

Komisie Zastupiteľstva Bratislavského samosprávneho kraja

Materiál na rokovania komisií Zastupiteľstva
Bratislavského samosprávneho kraja

PRACOVNÝ NÁVRH

Informácia

**o kontrole Najvyššieho kontrolného úradu
„Systém ochrany a bezpečnosti údajov vo verejnom sektore“ (GDPR)**

Materiál bude prerokovaný v nasledovných komisiách:

Finančná komisia

Zodpovedná:

Ing. Patrícia Mešťan
riaditeľka
Úradu Bratislavského samosprávneho kraja

Spracovateľ:

Mgr. Dušan Slovák
referent CO, zodpovedná osoba (GDPR)

Bratislava
máj 2020

N á v r h u z n e s e n i a

UZNESENIE č. /2020

zo dňa 29. 05. 2020

Zastupiteľstvo Bratislavského samosprávneho kraja po prerokovaní materiálu

b e r i e n a v e d o m i e

Informáciu o kontrole Najvyššieho kontrolného úradu – „Systém ochrany a bezpečnosti údajov vo verejnom sektore“ (GDPR) a prijatých opatreniach

D ô v o d o v á s p r á v a

Na základe poverenia predsedu Najvyššieho kontrolného úradu Slovenskej republiky (ďalej len „NKÚ SR“) č. 1737/08 zo 4.7.2019 bola v čase od 8.7.2019 do 6.11.2019 vykonaná kontrola „Systém ochrany a bezpečnosti údajov vo verejnom sektore“ v Bratislavskom samosprávnom kraji (ďalej len „BSK“). Kontrola bola zameraná na dodržiavanie Nariadenia 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) a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

V súlade s §15 ods. 1 písm. g) zákona NR SR č.39/1993 o NKÚ SR v znení neskorších predpisov bol dňa 3. decembra 2019 prerokovaný protokol o výsledku kontroly „Systém ochrany a bezpečnosti údajov vo verejnom sektore“ (KA-015/2019/1032).

Celý proces kontroly bol vzhľadom na rozsiahlosť kontroly, ako aj požiadavky na poskytnutie najkomplexnejšieho pohľadu na úroveň kvality technických a organizačných opatrení a ostatných pravidiel prijatých v súvislosti s ochranou osobných údajov prevádzkovateľom (BSK) v súlade s nariadením (EÚ) a ostatnými vnútroštátnymi predpismi rozdelený do niekoľkých ucelených samostatných preverovaných oblastí:

1. Harmonizácia vnútroštátneho práva ochrany osobných údajov s Nariadením (EÚ) (úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR pre prevádzkovateľov)
2. Zabezpečenie osobných údajov občanov v databázach a informačných systémoch
3. Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa Nariadenia (EÚ)

Záver kontroly podľa protokolu o výsledku kontroly:

Záver k bodu č.1:

Podľa zistení kontrolnej skupiny NKÚ SR bolo Nariadenie (EÚ) pre prevádzkovateľa v zásade primerane zrozumiteľné, jasné a aplikovateľné aj bez externého právneho poradenstva. Zákon 18/2018 bol pre prevádzkovateľa neporovnateľne viac nejasný a neprehľadný ako Nariadenie (EÚ), čo bolo spôsobené najmä prevzatím viacerých článkov Nariadenia (EÚ), a najmä nejasne a neúplne ustanovenou pôsobnosť zákona 18/2018.

BSK využíval webovú stránku ÚOOÚ SR, z ktorej čerpal informácie obsiahnuté v metodických usmerneniach a ďalších dokumentoch. O metodickom Usmernení ÚOOÚ SR - kedy Nariadenie, kedy zákon, prevádzkovateľ mal vedomosť. Konzultácia BSK v posledných rokoch podľa predloženej dokumentácie len raz sa týkala riešenia otázok súvisiacich s vypracovaním Bezpečnostného projektu k 31.3.2014.e-mailom komunikoval s ÚOOÚ SR,

Záver k bodu č.2:

BSK síce zabezpečil vypracovanie „GAP analýzy“ (analýzy zhody) ale prijaté opatrenia na riešenie uvedených nedostatkov nesplnil do 25.05.2018, čím nezabezpečil súlad s Nariadením (EÚ) a zákonom 18/2018.

BSK nepostupoval v súlade s čl. 12 ods. 1 až 7 a čl. 24 ods. 1 a 2 Nariadenia (EÚ), keď nevypracoval pravidlá a nezdokumentoval pokyny pre oprávnené osoby, ktoré by komplexne riešili postupy pri získavaní osobných údajov, uplatňovaní práv dotknutých osôb a plnení oznamovacej povinnosti prevádzkovateľa v súvislosti s opravou a vymazaním osobných údajov alebo obmedzením spracúvania.

Niektoré pokyny a postupy pre oprávnené osoby boli upravené v Poverení oprávnenej osoby podľa zákona 18/2018, ale len veľmi všeobecne. Informácie a oznámenia pre dotknuté osoby boli zverejnené na webovom sídle prevádzkovateľa.

Preverením interných predpisov súvisiacich s ochranou osobných údajov bolo zistené, že prevádzkovateľ nevydal pokyny pre oprávnené osoby, ktoré by obsahovali podrobnosti o nakladaní s osobnými údajmi, ktoré prevádzkovateľ zaznamenal pri kontrolnej činnosti podľa § 9 ods.1 písm. b) zákona o BOZP.

