

# NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo: Z-007846/2019/1090/BJB  
Číslo poverenia: 1737/38  
Zo dňa: 04.07.2019

Počet výtlačkov: 2  
Výtlačok číslo: 2  
Počet strán: 17  
Počet príloh: 0



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

Košický samosprávny kraj

---

Košice, október 2019

Zoznam použitých skratiek.....	3
Zhrnutie: .....	4
1. Harmonizácia vnútroštátneho práva ochrany OÚ s Nariedením EÚ 2016/679.....	7
2. Zabezpečenie OÚ občanov v databázach a informačných systémoch.....	8
2.1 Interné akty riadenia organizácie.....	8
2.2 Analýza procesov a povinností vyžadovaných podľa GDPR.....	8
2.3 Právny základ – pravidlá a postupy.....	9
2.4 Práva dotknutej osoby – pravidlá, postupy a oznámenia.....	10
2.5 Základné pravidlá a pokyny pre bezpečné spracúvanie údajov.....	10
2.6 Bezpečnostné smernice a dokumentácia.....	14
2.7 Informačná bezpečnosť – bezpečnostné štandardy.....	14
3. Výkon funkcie zodpovednej osoby.....	15
4. Činnosť sprostredkovateľov.....	16
5. Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia.....	17

Zoznam použitých skratiek

Skrátený názov	Úplné znenie
analýza	Analýza a zabezpečenie súladu ochrany OÚ s požiadavkami GDPR
smernica	Smernica Košického samosprávneho kraja na ochranu OÚ, účinná od 23.01.2019
BOZP	bezpečnosť a ochrana zdravia pri práci
EÚ	Európska únia
IB	Informačná bezpečnosť
IS	informačný systém
IT	informačné technológie
GDPR	General Data Protection Regulation (Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní OÚ a o voľnom pohybe takýchto údajov)
KSK, prevádzkovateľ, kontrolovaný subjekt, nariadenie GDPR	Košický samosprávny kraj Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní OÚ 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	osobný údaj
poverenie	Poverenie a poučenie prevádzkovateľa
ÚOOÚ SR	Úrad na ochranu OÚ Slovenskej republiky
Výnos MF SR	Výnos č. 55 Ministerstva financií Slovenskej republiky zo 4. marca 2014, o štandardoch pre informačné systémy verejnej správy
zákon o ochrane OÚ	Zákon č. 18/2018 Z. z. o ochrane OÚ a o zmene a doplnení niektorých zákonov
zákon o ochrane OÚ (2013)	Zákon č. 122/2013 Z. z. o ochrane OÚ a o zmene a doplnení niektorých zákonov



**Zhrnutie:**

Kontrola systému ochrany a bezpečnosti údajov vo verejnom sektore bola do plánu kontrol na rok 2019 zaradená z dôvodu preverenia implementácie nového právneho rámca ochrany OÚ – Nariadenia EÚ, ktoré nadobudlo účinnosť 25.05.2016. Nariadenie má charakter európskeho zákona, ktoré bolo priamo účinné, vykonateľné a uplatniteľné na území každého členského štátu EÚ, bez nutnosti prijatia vnútroštátnych vykonávacích predpisov. Nariadenie GDPR dáva členským štátom možnosť upraviť len niektoré jeho články v zmysle národných špecifik. Dňom 25.5.2018 došlo k zrušeniu dovtedy platnej smernice 95/46/ES a k zrušeniu zákona č. 122/2013 Z. z., ktorý bol s účinnosťou od 25.5.2018 nahradený zákonom o ochrane OÚ a doplnil nariadenia GDPR na národnej úrovni.

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

Kontrola bola zameraná najmä na overenie existencie príslušných interných aktov riadenia, dokumentov, primeraných postupov a opatrení a ich kvalitatívnu úroveň. Pri kontrole bolo použitých viacero metód a techník: štúdium právnych predpisov EÚ, všeobecne – záväzných právnych predpisov, interných predpisov, preskúmanie predložených dokladov a dokumentácie, analýza, dedukcia, rozhovor a výberové zisťovanie.

Kontrolou bolo zistené:

**Harmonizácie vnútroštátneho práva ochrany OÚ s Nariadením GDPR**

Účelom kontroly v oblasti Harmonizácie vnútroštátneho práva ochrany OÚ s Nariadením GDPR bolo preveriť, či legislatíva súvisiaca s ochranou OÚ a usmernenia ÚOOÚ SR boli pre prevádzkovateľa zrozumiteľné.

KSK využíval webovú stránku ÚOOÚ SR na získanie informácií o ochrane OÚ. Z pohľadu kontrolovaného subjektu bolo usmernenie "Kedy Nariadenie a kedy zákon o ochrane OÚ", ako celok jasné, zrozumiteľné a aplikovateľné, dokázal ho aplikovať a implementovať v praxi.

Nariadenie (EÚ) 2016/679 (GDPR) nie je podľa vyjadrenia KSK prehľadné, jasné a zrozumiteľné, aby ho bolo možné bez problémov aplikovať v praxi. Právne predpisy týkajúce sa OÚ KSK v kontrolovanom období aplikoval KSK v praxi bez toho, aby požiadal o metodické usmernenie ÚOOÚ SR. Podľa vyjadrenia KSK je možné správne implementovať a aplikovať nariadenie GDPR a zákon o ochrane OÚ aj bez externého právneho poradenstva, resp. odborného poradenstva napr. odborníka na IT. ÚOOÚ SR v KSK nevykonával kontrolu spracúvania OÚ.

**Zabezpečenie OÚ občanov v databázach a informačných systémoch**

Preverovaním v oblasti zabezpečenia OÚ občanov v databázach a informačných systémoch KSK mal vypracovaný organizačný poriadok vrátane organizačnej štruktúry a pracovný poriadok. Dokumenty boli v čase výkonu kontroly platné a účinné. Interný predpis upravujúci konanie a postup pri predkladaní a uchovávaní majetkových priznaní zamestnancov mal vypracovaný, predpis však neobsahoval ustanovenie, že majetkové priznania nie sú súčasťou osobných spisov zamestnancov. Ďalej subjekt mal vypracovaný registratúrny poriadok a interný predpis upravujúci pravidlá a postup pri zverejňovaní zmlúv.

Pred nadobudnutím účinnosti nariadenia bol prevádzkovateľ povinný analyzovať technické a organizačné opatrenia v oblasti ochrany OÚ prijatých v zmysle zákona č. 122/2013 Z. z. V súvislosti so zavedením GDPR externá spoločnosť pre prevádzkovateľa vypracovala Analýzu a zabezpečenie súladu ochrany OÚ s požiadavkami GDPR. Výsledkom bolo vypracovanie Smernice Košického samosprávneho kraja o ochrane OÚ, ktorá bola v súlade s nariadením GDPR s účinnosťou 23.1.2019. Prevádzkovateľ nekonal v súlade s čl. 1 ods. 1 nariadenia GDPR tým, že do doby jeho účinnosti, nedal do súladu pravidlá ochrany fyzických osôb pri spracovaní OÚ a pravidlá týkajúce sa voľného pohybu OÚ. Podľa vyjadrenia kontrolovaného subjektu v čase od 25.05.2018 do 23.01.2019, keď nebola dokumentácia v súlade s nariadením GDPR nebol zaznamenaný žiaden bezpečnostný incident.



KSK mala vypracované pravidlá, podľa ktorých postupujú oprávnené osoby prevádzkovateľa, ak je právnym základom spracúvania OÚ súhlas dotknutej osoby. Pravidlá obsahujú podrobnosti o tom, že oprávnená osoba je povinná v rámci písomného vyhlásenia oddeliť udelenie súhlasu dotknutej osoby na spracúvanie OÚ od iných skutočností.

Prevádzkovateľ preukázal, že oprávnené (poverené) osoby boli poučené, že pri získavaní OÚ priamo od dotknutej osoby sú povinné ju informovať, zverejniť informácie určené dotknutým osobám v požadovanom rozsahu a forme o jednotlivých právach, ktoré si môžu u prevádzkovateľa uplatniť. Kontrolou bolo zistené, že prevádzkovateľ mal vypracované pravidlá a postup pre prípady, ak by si dotknutá osoba uplatnila právo na prístup k svojim OÚ. Oprávnené osoby boli poučené prostredníctvom záznamu o poučení oprávnenej osoby, ako majú postupovať.

