovaním osobných údajov.

Podmienky spracúvania osobných údajov, ktoré usmerňovali oprávnené osoby pri nakladaní s osobnými údajmi boli obsiahnuté v „Poverení a poučení oprávnenej osoby", ktoré obsahovalo popis IS, účel spracúvania osobných údajov a identifikáciu jednotlivých spracovateľských operácií, ktoré môžu oprávnené osoby vykonávať. Účely a právne základy boli taktiež bližšie definované v „Záznamoch o spracovateľských činnostiach" prevádzkovateľa.

Kontrolou bolo zistené, že mesto spracúvalo osobné údaje na právnom základe podľa čl. 6 ods. 1 písm. f/ nariadenia GDPR „oprávnený záujem", ktorý sledoval prevádzkovateľ, a to v IS Evidencia zástupcov odberateľov a dodávateľov.

Pred spracúvaním osobných údajov v IS mesto vypracovalo tzv. „balančný test", aby zistilo, či práva alebo právom chránené záujmy fyzickej osoby, ktorej osobné údaje sa spracúvajú, neprevažujú nad oprávnenými záujmami prevádzkovateľa.

Oprávneným záujmom pre mesto bolo zabezpečenie kontinuálnej a efektívnej komunikácie so zástupcami dodávateľov a odberateľov. V rámci testu boli posúdené: legitímnosť, nevyhnutnosť, vhodnosť, proporcionalita

a primerané záruky prevádzkovateľa. Výsledkom balančného testu bolo konštatovanie, že prevádzkovateľ plne rešpektuje záujmy ako aj základné práva a slobody dotknutých osôb, najmä právo na súkromie. Uvedené právo dotknutej osoby však neprevyšuje nad oprávneným záujmom prevádzkovateľa.

Postupy pri prenose osobných údajov do tretích krajín podľa ktorých oprávnené osoby mali postupovať neboli zo strany mesta špecifikované, nakoľko prenos do tretích krajín nebol u prevádzkovateľa zamýšľaný.

2.1.4 Práva dotknutej osoby – pravidlá, postupy a oznámenia

V tejto oblasti bolo preverené, aké pokyny prevádzkovateľ vydal oprávneným osobám v súvislosti s poskytovaním informácií dotknutým osobám, aké pravidlá a postupy zadefinoval v zázname o poučení pre oprávnené osoby v súvislosti s uplatňovaním práv dotknutých osôb a do akej miery sú oznámenia o možnosti uplatniť si právo určené dotknutým osobám transparentné.

Pravidlá upravujúce rozsah informácií, ktoré oprávnené osoby poskytujú dotknutým osobám pri získavaní osobných údajov boli súčasťou Smernice o ochrane osobných údajov, s ktorou boli oboznámené všetky oprávnené osoby.

Pravidlá mali všeobecný charakter a bližšie nešpecifikovali podrobnosti o:

- postupe mesta, ak by malo v úmysle spracúvať získané osobné údaje na iný účel, ako na ten, na ktorý boli pôvodne získané;
- postupe, akým spôsobom informuje prevádzkovateľ dotknutú osobu o oprávnenom záujme,
- postupe, za akých okolností oprávnené osoby informácie dotknutej osobe neoznamujú (článok 14 ods. 5 nariadenia GDPR).

Rozsah údajov, ktoré mesto poskytovalo dotknutej osobe v zmysle čl. 13 a príslušných recitálov nariadenia GDPR, ako aj postup dotknutej osoby v súvislosti so získaním tých údajov, bol zverejnený na webovom sídle mesta pod názvom „Zásady ochrany osobných údajov".

Pravidlá pri uplatňovaní práv dotknutej osoby boli taktiež súčasťou Smernice o ochrane osobných údajov a z hľadiska obsahu boli formulované všeobecne bez podrobnejších postupov, pričom prevádzkovateľ pri ich uplatňovali vychádzal z jednotlivých ustanovení nariadenia GDPR.

Napríklad pravidlá neobsahovali podrobnosti, ako má oprávnená osoba postupovať pri rozhodovaní o tom, či poskytnutie kópie s osobnými údajmi dotknutej osobe nebude mať nepriaznivé dôsledky na práva a slobody iných osôb, podrobnosti, za akých okolností oprávnená osoba neopraví osobné údaje dotknutej osoby alebo kritériá pre posudzovanie resp. hodnotenie, či ide alebo nejde o situáciu, že oznámenie je nemožné, resp. si to vyžaduje neprimerané úsilie. Pravidlá ďalej neobsahovali podmienku, že odpoveď zaslaná listovou zásielkou môže byť len vo forme doporučenej zásielky s poznámkou "do vlastných rúk" a tiež nebola bližšie špecifikovaná metodika zdôvodňovania neopodstatnenosti alebo neprimeranosti žiadosti.

Dotknutá osoba si mohla svoje práva uplatňovať písomne alebo elektronicky prostredníctvom zodpovednej osoby, prípadne zodpovedných zamestnancov. V rokoch 2018 a 2019 (k 30.06.2019) nedošlo k uplatneniu práv dotknutými osobami.