Preverením interných predpisov súvisiacich s ochranou osobných údajov bolo zistené, že prevádzkovateľ nemal zdokumentované pokyny pre oprávnené osoby, ako postupovať pri sprístupňovaní informácií, ktoré obsahujú osobné údaje fyzických osôb podľa § 9 ods. 1 až 3 zákona o slobode informácií.

Kontrolou vzorky 5 zmlúv, ktoré mal prevádzkovateľ uzatvorené s externými subjektami a boli voči nemu v postavení sprostredkovateľa podľa čl. 28 Nariadenia (EÚ), bolo zistené, že kontrolované zmluvy boli vypracované v súlade s čl. 28 ods. 3 a 4 Nariadenia (EÚ). Prevádzkovateľ však nepreveroval, či sprostredkovatelia poskytujú dostatočné záruky, že osobné údaje budú bezpečne spracúvané v súlade s Nariadením (EÚ).

Prevádzkovateľ v rámci svojich IS prakticky dodržiaval bezpečnostné štandardy (§ 29 až § 43 výnosu MF SR), nedostatkom boli iba chýbajúce pravidlá alebo zdokumentované pokyny pre vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických systémov IS VS podľa § 31 písm. zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ podľa § 32 písm. b), zabezpečenie aktualizácií inštalovaného ochranného softvéru podľa štandardu pre aktualizáciu SW v súlade s § 36 a umožnenie fyzickým osobám.

Záver k bodu č.3:

BSK na zabezpečenie ochrany osobných údajov v rokoch 2016 - 2017 vynaložil finančné prostriedky v celkovej sume 38 859,13€ vrátane vzdelávacích aktivít a výdavkov na zodpovednú osobu.

Od 01.01.2018 do 30.06.2019 BSK vynaložil na zabezpečenie ochrany osobných údajov finančné prostriedky v celkovej sume 39 291, 1 O Eur vrátane vzdelávacích aktivít a výdavkov na zodpovednú osobu.

BSK do roku 2017 a ani po 25.05.2018 neboli navýšené finančné prostriedky zo ŠR z dôvodu zabezpečenia ochrany osobných údajov a povinností podľa zákona 122/2013 a ani povinností vyplývajúcich z Nariadenia (EÚ) a zákona 18/2018. BSK si nežiadal o navýšenie finančných prostriedkov.

Prijaté opatrenia na odstránenie kontrolou zistených nedostatkov.

Na základe výsledkov kontroly, uvedených v protokole o výsledku kontroly NKÚ SR BSK prijíma opatrenia na odstránenie kontrolou zistených nedostatkov v oblasti posúdenia bilančného testu pri spracovaní osobných údajov kamerovým systémom, dopracovania interných noriem v zmysle čl.24 ods. 1 a 2 Nariadenia (EÚ), dopracovania internej normy pri aplikácii ustanovenia § 9 ods. 1 až 3 zákona o slobode informácií. Doplnenia internej smernice v oblasti BOZP o podrobnosti o nakladaní s osobnými údajmi, ktoré boli zaznamenané pri kontrolnej činnosti. Preverenie sprostredkovateľov, či prijali primerané technické a organizačné opatrenia v súlade s Nariadením (EÚ). Určenia manažéra bezpečnosti v súlade § 78 ods.11 zákona č.18/2018 a dobrou praxou (Best Practice). Aktualizovať internú smernicu pre sieťovú bezpečnosť so zapracovaním pravidiel (pokynov) podľa štandardov pre sieťovú bezpečnosť podľa §34 výnosu MF SR.

V súlade s prijatými opatreniami na odstránenie kontrolou zistených nedostatkov bola už schválená nová Smernica č.100/2019 o bezpečnostných zásadách pri používaní VT a IS a postupoch zabezpečujúcich prevádzku VT a IS Úradu Bratislavského samosprávneho kraja (ďalej len „Ú BSK“).

Vykonaná kontrola ani prijaté opatrenia nemajú dopad na finančný rozpočet BSK.

NKÚ SR pri prerokovaní protokolu konštatoval, že BSK si plní povinnosti súvisiace s ochranou osobných údajov a prijaté opatrenia by sa mali zamerať najmä na dopracovanie interných aktov riadenia popisujúcich jednotlivé spracovateľské činnosti oprávnenými osobami. V súlade so Zápisnicou o prerokovaní protokolu o výsledku kontroly boli prijaté opatrenia na odstránenie kontrolou zistených nedostatkov a boli predložené NKÚ SR v stanovenom termíne (do 31.03.2020). Úrad BSK akceptoval všetky odporúčania

k jednotlivým kontrolným zisteniam, ktoré pretransformoval do návrhu opatrení zaslaných na NKÚ SR. Ku dňu predloženia tohto materiálu nebolo Úradu BSK doručené nesúhlasné stanovisko NKÚ SR a ani návrh na doplnenie navrhovaných opatrení.

Úrad BSK v súlade so závermi o prerokovaní protokolu o výsledku kontroly predkladá informáciu o výsledku kontroly a prijatých opatreniach zastupiteľstvu BSK.