KSK má vypracovanú internú smernicu upravujúcu základné pravidlá a pokyny pre bezpečné spracúvanie OÚ oprávnenými osobami, pravidlá a pokyny pre oprávnené osoby pri spracovaní údajov v papierovej forme, pravidlá a pokyny pre oprávnené osoby – identifikácia a autentizácia, pravidlá a pokyny pri práci s pracovnou stanicou, pravidlá a pokyny pre oprávnené osoby pri práci mobilnými prostriedkami IT, pravidlá a postupy pri práci s prenosnými médiami, pravidlá pri používaní internetu a elektronickej pošty bezpečnostné pravidlá a podmienky pri práci s kamerovým systémom a pri servise kamerového systému.

Preverovaním oblasti zabezpečenia OÚ občanov v databázach a informačných systémoch kontrolná skupina nezistila nedostatky, ktoré by mali za následok riziká v spracovaní a ochrane OÚ.

#### **Výkon funkcie zodpovednej osoby**

Preverovaním dodržiavania § 23 a § 24 zákona 122/2013 Z. z a čl. 37 ods. 1, písm. a) nariadenia GDPR ustanoviť ZO bolo zistené, že KSK v období pred 25. 05. 2018 mal ustanovenú ZO, ktorá úspešne absolvovala skúšku na ÚOOÚ SR a predložila potvrdenie o jej absolvovaní. Od 25.05.2018 kontrolovaný subjekt určil tri ZO. V období pred účinnosťou GDPR, do 25.05.2018, ani po nadobudnutí jeho účinnosti, nežiadal prevádzkovateľ finančné prostriedky na ich činnosť. Informácie o ZO v súlade s čl. 37 ods. 7 GDPR zverejnil KSK na svojom webovom sídle. Informácie o ZO boli na ÚOOÚ SR oznámené dňa 24.05.2018. Bezúhonnosť ZO KSK nepreveroval z dôvodu, že ZO boli zamestnancami KSK, do funkcie boli ZO ustanovené na základe odborných znalostí a kvalít.

ZO iniciovali úpravy interných noriem so zapracovaním opatrení na zabezpečenie OÚ. Mali možnosť vstupovať len do IS obsahujúcich údaje potrebné na plnenie ich úloh. Mali zamedzený vzdialený prístup do IS obsahujúcich OÚ organizácie. Zúčastňovali na zasadnutí vedenia ÚKSK, na ktorých sa riešili otázky súvisiace s ochranou OÚ a informačnou bezpečnosťou, ďalej iniciovali odporúčanie na zmenu smernice o ochrane OÚ a ďalšie interné normy, zabezpečenie dodržiavania štandardov informačnej bezpečnosti, návrh rozpočtu vo vzťahu k IB. Poskytovali konzultácie: - v oblasti sociálnej agendy, školstva, sprostredkovateľských zmlúv, športu, SAP R/3, registratúry, poverení, spracovateľských operácií, vyššiemu manažmentu a iným zamestnancom v súvislosti s ochranou OÚ a vypracúvali výkazy činnosti, ktoré boli potvrdené na prístupových formulároch pre ZO.

KSK nevymedzila pozície v organizačnej štruktúre, ktoré sú nezlučiteľné s výkonom funkcie ZO. Zodpovedné osoby podľa popisov pracovných činností plnia aj iné úlohy a povinnosti. Kontrolná skupina NKÚ SR zisťovala, či úlohy, ktoré ZO vykonávajú, nevedli ku konfliktom záujmov. Preverovaním nebolo zistené, že by činnosti ZO viedli ku konfliktu záujmov. Podľa vyjadrení kontrolovaného subjektu ZO nevykonávali v kontrolovanom období funkciu ZO pre subjekty v súkromnom sektore alebo vo verejnej správe.

#### **Činnosť sprostredkovateľov**

KSK v kontrolovanom období mal vypracované pravidlá (smernicu), podľa ktorých oprávnené osoby postupujú pri príprave a uzatváraní zmlúv so sprostredkovateľmi. V kontrolovanom období boli tri spoločnosti voči KSK v úlohe sprostredkovateľov. Kontrolou obsahu uzatvorených zmlúv neboli zistené nedostatky. Sprostredkovateľské zmluvy boli k účinnosti nariadenia GDPR aktualizované.

KSK podľa vyjadrenia nepreveroval sprostredkovateľov, či poskytujú dostatočné záruky na to, že príjmu primerané technické a organizačné opatrenia v súlade s GDPR, spoliehal sa na ich vyhlásenie.



Podmienkami v zmluvách bolo zabezpečené, že každá fyzická osoba konajúca na základe poverenia, ktorá má prístup k osobným údajom, spracúva tieto OÚ len na základe pokynov prevádzkovateľa. Prevádzkovateľ uzatvorené sprostredkovateľské zmluvy preskúmal a posúdil a konštatoval, že sprostredkovateľ si sám neurčil účely a prostriedky spracúvania OÚ. Uzatvorené sprostredkovateľské zmluvy obsahovali podmienky a náležitosti uvedené v čl. 28 nariadenia GDPR a to, že sprostredkovateľ nezapoji ďalšieho sprostredkovateľa bez písomného povolenia prevádzkovateľa. KSK nemal uložené OÚ v externých úložiskách (cloud), resp. nevyužíval služby aplikácií alebo programov uložených na serveroch na webe (cloud computing).

#### **Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia**

Kontrola NKÚ SR preverila výšku finančných prostriedkov, ktoré prevádzkovateľ vynaložil na technické a organizačné opatrenia súvisiace s plnením povinností vyplývajúcich z nariadenia GDPR.

V rokoch 2016 a 2017 neboli KSK poskytnuté finančné prostriedky štátom na zabezpečenie ochrany OÚ a povinností vyplývajúcich zo zákona č. 122/2013 Z. z. ÚKSK žiadal z dôvodu zavedenia GDPR na plnenie nových povinností vyplývajúcich z GDPR od 25.5.2018 o navýšenie finančných prostriedkov na zabezpečenie ochrany OÚ v IS na rok 2018, resp. od 25.5.2018 (na roky 2019, 2020). Požiadavka bola predložená na rokovaní zastupiteľstva KSK. Požadované finančné prostriedky neboli poskytnuté.

KSK v kontrolovanom období zabezpečil pre oprávnené osoby vzdelávanie v oblasti ochrany OÚ a posilňoval ich povedomie v súvislosti s plnením povinností, ktoré im vyplývajú z GDPR. Oprávnené osoby sa zúčastnili na seminároch, konferenciách k problematike GDPR. Náklady na vzdelávanie predstavovali 381,00 eur.

Z dôvodu plnenia nových povinností vyplývajúcich z GDPR štát neposkytol prevádzkovateľovi finančné prostriedky určené na zabezpečenie ochrany OÚ v IS v rokoch 2018 (od 25. 5. 2018) a 2019.

Čo sa týka dostatočnosti finančných prostriedkov a ľudských zdrojov, podľa vyjadrenia kontrolovaného subjektu chýbajú na zabezpečenie ochrany OÚ finančné prostriedky aj ľudské zdroje. KSK plne hradila náklady za plnenie povinností súvisiacich s prevádzkovaním IS, ktoré na ňu preniesol štát, zo svojho rozpočtu.

V súvislosti s plnením povinností zabezpečenia ochrany OÚ vyplývajúcich z nariadenia GDPR zaobstaral prevádzkovateľ v rokoch 2018 a 2019 technické prostriedky na posilnenie bezpečnosti OÚ v sume 60 352,75 eur. Na činnosť sprostredkovateľov KSK nevynaložil v kontrolovanom období žiadne finančné prostriedky.