Odporúčanie:

NKÚ SR odporúča primerane doplniť/upraviť platné interné predpisy a precizovať aj procesy súvisiace s nakladaním s osobnými údajmi podľa nariadenia GDPR, pri ktorých dochádza zo strany oprávnených osôb k rozhodovaniu, resp., posúdeniu skutočnosti. Tým bude zabezpečená jednotnosť rozhodovania oprávnených osôb v tých istých záležitostiach.

Kontrolou bolo zistené, že mesto transparentným spôsobom na svojom webovom sídle informovalo dotknuté osoby o ich právach, a to v „Zásadách ochrany osobných údajov" v sekcii Ochrana osobných údajov. O práve kedykoľvek odvolať súhlas boli dotknuté osoby informované priamo na tlačive na udelenie súhlasu. Zároveň boli dotknuté osoby informované o všetkých IS prevádzkovateľa, ich právnom základe a účele spracovania osobných údajov.

2.1.5 Základné pravidlá a pokyny pre bezpečné spracúvanie údajov

Mesto vykonávalo poučenie oprávnenej osoby pri nástupe do zamestnania, pred vykonaním prvej spracovateľskej operácie s osobnými údajmi. Mesto malo zadefinované pravidlá pre prideľovanie prístupov do IS a určenie rozsahu spracovateľských operácií. Práva boli prideľované na základe zásady minimalizácie, tzn. že oprávnená osoba mala len také prístupové práva, ktoré nevyhnutne súviseli s jej pracovnou náplňou. Poučenia vymedzovali IS s osobnými údajmi a rozsah povolených činností. Mesto vykonávalo preškolenie oprávnených osôb v oblasti ochrany osobných údajov raz ročne. Oprávnené osoby boli zaviazané povinnosťou dodržiavať mlčanlivosť o osobných údajoch, s ktorými prichádzali do styku.

V prípade ukončenia pracovného pomeru bol zamestnanec povinný vrátiť pridelené úložné médiá a boli mu bezodkladne odobraté prístupové práva do IS. Pracovné náplne zamestnancov definovali procesy v prípade zastupovania zamestnanca. Interné smernice neurčovali podmienku, že zastupovanie môže vykonávať len osoba s rovnakými, alebo väčšími prístupovými právami. Boli zadefinované procesy pre prípad opätovného poučenia.

Zamestnanci mesta zabezpečujúci upratovanie boli poučení o povinnosti mlčanlivosti v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov

V oblasti bezpečnostných opatrení prevádzkovateľa IS boli definované opatrenia na zabezpečenie ich ochrany pred zneužitím, odcudzením, poškodením, zničením, stratou v rámci technických opatrení (technické opatrenia realizované prostriedkami fyzickej povahy, ochrana pred neoprávneným prístupom, riadenia prístupu oprávnených osôb, ochrany proti škodlivému kódu, sieťovej bezpečnosti, zálohovania, likvidácie osobných údajov a dátových nosičov, aktualizácie operačného systému a programového aplikačného vybavenia), organizačných opatrení (personálne opatrenia, vedenie zoznamu aktív a jeho aktualizácia, riadenia prístupu oprávnených osôb k osobným údajom, organizácie spracúvania osobných údajov, likvidácie osobných údajov, bezpečnostných incidentov a kontrolnej činnosti) a programového vybavenia slúžiaceho na spracúvanie osobných údajov v podmienkach prevádzkovateľa IS. V prípade, ak by došlo k bezpečnostnému incidentu, bolo to potrebné nahlásiť neodkladne štatutárovi mesta.

Pokyny na získavanie osobných údajov kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to právny predpis predpokladá, boli definované v Smernici o ochrane osobných údajov z 11.12.2018 a Smernici o získavaní a manipulácií s osobnými údajmi z 02.01.2019.

Mesto malo v Smernici o ochrane osobných údajov zadefinovanú politiku čistého stola, povinnosť odkladať dokumenty v uzamykateľných skriniach, opatrenia pri kopírovaní dokumentov a evidencie prístupov do spisu. Opatrenia ako zákaz ponechávať dokumenty voľne odložené na chodbách, v rokovacích sálach a povinnosť pri práci s citlivými dokumentmi obsahujúcim osobitné kategórie údajov postupovať obozretnejšie neboli definované.

V podmienkach mesta boli upravené pravidlá a pokyny na identifikáciu a autentizáciu informačných prostriedkov oprávnenými osobami ako napríklad chrániť autentizačné heslo, zmena hesla pri prvom prihlásení a aktualizovať heslo raz za tri mesiace. Interné smernice neupravovali konkrétne požiadavky na zložitosť hesla (iba požiadavka na osem alfanumerických znakov), zákaz používania autentizačných prostriedkov elektronickou poštou alebo faxom vo forme voľne čitateľného textu a zákaz využívať funkcionalitu zapamätať heslo.