## Najvyšší kontrolný úrad Slovenskej republiky

Podľa poverenia predsedu NKÚ SR č. 1737/38 z 4.7.2019 vykonali:

Ing. Jana Beňová – vedúca kontrolnej skupiny

Ing. Tomáš Tokár – člen kontrolnej skupiny

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

Kontrola bola vykonaná v čase od 02.08.2019 do 30.09.2019 v kontrolovanom subjekte

Košický samosprávny kraj, Námestie Maratónu mieru 1, 042 66 Košice-Staré mesto, IČO 35541016

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 OÚ s nariadením GDPR,
- finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia GDPR,
- zabezpečenie OÚ občanov v databázach a IS.

Kontrola bola zameraná najmä na overenie existencie príslušných interných aktov riadenia, dokumentov, primeraných postupov a opatrení a ich kvalitatívnu úroveň. 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, dedukcia, rozhovor, výberové zisťovanie a pod.

### Charakteristika kontrolovaného subjektu



Košický samosprávny kraj vznikol na základe Zákona č. 416/2001 Z. z. o prechode niektorých pôsobností z orgánov štátnej správy na obce a vyššie územné celky. Historicky prvé zasadnutie Zastupiteľstva KSK sa uskutočnilo 19. decembra 2001. Sídli v historickej budove Divízie na Námestí Maratónu mieru 1 v Košiciach. Úrad KSK je výkonným orgánom Zastupiteľstva KSK a predsedu KSK. S počtom obyvateľov 799 217 je druhým najväčším krajom na Slovensku. Leží na juhovýchode Slovenska. Medzi najvýznamnejšie kultúrno-historické pamiatky mesta Košíc patria: Ochtinská aragonitová jaskyňa, Dobšinská ľadová jaskyňa, Domica, Jasovská jaskyňa, Gombasecká jaskyňa, vodná nádrž Zemplínska šírava, Herlianský gejzír, hrad Krásna Hôrka, kaštieľ Betliar,

Slovenský raj, Spišský hrad a okolie, lyžiarske stredisko Plejsy, Vinianske jazero, Morské oko, Košice – Kavečany, kde sa nachádza najväčšia ZOO na Slovensku a svojou rozlohou aj v strednej Európe (288 ha), drevené kostolíky v Ruskej Bystrej (UNESCO) a Inovce, klimatické kúpele Štós. Región dolného Zemplína vo východnej časti Košického kraja charakterizuje najmä vynikajúce tokajské víno.



Počas výkonu kontroly bolo zistené:

V kontrolovanom období mal KSK vypracované interné akty riadenia, podľa ktorých oprávnené osoby a ZO postupovali pri práci s OÚ. Smernica o ochrane OÚ upravuje ochranu OÚ spracovávaných KSK. Upravuje súhrn pravidiel, ktoré je potrebné dodržiavať pre zachovanie dôvernosti, dostupnosti a integrity spracúvaných OÚ a tiež povinnosti zamestnancov prevádzkovateľa tak, aby boli OÚ chránené v súlade s nariadením a zákonom a nedochádzalo k narušeniu práv a slobôd dotknutých osôb.

## **1. Harmonizácia vnútroštátneho práva ochrany OÚ s Nariadením GDPR**

### **1.1 Úroveň zrozumiteľnosti legislatívy a usmernení ÚOOÚ SR pre prevádzkovateľov**

Účelom kontroly v preverovanej oblasti bolo zistiť, či legislatíva, súvisiaca s ochranou OÚ a usmernenia ÚOOÚ SR boli pre prevádzkovateľa zrozumiteľné.

KSK využíval webovú stránku ÚOOÚ SR na získanie informácií o ochrane OÚ. Z pohľadu kontrolovaného subjektu bolo usmernenie "Kedy Nariadenie a kedy zákon o ochrane OÚ", ako celok jasné, zrozumiteľné a aplikovateľné, dokázal ho aplikovať a implementovať v praxi. Nariadenie (EÚ) 2016/679 (GDPR) nie je podľa vyjadrenia KSK prehľadné, jasné a zrozumiteľné, aby ho bolo možné bez problémov aplikovať v praxi. Právne predpisy týkajúce sa OÚ KSK v kontrolovanom období aplikoval KSK v praxi bez toho, aby požiadal o metodické usmernenie ÚOOÚ SR. Podľa jeho vyjadrenia je možné správne implementovať a aplikovať nariadenie GDPR a zákon o ochrane OÚ aj bez externého právneho poradenstva, resp. odborného poradenstva napr. odborníka na IT. ÚOOÚ SR v KSK nevykonával kontrolu spracúvania OÚ.

#### **Záver:**

Účelom kontroly v preverovanej oblasti bolo preveriť, či legislatíva súvisiaca s ochranou OÚ a usmernenia ÚOOÚ SR boli pre prevádzkovateľa zrozumiteľné.

KSK využíval webovú stránku ÚOOÚ SR na získanie informácií o ochrane OÚ. Z pohľadu kontrolovaného subjektu bolo usmernenie "Kedy Nariadenie a kedy zákon o ochrane OÚ?", ako celok jasné, zrozumiteľné a aplikovateľné, dokázal ho aplikovať a implementovať v praxi. Nariadenie (EÚ) 2016/679 (GDPR) nie je podľa vyjadrenia KSK prehľadné, jasné a zrozumiteľné, aby ho bolo možné bez problémov aplikovať v praxi. KSK v kontrolovanom období I KSK aplikoval právne predpisy týkajúce sa OÚ v praxi bez toho, aby požiadal o metodické usmernenie ÚOOÚ SR. ÚOOÚ SR v KSK nevykonával kontrolu spracúvania OÚ.

## **2. Zabezpečenie OÚ občanov v databázach a informačných systémoch**

### **2.1 Interné akty riadenia organizácie**

KSK mala vypracovaný organizačný poriadok vrátane organizačnej štruktúry aj pracovný poriadok. Dokumenty boli v čase výkonu kontroly platné a účinné. Interný predpis upravujúci konanie a postup pri predkladaní a uchovávaní majetkových priznaní zamestnancov mal vypracovaný, predpis neobsahoval ustanovenie, že majetkové priznania v zmysle § 114 ods. 8 zákona č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov nie sú súčasťou osobných spisov zamestnancov. Ďalej subjekt mal vypracovaný registratúrny poriadok, interný predpis upravujúci pravidlá a postup pri zverejňovaní zmlúv, objednávok a faktúr, interný predpis upravujúci konanie a postup pri sprístupňovaní informácií podľa zákona o slobode informácií a interný predpis upravujúci pravidlá bezpečnosti a ochrany zdravia pri práci. Registratúrny poriadok obsahuje podrobnosti o postupe pri spracovaní elektronických registratúrnych záznamoch. Elektronický IS na správu registratúry spĺňa štandardy podľa výnosu MV SR č. 525/2011 Z. z. t. j., že KSK požiadal o posúdenie zhody a disponuje certifikátom MV SR.

**Záver:** Preverením existencie a správnosti interných aktov riadenia KSK neboli zistené nedostatky.

**Odporúčanie:** Kontrolná skupina NKÚ SR odporúča doplniť do smernice ustanovenie, že majetkové priznania nie sú súčasťou osobných spisov zamestnancov.