IS prevádzkovateľa boli chránené softvérovým zabezpečením – antivírusovom programom, ktorý odhaľoval prítomnosť škodlivého kódu na serveri, na lokálnych pracovných staniciach, takisto vyhodnocoval každý prichádzajúci e-mail. Prevádzkovateľ zabezpečil aj spamový filter. V podmienkach mesta bol využívaných legálny a prevádzkovateľom schválený softvér. Rovnako boli definované pravidlá sťahovania súborov z verejne prístupnej počítačovej siete, blokovaním nežiaducich webových sídiel prostredníctvom firewallu.

Povinnosť pre oprávnené osoby bezodkladne mazať reťazové a iné podozrivé emailové správy a spamy nebola ustanovená. V predpise nebolo zakázané oprávneným osobám otvárať súbory alebo makrá pripojené k správe elektronickej pošty od neznámeho alebo podozrivého odosielateľa, resp. súbory uložené v priečinku „nevyžiadaná pošta", tzv. spam. Taktiež predpis nezakazoval oprávnenej osobe posielať v prílohe správy súbory s príponou exe, com, bat, scr a pod.

Mesto taktiež prijalo opatrenia na prácu s pracovnou stanicou a prenosnými zariadeniami, ktorými boli povinnosť uzamykania kancelárií, politiku čistej obrazovky, uzamykania priestorov, v ktorých sa nachádzala IT, ak sa v nej nenachádzala oprávnená osoba, vypnutia IT po skončení pracovnej doby. Prenosné média museli byť uložené tak, aby nedošlo k poškodenie záznamu. Do mechaník prenosných pamäťových médií nesmeli byť vkladané poškodené média. Prenosné média obsahujúce osobné údaje boli skladované v uzamykateľných skriniach a trezoroch. Povinnosť kontrolovať prenosné média antivírusovým programom pri ich vkladaní alebo výslovnú povinnosť používateľa, ktorý z rôznych dôvodov pracuje na PC pridelenom inému používateľovi, prihlasovať sa do systému výlučne pod svojim užívateľským účtom nebola definovaná.

Mesto ako prevádzkovateľ IS nespracovával osobné údaje prostredníctvom mobilných prostriedkov IT.

Zásady prístupu do siete internet boli upravené nasledovne:

1. Prístup do siete internet využívať predovšetkým v súlade s pracovnou náplňou.
2. Zdržať sa činností, ktoré by viedli k poškodeniu dobrého mena pracoviska.
3. Komunikácia nie je chránená pred odpočúvaním. V prípade potreby prenosu dôverných údajov je nevyhnutné tieto riadne zabezpečiť ich šifrovaním.

Mesto nemonitorovalo činnosť zamestnancov na internete.

Mesto ako prevádzkovateľ kamerového IS malo firmou CUBS, s. r. o. vypracovanú Smernicu o používaní IS kamerový systém monitorujúci priestory prístupné verejnosti z 11.12.2018, ktorá vymedzovala základné pojmy súvisiace s používaním kamerového systému, určovala okruh oprávnených užívateľov, vymedzovala účel použitia kamerového systému v zmysle nariadenia GDPR a zákona o ochrane osobných údajov.

Smernica upravovala bezpečnostné pravidlá a podmienky pri práci s kamerovým systémom a pravidlá pri oprave kamerového systému v častiach rozsah povinností, oprávnení a činností jednotlivých oprávnených osôb pri obsluhe kamerového systému a v časti rozsahu zodpovednosti oprávnených osôb pri ochrane osobných údajov.

Priestor monitorovaný kamerovým systémom bol označený ako „Tento priestor je monitorovaný kamerovým systémom". Záznamy boli uchovávané 15 dní. Zamestnanci obsluhujúci kamerový systém mali postavenie oprávnenej osoby. Kamerový systém neobsluhovala externá firma.

Kamerový systém bol prevádzkovaný zamestnancami mesta, ktorí boli v postavení oprávnenej osoby. Mesto ako prevádzkovateľ kamerového systému nemonitorovalo svojich zamestnancov na pracovisku a zároveň nemonitorovala ich pohyb v služobných automobiloch pomocou GPS.

Odporúčanie:

- definovať v interných smerniciach opatrenia ako zákaz ponechávať dokumenty voľne odložené na chodbách, v rokovacích sálach a povinnosť pri práci s citlivými dokumentmi obsahujúcim osobitné kategórie údajov postupovať obozretnejšie,
- definovať v interných smerniciach napríklad konkrétne požiadavky na zložitosť hesla, zákaz používania autentizačných prostriedkov elektronickou poštou alebo faxom vo forme voľne čitateľného textu a zákaz využívať funkcionalitu zapamätať heslo,
- definovať v interných smerniciach povinnosť kontrolovať prenosné média antivírusovým programom pri ich vkladaní alebo výslovnú povinnosť používateľa, ktorý z rôznych dôvodov pracuje na PC pridelenom inému používateľovi, prihlasovať sa do systému výlučne pod svojim užívateľským účtom.

2.1.6 Bezpečnostné smernice a dokumentácia

Mesto prijalo dňa 03.01.2019 Smernicu o riešení bezpečnostných incidentov, ktorá upravovala pravidlá, postupy, riešenia a ohlasovanie bezpečnostných incidentov prevádzkovateľa na ÚOOÚ a dotknutým osobám. Smernica vo všeobecnosti obsahovala podrobnosti o postupe ako oprávnená osoba rozhodne, či porušenie ochrany osobných

údajov povedie alebo nepovedie k riziku pre práva a slobody fyzických osôb. Evidenciu porušení ochrany osobných údajov vedie zodpovedná osoba. V čase výkonu kontroly nedošlo u prevádzkovateľa k žiadnemu bezpečnostnému incidentu.

Mesto nemalo vypracované pravidlá na zavedenie pseudonymizačných techník na ochranu osobných údajov. Šifrovacie techniky sa využívali v prípade elektronickej dokumentácie s poštou – zaplatené platby (daň, rodičovské príspevky.

Mesto malo vypracovaných 57 záznamov o spracovateľských činnostiach prevádzkovateľa v rozsahu podľa čl. 30 nariadenia GDPR. Nastavenie lehoty uchovávania údajov bolo zabezpečené tak, aby boli archivované najviac dovtedy, kým je to potrebné na splnenie účelu. Lehoty na archiváciu údajov v jednotlivých IS boli totožné s registratúrnym poriadkom mesta.

2.1.7 Informačná bezpečnosť – bezpečnostné štandardy

Kontrolou bolo preverené, či prevádzkovateľ rešpektoval ustanovenie § 78 ods. 11 zákona č. 18/2018 Z. z. o ochrane osobných údajov, podľa ktorého by mal pri prijímaní bezpečnostných opatrení postupovať primerane podľa medzinárodných noriem a štandardov bezpečnosti. Mesto bolo v postavení povinnej osoby, ktorá zodpovedala za vytváranie, správu a rozvoj IS verejnej správy. Kontrola preverila najmä tie ustanovenia výnosu MF SR o štandardoch pre IS verejnej správy, ktoré súviseli s ochranou osobných údajov:

- štandardy pre architektúru riadenia (§ 29 až § 32 výnosu MF SR o štandardoch pre IS verejnej správy): riadenie informačnej bezpečnosti, personálna bezpečnosť, manažment rizík pre oblasť informačnej bezpečnosti a kontrolný mechanizmus riadenia informačnej bezpečnosti,
- štandardy minimálneho technického zabezpečenia (§ 33 až § 43 výnosu MF SR o štandardoch pre IS verejnej správy): ochrana proti škodlivému kódu, sieťová bezpečnosť, fyzická bezpečnosť a bezpečnosť prostredia, aktualizácia softvéru, monitorovanie a manažment bezpečnostných incidentov, periodické hodnotenie zraniteľnosti, zálohovanie, fyzické ukladanie záloh, riadenie prístupu, aktualizácia informačno-komunikačných technológií a účasť tretej strany.

Štandardom pre riadenie informačnej bezpečnosti mesta bolo podľa § 29 písm. a) výnosu MF SR o štandardoch pre IS verejnej správy vypracovanie bezpečnostnej politiky. Bezpečnostná politika musela byť zadefinovaná aspoň v rozsahu určenom výnosom MF SR o štandardoch pre IS verejnej správy vypracovanie bezpečnostnej politiky, schválená vedením mesta a daná na vedomie všetkým zamestnancom ako aj zainteresovaným stranám. V kontrolovanom období boli platné a účinné tieto dokumenty v oblasti bezpečnostnej politiky:

- bezpečnostný projekt na ochranu osobných údajov z 31.03.2014 v znení dodatku č. 1 z 26.04.2017,
- usmernenie na spracúvanie osobných údajov pre oprávnené osoby z 01.06.2018,
- smernica o ochrane osobných údajov z 11.12.2018,
- smernica o získavaní a manipulácii s osobnými údajmi z 13.12.2018,
- smernica o riešení bezpečnostných incidentov z 03.01.2019.

Zistenie č. 1:

Bezpečnostná politika mesta nebola vypracovaná v rozsahu podľa § 29 písm. a) výnosu MF SR o štandardoch pre IS verejnej správy, keď neobsahovala napríklad určenie špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti alebo určenie aktív, ktoré sú pre povinnú osobu kritické, čo ich ohrozuje a zásady ich ochrany.

Zistenie č. 2:

Mesto neustanovilo konkrétnu osobu zodpovednú za informačnú bezpečnosť, čo nebolo v súlade s § 29 ods. c) a d) výnosu MF SR o štandardoch pre IS verejnej správy.

Personálna bezpečnosť spracovania osobných údajov bola upravená v interných smerniciach mesta: smernica o riešení bezpečnostných incidentov a smernici o ochrane osobných údajov. Poučenie o bezpečnostnej politike a ochrane údajov zamestnancov mesta pred ich prvým vstupom do IS bolo realizované v rámci Poverenia a poučenia oprávnenej osoby.