## 2.2 Analýza procesov a povinností vyžadovaných podľa GDPR

Pred nadobudnutím účinnosti nariadenia bol prevádzkovateľ povinný analyzovať technické a organizačné opatrenia v oblasti ochrany OÚ prijatých v zmysle zákona č. 122/2013 Z. z. V súvislosti so zavedením GDPR externá spoločnosť pre prevádzkovateľa vypracovala Analýzu a zabezpečenie súladu ochrany OÚ s požiadavkami GDPR. Spracovateľ analýzy preskúmal všetky IS, v ktorých prevádzkovateľ spracováva OÚ a analyzoval, či spracovanie v každom z nich je zákonné aj podľa GDPR, či OÚ sú spracované v každom IS len na výslovne uvedený a legitímny účel, či údaje spracované v každom IS sú relevantné, primerané a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účel ich spracovania, či sú v IS uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na plnenie účelu ich spracovania, či v jednotlivých IS, posudzujúc podľa GDPR, je zaručená primeraná bezpečnosť spracúvaných OÚ. Ďalej preskúmal, či všetky informačné IS, v ktorých spracováva OÚ a analyzoval, či OÚ v rámci IS nespracúva v mene prevádzkovateľa iný subjekt, pričom tento subjekt nemá postavenie sprostredkovateľa a identifikovala zmeny, ktoré je potrebné vykonať na uvedenie spracúvania do súladu s GDPR. Na záver identifikoval zásadné riziká a návrhy na prijatie opatrení pre zabezpečenie súladu s požiadavkami nariadenia GDPR. Napr. medzi opatrenia na úrovni strategického riadenia patrili zabezpečiť dostatočný počet osôb, ktoré by sa venovali informačnej a kybernetickej bezpečnosti, bez toho, aby plnili aj iné úlohy, pravidelne a najmä pri každej podstatnej zmene v rámci organizačnej štruktúry, v prípade legislatívnych zmien, zmien na úrovni výkonu jednotlivých agend a pod., aktualizovať zverejnené informácie na webovom sídle KSK v rámci informačnej povinnosti a povinnosti zverejňovania informácií v súlade s § 60 ods. 1 zákona o ochrane OÚ.

Výsledkom bolo vypracovanie Smernice Košického samosprávneho kraja o ochrane OÚ, ktorá bola v súlade s nariadením GDPR s účinnosťou 23.1.2019. Zároveň bola zrušená smernica č. 3/2014 z 31.03.2014.

### Kontrolné zistenie č.1:

Prevádzkovateľ nekonal v súlade s čl. 1 ods. 1 nariadenia GDPR tým, že do doby jeho účinnosti, nedal do súladu pravidlá ochrany fyzických osôb pri spracovaní OÚ a pravidlá týkajúce sa voľného pohybu OÚ. Z dôvodu, že kontrolné zistenie bolo v čase kontroly odstránené, nemá kontrolovaný subjekt povinnosť prijať opatrenie.

Preverené boli všetky zmluvy so sprostredkovateľmi a boli dané do súladu s GDPR, všetky IS, v ktorých spracováva subjekt OÚ a analyzoval, v ktorých IS je potrebné vykonať "posúdenie vplyvu na ochranu údajov". Na základe zmluvy o dielo KSK uhradil za spracovanú analýzu 56 160,00 eur s DPH.

### Záver:

Prevádzkovateľ prostredníctvom externej spoločnosti zabezpečil vykonanie analýzy technických a organizačných opatrení v oblasti ochrany OÚ prijatých v zmysle zákona č. 122/2013 Z. z. Spracovateľ analýzy preskúmal všetky IS, v ktorých prevádzkovateľ spracováva OÚ a analyzoval, či spracovanie v každom z nich je zákonné aj podľa GDPR, či OÚ sú spracované v každom IS len na výslovne uvedený a legitímny účel, či údaje spracované v každom IS sú relevantné, primerané a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účel ich spracovania, či sú v IS uchovávané vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na plnenie účelu ich spracovania, či v jednotlivých IS, posudzujúc podľa GDPR, je zaručená primeraná bezpečnosť spracúvaných OÚ. Na záver identifikovala zásadné riziká a návrhy na prijatie opatrení pre zabezpečenie súladu s požiadavkami nariadenia GDPR.

V kontrolovanej oblasti bolo identifikované kontrolné zistenie, do doby účinnosti nariadenia GDPR a zákona o ochrane OÚ, KSK nedal do súladu pravidlá ochrany fyzických osôb pri spracovaní OÚ a pravidlá týkajúce sa voľného pohybu OÚ.



## 2.3 Právny základ spracúvania OÚ – pravidlá a postupy

V danej oblasti kontrolná skupina NKÚ SR preverovala, či pravidlá a postupy spracovania OÚ majú oporu v platnej legislatíve.

KSK mala vypracované pravidlá, podľa ktorých postupujú oprávnené osoby prevádzkovateľa, ak je právnym základom spracúvania OÚ súhlas dotknutej osoby. Pravidlá obsahujú podrobnosti o tom, že oprávnená osoba je povinná v rámci písomného vyhlásenia oddeliť udelenie súhlasu dotknutej osoby na spracúvanie OÚ od iných skutočností.

V prílohe Smernice KSK o ochrane OÚ je uvedený vzor súhlasu so spracovaním OÚ, kde dotknutá osoba vyjadrila súhlas so spracúvaním svojich OÚ, pri udeľovaní súhlasu bola informovaná na aký konkrétny účel/alebo viacero účelov a v akom rozsahu budú OÚ spracovávané. Taktiež je na tlačive uvedené, že udelený súhlas môže dotknutá osoba kedykoľvek odvolať.

Preverením sprostredkovateľských zmlúv bolo zistené, že prevádzkovateľ uzatvoril zmluvy bez toho, aby spracúvanie OÚ v zmluve podmieňoval udelením súhlasu osoby, ktorá v zmluve vystupovala ako jedna zo zmluvných strán.

Kontrolou podmienok pre výberové konania na uchádzačov o zamestnanie bolo zistené, že prevádzkovateľ medzi požadovanými dokladmi uviedol aj súhlas dotknutej osoby so spracovaním OÚ.

### Kontrolné zistenie č. 2

Prevádzkovateľ tým, že v prípade výberových konaní medzi požadovanými dokladmi vyžadoval aj súhlas dotknutej osoby so spracovaním OÚ konal v rozpore s čl. 7 ods. 4 nariadenia GDPR. V prípade výberových konaní dochádza k spracúvaniu priamo na základe nariadenia a súhlas nie je potrebný, čo priamo vyplýva z ustanovenia.

Prevádzkovateľ mal vypracované pravidlá, podľa ktorých oprávnené osoby prevádzkovateľa postupujú, ak je právnym základom spracúvania OÚ zákon, osobitný predpis alebo medzinárodná zmluva, pravidlá, podľa ktorých oprávnené osoby prevádzkovateľa postupujú pri posudzovaní, či je spracúvanie získaných OÚ možné na iný účel, ako na účel, na ktorý boli pôvodne získané.

Pravidlá, podľa ktorých oprávnené osoby postupujú pri spracúvaní osobitných kategórií OÚ prevádzkovateľ vypracoval. KSK mala vypracované pravidlá (test proporcionality), podľa ktorých oprávnené osoby prevádzkovateľa postupujú pri posudzovaní, do akej miery možno na dané spracúvanie OÚ aplikovať právny základ podľa čl. 6 ods. 1 písm. f) GDPR, t. j. "spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana".

Prevádzkovateľ mal vypracované pravidlá, podľa ktorých oprávnené osoby rozhodujú o tom, či prenos OÚ do tretích krajín alebo medzinárodným organizáciám je možný (oprávnený) a pri prenosoch vyžadujúcich primerané záruky /čl. 46 GDPR/ posudzujú, či pre daný prenos primerané záruky skutočne existujú.

## 2.4 Práva dotknutej osoby – pravidlá, postupy a oznámenia

Prevádzkovateľ preukázal, že oprávnené (poverené) osoby boli poučené, že pri získavaní OÚ priamo od dotknutej osoby sú povinné ju informovať; oprávnené osoby boli poučené o tom, za akých okolností informácie dotknutej osobe neoznamujú, že boli poučené o tom, že ak získavajú OÚ priamo od dotknutej osoby, sú povinné ju o tom informovať. Povinnosti poverenej osoby voči dotknutým osobám sú spracované v Smernici. V čl. 13 v Smernici je uvedený postup prevádzkovateľa, kedy prevádzkovateľ neoznámí dotknutej osobe požadované informácie, má vypracované pravidlá upravujúce rozsah informácií, ktoré oprávnené osoby poskytujú dotknutým osobám.

Prevádzkovateľ na svojom webovom sídle zverejnil informácie určené dotknutým osobám v požadovanom rozsahu a forme o jednotlivých právach, ktoré si môže u prevádzkovateľa uplatniť.