Zistenie č. 3:

Mesto nemalo zavedený postup pre disciplinárne konanie v prípade porušenia bezpečnostnej politiky, čo nebolo v súlade § 30 písm. d) výnosu MF SR o štandardoch pre IS verejnej správy.

Zistenie č. 4:

Mesto nemalo vypracovaný dokument podľa štandardu pre manažment rizík pre oblasti informačnej politiky podľa § 31 výnosu MF SR o štandardoch pre IS verejnej správy. Neboli určené kritické procesy, ktoré by mohli prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných IS a vypracované plány na obnovu činnosti nefunkčných, poškodených alebo zničených kritických IS verejnej správy, čo nebolo v súlade s § 31 písm. d) a f) výnosu MF SR o štandardoch pre IS verejnej správy.

Mesto malo upravený kontrolný mechanizmu riadenia informačnej bezpečnosti v súlade s § 32 výnosu MF SR o štandardoch pre IS verejnej správy. Ochrana proti škodlivému kódu v podmienkach mesta bola upravená v týchto oblastiach: detekcia prítomnosti škodlivého kódu v prichádzajúcej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov, ochranu pred nevyžiadanou poštou prostredníctvom spamového filtra.

Mesto zaviedlo ochranu proti škodlivému kódu v prichádzajúcich e-mailoch, detekciu prítomnosti škodlivého kódu zabezpečenú antivírusovým softvér, kontrolu legálnosti softvéru prostredníctvom pravidelných aktualizácii. Mesto ako prevádzkovateľ nekontrolovalo prijímané súbory zo siete internet a nezaviedlo pravidlá pre sťahovanie súborov z externých sietí.

Mesto zabezpečovalo ochranu voči prístupu z vonkajšieho prostredia do IS a ochranu vnútorného prostredia formou hardvérových a softvérových firewallov. Evidenciu o všetkých miestach prepojenia sietí, ktoré boli v správe mesta vrátane prepojení s externými sieťami bola zabezpečovaná administrátorom IS.

Mesto malo v bezpečnostnom projekte vypracované a implementované pravidlá pre prácu v zabezpečenom priestore, bola zabezpečená ochrana pred výpadkom zdroja elektrickej energie, vypracované pravidlá pre vymazávanie, vyraďovanie a likvidáciu zariadení IS a všetkých záloh.

Interné smernice určili pravidlá pre narábanie s údajmi v elektronickej podobe, dokumentáciou systému a pamäťovými médiami tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu a modifikácii.

V bezpečnostnom projekte boli definované štandardy pre aktualizáciu softvéru, ktorá sa uskutočňovala pravidelne.

V podmienkach mesta bola vypracovaná smernica o riešení bezpečnostných, ktorá upravovala postup pri ohlasovaní bezpečnostných incidentov a ich evidenciu. Za bezpečnostné incidenty nebol považovaný podozrivý obsah na zázname z kamerového systému alebo strata mobilného prostriedku IT, keďže tieto prostriedky neboli pri spracúvaní osobných využívané.

Zistenie č. 5:

Mesto nemalo vypracovaný dokument podľa štandardu pre periodické hodnotenie zraniteľnosti, čo nebolo v súlade s § 38 výnosu MF SR o štandardoch pre IS verejnej správy, podľa ktorého štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS verejnej správy identifikovaných podľa bezpečnostnej politiky povinnej osoby s periodicitou najmenej raz ročne.

Archivácia a zálohovanie údajov jednotlivých IS sa prevádzala na server a na externé zariadenia. Prevádzkové zálohy – rozdielové boli uskutočňované na dennej báze a cez víkend boli uskutočňované kompletné zálohy v dvoch kópiách, ktoré boli uložené v uzamykateľných kanceláriách. Archivačné zálohy boli uskutočňované v súlade s § 39 písm. a) výnosu MF SR o štandardoch pre IS verejnej správy. Boli zadefinované údaje, ktoré povinne podliehali zálohovaniu (personálna a mzdová agenda a e-mailová pošta).

Zistenie č. 6:

Mesto nemalo vypracovaný dokument podľa štandardu pre riadenie prístupu podľa § 41 výnosu MF SR o štandardoch pre IS verejnej správy. Mesto neurčilo postup a zodpovednosť pre prideľovanie prístupových práv, nevypracovalo bezpečnostné zásady pre mobilné pripojenie do IS verejnej správy a pre prácu na diaľku a nevypracovalo pravidlá pre administrátorov systému, čo nebolo v súlade s § 41 výnosu MF SR o štandardoch pre IS verejnej správy.

Zistenie č. 7:

Mesto nemalo vypracovaný dokument podľa štandardu pre aktualizáciu informačno-komunikačných technológií podľa § 42 výnosu MF SR o štandardoch pre IS verejnej správy a dokument podľa štandardu pre účasť tretej strany podľa § 43 výnosu MF SR o štandardoch pre IS verejnej správy.

2.2 Výkon funkcie zodpovednej osoby

Do účinnosti nariadenia GDPR mesto malo určenú zodpovednú osobu (Mgr. Milan Ďurica), ktorá absolvovala skúšku na UOOÚ (potvrdenie o absolvovaní skúšky dňa 26.03.2014, č. 2128/2014). Poverená zodpovedná osoba bola interným zamestnancom mesta a vykonávala túto činnosť v rámci svojej pracovnej náplne. Jej bezúhonnosť bola zo strany mesta overená výpisom z registra trestov.

Po nadobudnutí účinnosti nariadenia GDPR vykonával funkciu zodpovednej osoby naďalej Mgr. Milan Ďurica, pričom poverenie výkonom funkcie zodpovednej osoby bolo vypracované až s účinnosťou od 10.12.2018. V súvislosti s postavením zodpovednej osoby od 25.05.2018 mesto zachovalo kontinuitu výkonu činnosti zodpovednej osoby, a to aj napriek legislatívne nedokonalej úprave jej činnosti v podmienkach mesta, nakoľko išlo o tú istú osobu.

Určená zodpovedná osoba bola zamestnancom mesta, mala vysokoškolské vzdelanie druhého stupňa a podľa prevádzkovateľa spĺňala odborné kvality a disponovala odbornými znalosťami v oblasti ochrany osobných údajov. V prípade, že v rámci ochrany osobných údajov bolo potrebné riešiť právne otázky, zabezpečoval súčinnosť právnik mesta a v prípade otázok týkajúcich sa informačných technológii zabezpečoval súčinnosť informatik.

Mesto v súlade s čl. 37 ods. 7 nariadenia GDPR zverejnilo kontaktné údaje zodpovednej osoby na svojom webovom sídle www.sabinov.sk v sekcii Transparentné mesto - Ochrana osobných údajov v rozsahu e-mailovej adresy a telefónneho čísla a oznámilo kontaktné údaje zodpovednej osoby ÚOOÚ prostredníctvom na to určeného webového rozhrania na stránke ÚOOÚ.

Zodpovedná osoba vykonávala kumulované činnosti vo funkcii referent pre civilnú ochranu, požiarnu ochranu a BOZP a bola odmeňovaná v rámci výkonu svojej pracovnej činnosti z vlastných zdrojov mesta. Podľa pracovnej náplne bola agenda uvedeného referátu začlenená do útvaru prednostu mestského úradu.

V rámci popisu pracovnej činnosti neboli zadefinované bližšie úlohy spojené s činnosťou zodpovednej osoby. Úlohy zodpovednej osobe vyplývali z jej poverenia odkazom na článok 39 nariadenia GDPR. Zodpovedná osoba bola na základe poverenia povinná vykonávať úlohy v súvislosti s ochranou osobných údajov len na základe pokynov primátora mesta (bod 2 a 3 poverenia) a bol jej zabezpečený prístup do všetkých IS. V podmienkach mesta neboli určené konkrétne pracovné pozície, ktoré by boli nezlučiteľné s funkciou zodpovednej osoby s cieľom eliminovať riziko konfliktu záujmov.

Zodpovedná osoba zabezpečovala v spolupráci s referátom pre personalistikou a mzdy poučenia oprávnených osôb pri nástupe do zamestnania a v rámci pridelenej agendy vypracovala usmernenie na spracúvanie osobných údajov pre oprávnené osoby. Svoju činnosť v oblasti poskytovania informácií a poradenstva zamestnancom nevedela preukázať, nakoľko o svojej činnosti neviedla žiadne záznamy. Z dôvodu, že zo strany dotknutých osôb neboli počas kontrolovaného obdobia podané žiadosti o výkon ich práv, zodpovedná osoba nevykazovala činnosť v predmetnej oblasti.

Odporúčanie:

NKÚ SR odporúča za účelom preukázateľnosti činnosti zodpovednej osoby vypracúvať priebežné výkazy činnosti a ročnú správu o svojej činnosti, vrátane vypracúvania písomných záznamov z každej komunikácie zodpovednej osoby s najvyšším vedením mesta.

2.3 Činnosť sprostredkovateľov

Mesto nemalo detailnejšie upravené pravidlá, ktoré by bližšie špecifikovali postup pri výbere sprostredkovateľa pri spracúvaní osobných údajov a pri uzatváraní zmluvy o sprostredkovaní tak, aby boli dodržané platnou legislatívou určené podmienky pre danú oblasť.

Pre mesto zabezpečovali činnosti, pri ktorých dochádza k spracúvaniu osobných údajov v mene prevádzkovateľa dva externé subjekty (sprostredkovatelia), a to DATALAN, a. s. v súvislosti s využívaním cloudových služieb a Združenie DEUS, ktoré neuzatvorilo s mestom sprostredkovateľskú zmluvu z dôvodu, že problematika spracovania osobných údajov bola s účinnosťou od 26.04.2018 upravená v článku 17 „Všeobecné zmluvné podmienky pre používanie služieb IS DCOM", ktoré sú neoddeliteľnou súčasťou Zmluvy o pripojení k informačnému systému Dátového centra obcí a miest zo 17.12.2015.