### Uplatňovanie práv dotknutej osoby

Kontrolou bolo zistené, že prevádzkovateľ mal vypracované pravidlá a postup pre prípady, ak by si dotknutá osoba uplatnila právo na prístup k svojim OÚ. Oprávnené osoby sú poučené prostredníctvom Záznamu o poučení oprávnenej osoby, ako majú postupovať pri:

- rozhodovaní o tom, či poskytnutie kópie s OÚ dotknutej osobe nebude mať nepriaznivé dôsledky na práva a slobody iných osôb,
- práve na opravu svojich OÚ,
- práve na výmaz svojich OÚ,
- práve na obmedzenie spracovania svojich OÚ,
- práve na prenosnosť svojich OÚ,
- práve namietat' proti spracovaniu svojich OÚ,
- práve namietat' proti rozhodnutiu založenom výlučne na automatizovanom spracovaní OÚ, vrátane profilovania, ktoré sa jej týka a má právne účinky,
- práve odvolať udelený súhlas na spracovávanie jej OÚ,
- pochybnostiach v súvislosti s totožnosťou fyzickej osoby, ktorá si uplatnila niektoré právo,
- oznamovaní vybavenia žiadosti dotknutej osobe ako odpoveď na jej žiadosť o uplatnenie niektorého z práv.

### Záver:

Preverením práv poskytovaných dotknutým osobám kontrolná skupina NKÚ SR nezistila nedostatky.

### 2.5 Základné pravidlá a pokyny pre bezpečné spracúvanie údajov

V tejto oblasti kontrolná skupina preverovala, aké pokyny vydal prevádzkovateľ oprávneným osobám v súvislosti s poskytovaním informácií dotknutým osobám.

KSK mala v rámci Smernice vypracované pokyny na spracúvanie OÚ s poučením pre oprávnené osoby, pri nástupe zamestnancov do zamestnania uskutočňuje poučenie a vzdáva sa pokyn na spracovanie OÚ. Mal vypracované pravidlá a postup pre pridelenie prístupových práv jednotlivým oprávneným osobám do IS obsahujúcich OÚ, ďalej mal vypracované pravidlá a postup pre pridelenie oprávnení jednotlivým oprávneným osobám podľa úloh, ktoré v IS obsahujúcich OÚ plnia. Zamestnancovi, oprávnenej osobe, s ktorým má byť z rôznych dôvodov so rozviazaný pracovný pomer prevádzkovateľ odoberie prístupové práva do IS, do ktorých mal prístup, ako aj výsledky práce v elektronickej forme, prenosné pamäťové médiá /USB/, mobilné prostriedky IT. Zastupiteľnosť oprávnených osôb, bola zabezpečená, pričom oprávnenú osobu mohla zastupovať len iná oprávnená osoba s rovnakými alebo rozsiahlejšími prístupovými právami a rovnakými alebo rozsiahlejšími oprávneniami. Prevádzkovateľ vykonal opätovné poučenie oprávnenej osoby spoločnosťou, ktorá vykonala Analýzu a zároveň vykonáva pravidelné preškolenia. Oprávnené osoby boli zaviazané povinnosťou dodržiavať mlčanlivosť o OÚ, s ktorými prichádzajú do styku. Upratovanie priestorov KSK zabezpečuje externá firma. Upratovanie priestorov, v ktorých sa nachádza IKT technika je zabezpečené prítomnosťou poverenej osoby.

KSK má vypracovanú internú smernicu upravujúcu základné pravidlá a pokyny pre bezpečné spracúvanie OÚ oprávnenými osobami. Smernica ukladala používateľovi povinnosť vykonávať spracovateľské operácie s OÚ len vo vybraných IS, ku ktorým mal pridelené prístupové práva a to len v rozsahu operácií, ukladala používateľovi povinnosť chrániť spracúvané OÚ (dokumenty, spisy a súbory obsahujúce OÚ vrátane údajov spracúvaných v elektronickej forme) pred ich zneužitím, odcudzením, poškodením, zničením, stratou, neoprávneným prístupom. Používateľ mal povinnosť bezodkladne oznámiť svojmu nadriadenému, že spracúva nesprávne, neúplné alebo neaktuálne OÚ, ak v rámci vybraného IS nemal pridelené oprávnenie na ich zmenu, opravu, doplnenie a aktualizáciu. Smernica používateľovi ukladala povinnosť priebežne likvidovať bezpečným spôsobom pracovné verzie dokumentov v papierovej forme (skartačným zariadením) a ich výmazom v elektronickej forme, ktoré obsahujú OÚ a sú už nepotrebné. Používateľ nemá povinnosť priebežne zálohovať OÚ (dokumenty) spracúvané v elektronickej forme, u ktorých nedochádza k automatickému zálohovaniu. Smernica zahŕňa aj povinnosť vykonať opatrenia, aby nedochádzalo k sprístupneniu



spracúvaných OÚ (napr. o inej fyzickej osobe) z IS obce neoprávnenej osobe. Smernica ďalej ukladá používateľovi povinnosť získavať OÚ kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií len vtedy, ak to právny predpis predpokladá, prípadne je to nevyhnutné na dosiahnutie účelu spracúvania OÚ, bezodkladne nahlásiť bezpečnostný incident, pri ktorom došlo k odcudzeniu, poškodeniu alebo zničeniu dokumentov alebo spisov obsahujúcich OÚ alebo k neoprávnenému skopírovaniu dokumentu v elektronickej forme, alebo k jeho vymazaniu zo systému.

V Smernici je určený postup pri komunikácii so sprostredkovateľom v rozsahu zmluvne dohodnutých podmienok. Smernica ukladá používateľovi povinnosť zabezpečiť diskretnosť pri spracúvaní OÚ tak, aby OÚ neboli sprístupnené nepovolánym osobám, ak oprávnená osoba získava OÚ od inej osoby alebo inej osobe OÚ sprístupňuje v priestore prístupnom verejnosti, alebo v priestore, kde sa zdržuje aj iný zamestnanec organizácie, ktorý nie je oprávnenou osobou spracúvať predmetné OÚ.

Používateľ vrátane zamestnancov tretích strán majú povinnosť zdržať sa akýchkoľvek úkonov, ktoré by viedli k získaniu (odcudzeniu) údajov spracúvaných v IS organizácie alebo k narušeniu alebo k prekonaniu bezpečnostných opatrení vo vzťahu k prostriedkom IT, do ktorých nie je oprávnená vstupovať. Smernica zakazuje používateľovi poskytovať informácie o rozmiestnení prostriedkov IT, ich parametroch, informačných systémoch a ich technickom a organizačnom zabezpečení nepovolánym osobám. Používateľovi sa v zmysle smernice zakazuje zneužiť nedbanlivosť iného používateľa na to, aby použil PC, informačný systém alebo počítačovú sieť pod jeho identitou a vyvíjať akúkoľvek komerčnú, podnikateľskú alebo inú zárobkovú činnosť prostredníctvom prostriedkov IT organizácie.

Kontrolou základných pravidiel a pokynov pre oprávnené osoby pri spracovaní údajov v papierovej forme bolo zistené, že smernica ukladala používateľovi povinnosť riadiť sa politikou „čistého stola“, t. j. manipulovať s dokumentáciou tak, aby bol zamedzený prístup k osobným údajom nepovolánym osobám. Dokumenty obsahujúce OÚ sú umiestnené v uzamykateľných skrinách, do ktorých majú prístup len oprávnené osoby s pridelenými prístupovými právami. Pri nakladaní s dokumentami, ktorých obsah majú citlivejší charakter smernica osobitne neukladá postup oprávnených osôb, aby postupovali pri ich poskytovaní, sprístupňovaní a zverejňovaní so zvýšenou opatrnosťou.