So sprostredkovateľom DATALAN, a. s. bola uzatvorená zmluva, ktorá riešila podmienky, za ktorých je sprostredkovateľ oprávnený zapojiť do spracúvania ďalšieho sprostredkovateľa. Súčasťou zmluvy bolo aj vymedzenie operácií s osobnými údajmi, ktoré má sprostredkovateľ povolené vykonávať. Kontrolou obsahových náležitostí sprostredkovateľskej zmluvy neboli zistené nedostatky.

Mesto ako prevádzkovateľ preverovalo záruky o primeraných technických a organizačných opatreniach na základe oboznámenia a zhodnotenia všetkých prijatých technických a organizačných opatrení zo strany sprostredkovateľa, resp. vychádzalo z vyhlásenia sprostredkovateľa (DEUS), že dodržiava technické a organizačné opatrenia v súlade s čl. 28 ods. 1 nariadenia GDPR. O preverení záruk nevyhotovovalo mesto žiadnu dokumentáciu.

Zároveň bolo mesto sprostredkovateľom voči obciam na základe zmluvy o zriadení spoločného obecného úradu na zabezpečenie úloh preneseného výkonu štátnej správy na týchto úsekoch: školstvo, úsek vodnej správy, ochrany ovzdušia, ochrany prírody a krajiny, územného plánovania, stavebného poriadku a bývania, cestnej dopravy a pozemných komunikácií a sociálnych služieb.

Sprostredkovateľské zmluvy boli uzatvárané bezodplatne, t. j. bez vzájomného finančného plnenia za výkon činností sprostredkovateľa.

Záver:

Mesto ešte pred účinnosťou nariadenia GDPR preskúmalo a identifikovalo IS, v ktorých spracúvalo osobné údaje za účelom ich zosúladenia s novou legislatívou platnou od 25.05.2018. Zároveň transparentným spôsobom na svojom webovom sídle informovalo dotknuté osoby o i právach a všetkých IS prevádzkovateľa, s uvedením ich právneho základu a účele spracovania osobných údajov.

Mesto nemalo vypracované pravidlá a postupy pre oprávnené osoby napríklad pre prípady, keď dochádzalo k získavaniu osobných údajov alebo uplatňovaniu práv dotknutých osôb, ale vychádzalo z jednotlivých ustanovení nariadenia GDPR. Kontrolou bolo ďalej zistené, že mesto vyžadovalo súhlasy dotknutých osôb so spracovaním osobných údajov aj pri výberových konaniach na voľné pracovné miesto v rámci predzmluvných vzťahov.

Do účinnosti nariadenia GDPR mesto malo určenú zodpovednú osobu z interných zamestnancov mesta, ktorá vykonávala túto funkciu aj po 25.05.2018. Dve organizácie bolo voči kontrolovanému subjektu v postavení sprostredkovateľa. Mesto ako spoločný obecný úrad bolo taktiež v pozícii sprostredkovateľa pre obce pri zabezpečovaní úloh preneseného výkonu štátnej správy.

V podmienkach mesta boli pre oprávnené osoby určené pravidlá a pokyny v interných smerniciach ako bezpečnostný projekt v znení dodatku č. 1, Smernici o ochrane osobných údajov a Smernici o používaní IS kamerový systém.

Ďalej bolo zistené, že mesto malo vypracovaných 57 záznamov o spracovateľských činnostiach prevádzkovateľa v rozsahu podľa čl. 30 nariadenia GDPR.

V prípade prijatých bezpečnostných opatrení boli zistené niektoré nedostatky, keď interné smernice neupravovali všetky požiadavky na štandardy pre architektúru riadenia a minimálneho technického zabezpečenia podľa výnosu MF SR o štandardoch pre IS verejnej správy. Napriek uvedenému však bola zabezpečená primeraná úroveň ochrany osobných údajov a kľúčových komponentov IS.

3 Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia GDPR

Kontrolou bolo preverené, koľko finančných prostriedkov vynaložil prevádzkovateľ na technické a organizačné opatrenia, na výkon funkcie zodpovednej osoby a na vzdelávanie v oblasti ochrany osobných údajov počas platnosti zákona č. 122/2013 Z. z. o ochrane osobných údajov v rokoch 2016 a 2017 a v súvislosti s plnením nových povinností vyplývajúcich z nariadenia GDPR v rokoch 2018 a 2019 (do 30.06.2019).

Prevádzkovateľ zabezpečoval oblasť ochrany osobných za obdobie rokov 2016 až 2019 vlastnými zamestnancami, ktorí boli v postavení oprávnených osôb. Mesto nemalo na zabezpečenie ochrany osobných údajov v rokoch 2016 až 2019 osobitne vyčlenených zamestnancov. Od 25.03.2013 vykonával funkciu zodpovednej osoby jeden zamestnanec s kumulovanými funkciami.