Povinnosť zabezpečiť pri kopírovaní (skenovaní) dokumentov obsahujúcich OÚ alebo ich tlačení v papierovej forme, aby sa s ich obsahom neoboznámila nepovolaná osoba a v prípade, že príslušné zariadenie je umiestnené mimo priamy dosah oprávnenej osoby (napr. na chodbe), oprávnená osoba je po zadaní príkazu na tlačenie dokumentu povinná bezodkladne sa presunúť k tlačiarňe a vytlačený dokument z nej odobrať smernica neobsahuje. Smernica ďalej neobsahuje povinnosť používateľa bezodkladne zlikvidovať v skartačnom zariadení nadbytočné a chybné vytlačené alebo nakopírované dokumenty. Túto povinnosť ukladá prevádzkovateľ v poverení a poučení prevádzkovateľa. Viest evidenciu alebo vyznačiť, napr. v spise, z ktorého dokument obsahujúci OÚ pochádza (napr. životopis), že bola vyhotovená kópia, kedy bola vyhotovená a na aký účel smernica ani poverenie neukladá.

Smernica ukladá používateľovi oprávnenie poskytnúť alebo sprístupniť OÚ zamestnanca na telefonické (e-mailové, faxové) dožiadanie len vtedy, ak má naň preukázateľne predchádzajúci písomný súhlas zamestnanca organizácie. Používateľ má zakázané ponechávať dokumenty (spisy) obsahujúce OÚ voľne dostupné na chodbách organizácie, voľne odložené v priestoroch KSK, alebo v iných verejne prístupných priestoroch a v opustenom dopravnom prostriedku. Zákaz sa týka poskytovania informácií na telefonické, e-mailové, a faxové vyžiadanie o spracúvaných osobných údajoch dotknutých osôb alebo osobných údajoch zamestnancov obce nepovolánym osobám a to žiadnym spôsobom (telefónom, e-mailom, faxom, písomne, osobne...), ak ho na to neoprávňuje právny predpis.

V kontrolovanej oblasti základné pravidlá a pokyny pre oprávnené osoby – identifikácia a autentizácia bolo zistené, že smernica KSK ukladala povinnosť používateľa chrániť autentizačné prostriedky (heslo, PIN, služobný preukaz, token – čipovú kartu, klientsky certifikát, šifrovací kľúč a pod.) pred sprístupnením nepovolanej osobe, odcudzením a zneužitím, ukladala povinnosť používateľovi na výzvu systému aspoň 90 dní zmeniť heslo, ukladala povinnosť po prípadnom vyzrazení hesla alebo pri podozrení z jeho možného zneužitia heslo bezodkladne zmeniť, povinnosť bezodkladne oznámiť príslušnému zamestnancovi (administrátorovi systému) stratu alebo odcudzenie hardvérového autentizačného prostriedku a zároveň boli uložené požiadavky na zložitosť hesla podľa určitých kritérií. Smernica ukladala používateľovi povinnosť zmeniť heslo pridelené príslušným zamestnancom po prvom prihlásení a zadať svoje heslo, zakazuje používateľovi ponechávať svoje autentizačné prostriedky voľne prístupné alebo odložené bez dozoru. Smernica nezakazuje používateľovi heslo (PIN) uchovávať (archivovať) na voľne dostupnom nosiči dát, zapožičať alebo odovzdať



(sprístupniť) neoprávnenej osobe a to ani inému používateľovi svoje autentizačné prostriedky. Smernica zakazuje užívateľovi zasielať autentizačné prostriedky (užívateľský účet, PIN a pod.) elektronickou poštou alebo faxom vo forme voľne čitateľného textu. Naopak smernica nezakazuje využívať v rámci aplikácie funkcionality systému „zapamätať heslo“.

Pri kontrole dodržiavania základných pravidiel a pokynov pri práci s pracovnou stanicou bolo zistené, že Smernica ukladá používateľom dodržiavať pravidlo „čistej obrazovky“ pre prostriedky IT, na ktorých sú spracúvané údaje, čo znamená, že pri dlhšom vzdialení sa od obrazovky PC, uzamknúť priestor (miestnosť), v ktorej sa nachádzajú prostriedky IT (počítač, notebook, tlačiareň, USB kľúče a pod.) pri odchode z miestnosti, po skončení pracovnej doby, resp. po ukončení práce odhlásiť sa zo systému, vypnúť PC a príslušné periférne zariadenia, dbať na antivírusovú ochranu PC a umožniť operačnému systému a antivírusovému programu automatickú aktualizáciu systému a spustiť reštart PC, nahlásiť príslušnému zamestnancovi chyby alebo zlyhanie operačného systému, aplikácií alebo periférneho zariadenia alebo ich akékoľvek neštandardné správanie sa, používateľovi povinnosť, ktorý z rôznych dôvodov pracuje na PC (notebooku) pridelenom inému používateľovi, prihlasovať sa do systému výlučne pod svojim užívateľským účtom. Zakazuje sa umožniť použitie svojho PC (notebooku) nepovolaným osobám, inštalovať, používať a uchovávať na hardvérovom vybavení pridelených prostriedkov IT neautorizovaný (nelegálny) softvér, používateľovi nechať po skončení pracovnej doby a odchode zamestnancov z pracoviska alebo počas ich dlhodobej neprítomnosti nezabezpečené (otvorené) okná na miestnosti, v ktorej sa nachádzajú prostriedky IT. Smernica obsahuje podmienku, že pracovná stanica pridelená používateľovi nesmie zároveň slúžiť ako server pre iných používateľov.

Pri preverení pravidiel a pokynov pre oprávnené osoby pri práci mobilnými prostriedkami IT bolo zistené, že smernica o ochrane OÚ ukladá používateľovi povinnosť:

- odložiť mobilný prostriedok IT (napr. notebook, tablet, smartfón), ktorý zostáva v organizácii po skončení pracovnej doby alebo počas jeho dlhodobej neprítomnosti na pracovisku, do chráneného priestoru (uzamykateľná skriňa, trezor a pod.), alebo ho zabezpečiť bezpečnostným mechanizmom (napr. bezpečnostná retiazka) tak, aby bolo zabránené jeho použitiu, poškodeniu alebo odcudzeniu,
- povinnosť prenášať mobilné prostriedky IT mimo organizáciu v ochrannom obale (taška, puzdro a pod.) určenom na tento účel,
- povinnosť mať mobilné prostriedky IT prenášané mimo organizácie pod neustálym dohľadom, čím sa rozumie, že používateľ nesmie ponechávať mobilné prostriedky IT odložené v opustenom (ani uzamknutom) dopravnom prostriedku (napr. služobnom alebo súkromnom automobile), voľne odložené v rokovacích sálach (bez dozoru) alebo na iných verejne prístupných miestach pri pracovných rokovaniach,
- povinnosť priebežne vykonávať zálohovanie informácií uložených lokálne v mobilnom prostriedku IT na prenosné médium (prípadne pevný disk iného PC) z dôvodu možnej obnovy spracúvaných informácií pri zlyhaní systému,
- používateľovi pripájať mobilný prostriedok IT do nezabezpečených verejných dátových sietí.

Smernica o bezpečnostnej politike IS KSK ukladá používateľovi povinnosť prihlasovať sa do systému len pod prideleným užívateľským účtom, povinnosť nahlásiť zlyhanie mobilného prostriedku IT alebo jeho akékoľvek neštandardné správanie sa, dbať na antivírusovú ochranu mobilného prostriedku IT a umožniť operačnému systému a antivírusovému programu automatickú aktualizáciu systému, uchovávať lokálne na mobilnom prostriedku IT z informačných systémov organizácie len údaje (informácie), s ktorými nevyhnutne potrebuje pracovať mimo organizácie, zakazuje používateľovi vykonávať technické zásahy do mobilného prostriedku IT, zakazuje používateľovi zasahovať do bezpečnostnej konfigurácie softvéru nainštalovaného na mobilného prostriedku, zakazuje smernica používateľovi umožniť využívať mobilný prostriedok IT nepovolaným osobám alebo mobilný prostriedok IT zapožičať, prenechať alebo odovzdať tretej osobe, ani u tretej osoby takéto zariadenie založiť formou záložného práva, zakazuje používateľovi umožniť prístup cez svoj mobilný prostriedok IT do informačného systému obsahujúceho OÚ osobám (zamestnancom), ktoré nie sú v postavení oprávnenej osôb a zakazuje používateľovi inštalovať a používať na mobilnom prostriedku IT neautorizovaný softvér.