Mesto v kontrolovanom období nakúpilo skartovacie zariadenia v celkovej sume 708,00 eur a zabezpečilo kamerový systém na monitorovanie vstupu na parkovisko mestského úradu v sume 396,00 eur. Na vypracovanie bezpečnostnej dokumentácie bolo vynaložených 990,00 eur, a to v roku 2017 za aktualizáciu bezpečnostného projektu suma 190,00 eur a za vypracovanie posúdenia vplyvu na ochranu osobných údajov (personálne, organizačné a technické opatrenia) prevádzkovateľa suma 800,00 eur v roku 2018. Bezpečnostná dokumentácia bola vypracovaná firmou CUBS, s. r. o. Ochrana osobných údajov bola zabezpečovaná výlučne z vlastných zdrojov mesta.

Mesto pre oprávnené osoby zabezpečovalo pravidelné vzdelávanie v oblasti ochrany osobných údajov buď prostredníctvom zodpovednej osoby, firmy CUBS, s. r. o. (19.10.2018 bolo školených 55 oprávnených osôb) alebo školení organizovaných regionálnym vzdelávacím centrom. V roku 2019 boli bezodplatne školení štyria zamestnanci. Celková výška nákladov na vzdelávanie zamestnancov za kontrolované obdobie nielen v oblasti ochrany osobných údajov bola 17 760,84 eur.

Mesto za kontrolované obdobie nepožiadalo o navýšenie finančných prostriedkov z dôvodu zavedenia GDPR na zabezpečenie ochrany osobných údajov v IS.

Záver:

Mesto uhrádzalo výdavky na ochranu osobných údajov len z vlastných zdrojov, nežiadalo ďalšie subjekt o poskytnutie finančných zdrojov na ochranu osobných údajov. Finančné prostriedky na oblasť ochrany osobných údajov boli obmedzené.

Za kontrolnú skupinu dňa: 18.10.2019

Mgr. Lucia Vasičková ...
vedúca kontrolnej skupiny

Mgr. Ivana Petričová ...
členka kontrolnej skupiny

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

Ing. Michal Repaský ....
primátor mesta

Mesto SABINOV

Mestský úrad Sabinov, Námestie slobody 57, 083 01 Sabinov

Najvyšší kontrolný úrad Slovenskej republiky
Expozitúra Prešov
Obrancov mieru 6
081 92 Prešov

Váš list číslo/zo dňa	Naše číslo	Vybavuje	Sabinov
Z-008217/2019/1110VLB / 31.10.2019	27175/2019-ÚP	JUDr. Martin Judičák	18.11.2019

Vec
Prijaté opatrenia na odstránenie zistených nedostatkov

Mesto Sabinov na základe Protokolu Najvyššieho kontrolného úradu SR o výsledku kontroly systému ochrany a bezpečnosti údajov vo verejnom sektore KA-015/2019/1032 vykonanej v čase od 17.07.2019 do 18.10.2019 prijíma tieto opatrenia na odstránenie zistených nedostatkov.

Povinná osoba vyhovuje Vašej žiadosti a informácie poskytujeme v zákonnej lehote v nasledovnom znení:

1. Vypracovať bezpečnostnú politiku mesta v rozsahu podľa § 29 písm. a) výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

   Termín: 30.06.2020
   Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

2. Ustanoviť konkrétnu osobu zodpovednú za informačnú bezpečnosť v súlade s § 29 ods. c) a d) výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

   Termín: 30.06.2020
   Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

3. Zaviesť postup pre disciplinárne konanie v prípade porušenia bezpečnostnej politiky, čo nebolo v súlade § 30 písm. d) výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

   Termín: 30.06.2020
   Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

4. Vypracovať dokument podľa štandardu pre manažment rizík pre oblasti informačnej politiky podľa § 31 výnosu MF SR, určiť kritické procesy, ktoré by mohli prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných IS a vypracovať plány na obnovu činnosti nefunkčných, poškodených alebo zničených kritických IS verejnej správy v súlade s § 31

písm. d) a f) výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

Termín: 30.06.2020
Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

5. Vypracovať dokument podľa štandardu pre periodické hodnotenie zraniteľnosti v súlade s § 38 výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

   Termín: 30.06.2020
   Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

6. Vypracovať dokument podľa štandardu pre riadenie prístupu, určiť postup a zodpovednosť pre prideľovanie prístupových práv, vypracovať bezpečnostné zásady pre mobilné pripojenie do IS verejnej správy a pre prácu na diaľku a vypracovať pravidlá pre administrátorov systému v súlade s § 41 výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

   Termín: 30.06.2020
   Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

7. Vypracovať dokument podľa štandardu pre aktualizáciu informačno-komunikačných technológií podľa § 42 výnosu MF SR a dokument podľa štandardu pre účasť tretej strany podľa § 43 výnosu MF SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

   Termín: 30.06.2020
   Zodpovedný: JUDr. Judičák Martin, prednosta MsÚ

S pozdravom

MESTO SABINOV
Mestský úrad
083 17 Sabinov

Ing. Michal Repaský
primátor mesta