Preverení pravidiel a postupov pri práci s prenosnými médiami bolo zistené, že smernica: KSK ukladá používateľovi povinnosti v zmysle zákona a to: používať pri práci len prenosné médiá, ktoré používateľovi pridelená organizácia a sú preverené licencovaným antivírusovým programom, povinnosť uchovávať lokálne na prenosnom médiu



## Najvyšší kontrolný úrad Slovenskej republiky

z informačných systémov organizácie len údaje, ktoré nevyhnutne potrebuje k svojej práci a potrebuje ich mať v bezprostrednom dosahu, povinnosť zašifrovať údaje uchovávané na prenosných médiách prenášaných mimo organizácie s využitím autorizovaných šifrovacích prostriedkov, chrániť prenosné médium a to aj počas transportu pred stratou, odcudzením, zneužitím a neautorizovaným prístupom nepovolanych osôb.

Kontrolná skupina pri preverovaní dodržiavania pravidiel pri používaní internetu a elektronickej pošty zistila, že prevádzkovateľ:

- nemonitoruje zamestnancov, či v pracovnej dobe nepristupujú na webové stránky, ktoré nesúvisia s výkonom ich pracovnej činnosti,
- nekontroluje poštu odoslanú z pracovnej elektronickej adresy a doručeníu na túto adresu
- nezakazuje používateľovi zadávať svoje prihlasovacie meno a heslo do prostredia neznámych alebo podozrivých webových stránok a to ani v prípade, ak je o to požiadaný
- nezakazuje posilať v prílohe správy súbory s príponou exe, com, bat, scr a pod.

Prijaté technické a organizačné opatrenia pre prácu s internetom a elektronickou poštou zabezpečia, že spracovanie OÚ prevádzkovateľ vykonáva v súlade s Nariadením GDPR.

KSK v kontrolovanom období nemal vypracovanú internú smernicu upravujúcu bezpečnostné pravidlá a podmienky pri práci s kamerovým systémom a pri servise kamerového systému. Verejné priestory sú monitorované kamerovým systémom. Monitorovanými priestormi boli: vonkajšie vchody, dvor, 1. poschodie Budovy 1 – kancelária predsedu, 2. poschodie Budovy 1, a suterén. Záznam je uchovávaný po dobu 14 dní. Server kamerového systému je umiestnený v priestoroch informátora. Systém nie je zálohovaný a je spravovaný externým dodávateľom. (č. 20 z analýzy rizík). Kamerovým systémom prevádzkovateľ nemonitoroval miestnosti, kde sa nachádzajú servery. KSK nemonitoroval zamestnancov na pracovisku alebo v spoločných priestoroch organizácie pri výkone ich pracovnej činnosti ani pohyb zamestnancov v služobných automobiloch pomocou GPS. Kamerový systém prevádzkuje KSK, zamestnanci obsluhujúci kamerový systém majú postavenie oprávnených osôb.

### Záver:

Preverení základných pravidiel a pokynov pre bezpečné spracúvanie údajov kontrolná skupina NKÚ SR zistila, že prevádzkovateľ aj na základe vypracovanej analýzy vypracoval podrobné pravidlá a postupy oprávneným osobám v súvislosti s poskytovaním informácií dotknutým osobám, postupy pre bezpečné spracúvanie OÚ oprávnenými osobami, postupy pre oprávnené osoby pri spracovaní údajov v papierovej forme, pre prácu s pracovnou stanicou, mobilnými prostriedkami IT a prácu s prenosnými médiami. Prijaté pravidlá a postupy dávajú predpoklad pre bezpečné spracúvanie údajov.

## 2.6 Bezpečnostné smernice a dokumentácia

Procesy súvisiace s ohlasovaním porušenia ochrany OÚ podľa nariadenia GDPR boli špecifikované v Smernici riadenie bezpečnostných incidentov s účinnosťou od 25.05.2018. Posúdenie vplyvu na ochranu údajov v rámci IS, ktoré prevádzkovateľ prevádzkuje a vypracovanie analýzy zabezpečila externá firma. prevádzkovateľ má zároveň vypracované pravidlá na zavedenie pseudonymizačných techník, ktoré v rámci nariadenia GDPR implementovala v IS SAP/R3. Zároveň KSK vypracovala záznamy o spracovateľských činnostiach, pravidlá na zavedenie šifrovacích techník na ochranu OÚ v IS a šifrovacie techniky v IS zaviedla.

### Záver:

Kontrolou bezpečnostnej smernice, súvisiacich dokumentov a ich aplikáciou neboli zistené nedostatky.

## 2.7 Informačná bezpečnosť - bezpečnostné štandardy

Kontrolná skupina NKÚ SR preverila, či prevádzkovateľ konal v zmysle ust. § 78 ods. 11 zákona o ochrane OÚ, podľa ktorého mal pri prijímaní bezpečnostných opatrení postupovať primerane podľa medzinárodných noriem a štandardov.



Prevádzkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu OÚ postupov primerane podľa medzinárodných noriem a štandardov bezpečnosti. Za účelom zabezpečenia informačnej bezpečnosti vypracoval bezpečnostné štandardy:

- o "Bezpečnostná politika" podľa štandardu pre riadenie informačnej bezpečnosti /§ 29 písm. a) výnos MF SR 55/2014 Z. z., ktorým priradila zodpovednosť za bezpečnosť a obsah každého významného aktíva konkrétnemu vlastníkovi a ustanovila osobu zodpovednú za informačnú bezpečnosť,
- o štandard pre personálnu bezpečnosť, ktoré obsahuje poučenie o bezpečnostnej politike a ochranu údajov zamestnancov organizácie a tretích strán pred ich prvým vstupom do IS a ukladá zamestnancov povinnosť nahlásovať bezpečnostné incidenty,
- o štandard pre manažment rizík pre oblasť informačnej bezpečnosti, ktorý rieši kritické procesy, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných IS a plány na obnovu činnosti nefunkčných, zničených alebo poškodených IS VS,
- o štandard pre kontrolný mechanizmus riadenia informačnej bezpečnosti, prevádzkovateľ vykonáva vnútornú kontrolu/audit informačnej bezpečnosti,
- o štandard pre ochranu proti škodlivému kódu,
- o štandard pre sieťovú bezpečnosť,
- o štandard pre fyzickú bezpečnosť a bezpečnosť prostredia,
- o štandard pre aktualizáciu softvéru,
- o štandard pre monitorovanie a manažment bezpečnostných incidentov,
- o štandard pre periodické hodnotenie zraniteľnosti,
- o štandard pre zálohovanie a fyzické ukladanie záloh,
- o štandard pre riadenie prístupu,
- o štandard pre aktualizáciu IKT,
- o štandard pre účasť tretej strany.

Bezpečnostné štandardy boli vypracované v zmysle § 30 až 43 výnosu MF SR.

#### Záver:

Pri preverovaní dodržiavania základných pravidiel a pokynov pre bezpečné spracúvanie OÚ kontrolná skupina NKÚ SR konštatuje, že prevádzkovateľ dodržiava základné pravidlá a pokyny nariadenia GDPR a smernice o ochrane OÚ.

### 3. Výkon funkcie zodpovednej osoby

KSK v období pred 25. 05. 2018 mal určenú ZO, ktorá úspešne absolvovala skúšku na ÚOOÚ SR a predložila potvrdenie o jej absolvovaní č. 15782/2013 z 21.11.2013. Od 25.05.2018 kontrolovaný subjekt určil tri ZO. V období pred účinnosťou GDPR, do 25.5.2018, ani po nadobudnutí jeho účinnosti, nežiadal prevádzkovateľ finančné prostriedky na ich činnosť.

Informácie o ZO v súlade s čl. 37 ods. 7 GDPR zverejnil KSK na svojom webovom sídle a boli na ÚOOÚ SR oznámené 24. 05.2018. Bezúhonnosť ZO KSK nepreveroval z dôvodu, že boli zamestnancami KSK. ZO boli ustanovené do funkcie na základe odborných znalostí a kvalít. Monitorovali zavedené pravidlá ochrany OÚ v organizácii, vrátane rozdeľovania povinností osobám oprávneným spracúvať OÚ a posudzovali ich súlad, resp. úplnosť s GDPR a zákonom o ochrane OÚ, čl. 39 ods. 1 písm. b) nariadenia GDPR. V kontrolovanom období iniciovali úpravy interných noriem so zapracovaním opatrení na zabezpečenie OÚ.

ZO mali možnosť vstupovať len do IS obsahujúcich údaje potrebné na plnenie ich úloh. Mali zamedzený vzdialený prístup do IS obsahujúcich OÚ organizácie, ZO sa zúčastňovali na zasadnutí vedenia ÚKSK, na ktorých sa riešili otázky súvisiace s ochranou OÚ a informačnou bezpečnosťou. Iniciovali odporúčanie na zmenu smernice o ochrane OÚ a ďalšie interné normy, zabezpečenie dodržiavania Štandardov informačnej bezpečnosti, návrh rozpočtu vo vzťahu k IB. Poskytovali konzultácie: - v oblasti sociálnej agendy, školstva, sprostredkovateľských zmlúv, športu, SAP R/3,



registratúry, poverení, spracovateľských operácií, vyššiemu manažmentu a iným zamestnancom v súvislosti s ochranou OÚ. ZO vypracúvali výkazy činnosti, ktoré boli potvrdené na prístupových formulároch pre oprávnené osoby.

ZO za výkon funkcie nepoberali odmenu. Sú internými zamestnancami a majú vysokoškolské vzdelanie. KSK nevymedzila pozície v organizačnej štruktúre, ktoré sú nezlučiteľné s výkonom funkcie ZO. Zodpovedné osoby podľa popisov pracovných činností plnia aj iné úlohy a povinnosti. Kontrolná skupina NKÚ SR zisťovala, či úlohy, ktoré ZO vykonávajú, nevedli ku konfliktom záujmov. Preverenie nebolo zistené, že by činnosti ZO viedli ku konfliktu záujmov. Podľa vyjadrení kontrolovaného subjektu ZO nevykonávali v kontrolovanom období funkciu ZO pre subjekty v súkromnom sektore alebo vo verejnej správe.

#### **Záver:**

Pri preverovaní funkcie ZO kontrolná skupina NKÚ SR nezistila nedostatky.

#### **4. Činnosť sprostredkovateľov**

KSK v kontrolovanom období mal vypracované pravidlá (smernicu), podľa ktorých oprávnené osoby postupujú pri príprave a uzatváraní zmlúv so sprostredkovateľmi. Tri spoločnosti boli voči KSK v úlohe sprostredkovateľov. Kontrolou obsahu uzatvorených zmlúv neboli zistené nedostatky. Sprostredkovateľské zmluvy boli k účinnosti nariadenia GDPR aktualizované.

Podľa vyjadrenia kontrolovaného subjektu KSK nepreveroval sprostredkovateľov, či poskytujú dostatočné záruky na to, že príjmu primerané technické a organizačné opatrenia v súlade s GDPR, spoliehal sa na ich vyhlásenie. Podmienkami v zmluvách bolo zabezpečené, že každá fyzická osoba konajúca na základe poverenia, ktorá má prístup k osobným údajom, spracúva tieto OÚ len na základe pokynov prevádzkovateľa. Prevádzkovateľ uzatvorené sprostredkovateľské zmluvy preskúmal a posúdil a konštatoval, že sprostredkovateľ si sám neurčil účely a prostriedky spracúvania OÚ. Uzatvorené sprostredkovateľské zmluvy obsahovali podmienky a náležitosti uvedené v čl. 28 nariadenia a to, že sprostredkovateľ nezapojí ďalšieho sprostredkovateľa bez písomného povolenia prevádzkovateľa.

KSK nemal uložené OÚ v externých úložiskách (cloud), resp. nevyužíval služby aplikácií alebo programov uložených na serveroch na webe (cloud computing).

#### **Záver:**

Pri preverovaní činnosti sprostredkovateľov neboli zistené nedostatky

#### **5. Finančné prostriedky vyčlenené na implementáciu povinností a opatrení podľa nariadenia**

Kontrolou bolo preverené, koľko finančných prostriedkov vynaložil prevádzkovateľ na technické a organizačné opatrenia súvisiace s plnením nových povinností vyplývajúcich z nariadenia GDPR na ochranu OÚ.

V rokoch 2016 až 2017 neboli KSK poskytnuté finančné prostriedky štátom na zabezpečenie ochrany OÚ a povinností vyplývajúcich zo zákona č. 122/2013 Z. z. Z dôvodu plnenia nových povinností vyplývajúcich z GDPR neboli KSK poskytnuté finančné prostriedky štátom ani na roky 2018 a 2019 určené na zabezpečenie ochrany OÚ v IS od 25. 5. 2018.

ÚKSK žiadal z dôvodu zavedenia GDPR na plnenie nových povinností vyplývajúcich z GDPR od 25.5.2018 o navýšenie finančných prostriedkov na zabezpečenie ochrany OÚ v IS na rok 2018/resp. od 25.5.2018 (na roky 2019, 2020). Požiadavka bola prednesená na rokovaní zastupiteľstva KSK. Požadované finančné prostriedky neboli poskytnuté.

KSK v kontrolovanom období zabezpečil pre oprávnené osoby vzdelávanie v oblasti ochrany OÚ a posilňoval ich povedomie v súvislosti s plnením povinností, ktoré im vyplývajú z GDPR. Oprávnené osoby sa zúčastnili na



## Najvyšší kontrolný úrad Slovenskej republiky

seminároch, konferenciách k problematike GDPR: napr. v roku 2018 konferencia o kybernetickej bezpečnosti, v roku 2017 Seminár k ochrane OÚ podľa nového zákona a nariadenia GDPR a konferencia ESET SECURITY DAYS 2019, kybernetická bezpečnosť 2019 v roku 2019. Náklady na vzdelávanie predstavovali 381,00 eur.

Podľa vyjadrenia kontrolovaného subjektu chýbajú na zabezpečenie ochrany OÚ finančné prostriedky aj ľudské zdroje. KSK plne hradila náklady za plnenie povinností súvisiacich s prevádzkovaním IS, ktoré na ňu preniesol štát zo svojho rozpočtu.

V súvislosti s plnením povinností zabezpečenia ochrany OÚ vyplývajúcich z GDPR KSK nakúpil v rokoch 2018 a 2019 technické prostriedky na posilnenie bezpečnosti údajov. V roku 2018 nakúpil skartovače v počte 5 ks, v hodnote 967,11 eur. V roku 2019 KSK zabezpečil nábytkový trezor v hodnote 1 160,00 eur, kartotékové skrine v počte 12 kusov, v hodnote 1 220,00 eur a tri skartovače v hodnote 464,64 eur.

### Záver:

Kontrola NKÚ SR preverila výšku finančných prostriedkov, ktoré prevádzkovateľ vynaložil na technické a organizačné opatrenia súvisiace s plnením povinností vyplývajúcich z nariadenia GDPR.

V rokoch 2016 a 2019 neboli KSK poskytnuté finančné prostriedky štátom na zabezpečenie ochrany OÚ a povinností vyplývajúcich zo zákona č. 122/2013 Z. z. a nariadenia GDPR a zákona o ochrane OÚ. ÚKSK žiadal z dôvodu zavedenia GDPR na plnenie nových povinností vyplývajúcich z GDPR od 25.5.2018 o navýšenie finančných prostriedkov na zabezpečenie ochrany OÚ v IS na rok 2018, resp. od 25.5.2018 (na roky 2019, 2020). Požiadavka bola predložená na rokovanie zastupiteľstva KSK. Požadované finančné prostriedky neboli poskytnuté. Celkové náklady KSK na zabezpečenie spracúvaných OÚ predstavovali 60 352,75 eur.

Za kontrolnú skupinu dňa 18.10.2019

Ing. Jana Beňová  
vedúci kontrolnej skupiny

Ing. Tomáš Tokár  
člen kontrolnej skupiny

S obsahom záznamu o výsledku kontroly bol oboznámený dňa

9.11.2019

Ing. Rastislav Trnka  
predseda KSK