2019

Záverečná správa

Systém ochrany a bezpečnosti údajov vo verejnom sektore

Záverečná správa

Systém ochrany a bezpečnosti údajov vo verejnom sektore

PREDKLADÁ
Ing. Karol Mitrík, predseda
Najvyšší kontrolný úrad Slovenskej republiky

Bratislava, apríl 2020

OBSAH

ZOZNAM SKRATIEK

SKRATKA / SKRÁTENÉ POMENOVANIE	VÝZNAM
BSK	Bratislavský samosprávny kraj
DataCentrum	DataCentrum elektronizácie územnej samosprávy Slovenska
EK	Európska Komisia
EÚ	Európska únia
IS	Informačný systém
KSK	Košický samosprávny kraj
MF SR	Ministerstvo financií Slovenskej republiky
MPK	Medzirezortné pripomienkové konanie
MPSVaR SR	Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky
MS SR	Ministerstvo spravodlivosti Slovenskej republiky
Nariadenie (EÚ)	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
NKÚ SR	Najvyšší kontrolný úrad Slovenskej republiky
NR SR	Národná rada Slovenskej republiky
NSK	Nitriansky samosprávny kraj
Orgány štátu	Orgány verejnej moci, verejnoprávne inštitúcie a iné spoločnosti s účasťou štátu (MPSVaR SR, ÚPSVaR SR, ÚGKK SR, Sociálna poisťovňa, VšZP, DataCentrum)
Smernica 95/46/ES	Smernica Európskeho parlamentu a Rady 95/46/ES z 24.októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov
SR	Slovenská republika
ŠR	Štátny rozpočet
ÚGKK SR	Úrad geodézie, kartografie a katastra Slovenskej republiky
ÚOOÚ SR	Úrad na ochranu osobných údajov Slovenskej republiky
ÚPSVaR SR	Úrad práce, sociálnych vecí a rodiny Slovenskej republiky
VšZP	Všeobecná zdravotná poisťovňa
VÚC	Vyšší územný celok
výnos MF SR	Výnos Ministerstva financií SR č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy 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 č. 428/2002 Z. z.	Zákon č. 428/2002 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
zákon č. 122/2013 Z. z.	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.	Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z.
ŽSK	Žilinský samosprávny kraj

ZOZNAM TABULIEK

ZOZNAM GRAFOV

ZHRNUTIE

Rôzne údaje sa stávajú osobnými údajmi až vtedy, keď na ich základe dôjde k identifikovaniu konkrétnej fyzickej osoby alebo k vytvoreniu predpokladu pre jej identifikovanie. **Ochrana osobných údajov** neznamená ich neposkytovanie zo strany občanov, ale znamená zabezpečenie nenarušenia vážnosti, dôstojnosti a bezpečnosti osôb, ktoré osobné údaje poskytli verejnému alebo súkromnému subjektu na účely ich ďalšieho spracovania.

Ochrane osobných údajov, ako dôležitej verejnej politike, sa venuje aj Programové vyhlásenie vlády SR (2016), ktoré výslovne poukazuje na plnenie základnej povinnosti vyplývajúcej z GDPR, a to **klásť dôraz na bezpečnosť spracúvaných údajov občanov a posilňovanie ich dôvery vo využívanie elektronických/digitálnych služieb**.

GDPR (General Data Protection Regulation) je všeobecné Nariadenie (EÚ) o ochrane údajov, ktoré nadobudlo platnosť 25. mája 2016 a **od tohto momentu začalo plynúť dvojročné prechodné obdobie**, počas ktorého boli povinné všetky subjekty verejného aj súkromného sektora, spracúvajúce osobné údaje v IS, pripraviť sa na jeho uplatňovanie **v plnom rozsahu od 25. mája 2018.** Nariadenie (EÚ) má charakter európskeho zákona, ktoré je **priamo účinné, vykonateľné a uplatniteľné na území každého členského štátu EÚ**. Členským štátom dáva priestor upraviť len niektoré jeho články v zmysle národných špecifík. **Nariadenie (EÚ) na vnútroštátnej úrovni doplnil s účinnosťou od 25. mája 2018 nový zákon o ochrane osobných údajov, zákon č. 18/2018 Z. z.**

Osobné údaje sú prevádzkovateľmi spracúvané naprieč celým verejným aj súkromným sektorom, a tak sa ochrana a spracúvanie osobných údajov týka bez výnimky všetkých občanov SR. Každý orgán verejnej správy je s určitosťou prevádzkovateľom personálnej a mzdovej agendy aj správy registratúry. Štát okrem toho prevádzkuje ďalšie stovky databáz, IS a registrov (matriku, kataster nehnuteľností, daňový IS, register trestov, evideciu obyvateľov a ďalšie), v ktorých spracúva osobné údaje v elektronickej a papierovej forme, v mnohých prípadoch prostredníctvom samospráv v rámci preneseného výkonu štátnej správy.

V rámci kontrolnej akcie bolo preverených **62 subjektov – prevádzkovateľov IS**, spracúvajúcich osobné údaje vo verejnom sektore **a MS SR**. Prevádzkovatelia IS boli vybraní tak, aby v rámci kontroly mali zastúpenie rôzne orgány verejnej správy a to plošne v rámci celej SR. Podstatným kritériom pri výbere orgánov štátu bol rozsah, obsah a dôležitosť IS, v ktorých prevádzkovatelia spracúvajú osobné údaje občanov SR. Kontrola na MS SR mala osobité zameranie. V rámci kontroly boli preverované najmä oblasti:

- *analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ)*
- *práva dotknutej osoby – pravidlá, postupy a oznámenia*
- *výkon funkcie zodpovednej osoby a*
- *stav ochrany osobných údajov v oblasti bezpečnosti spracúvania údajov.*

Štát je povinný postarať sa v súlade s princípmi zakotvenými v Nariadení (EÚ) o bezpečnosť osobných údajov svojich občanov, ktoré od nich vyžaduje na rôzne účely a spracúva vo svojich IS. Na tento účel je povinný pre orgány štátnej správy aj územnej samosprávy **vyčleniť potrebné finančné prostriedky.** Je zrejmé, že ochrana osobných údajov sa sčasti prekrýva s informačnou bezpečnosťou, najmä v oblasti automatizovaného spracúvania údajov. Napriek tomu je však potrebné vedieť, koľko finančných prostriedkov bolo určených priamo na plnenie povinností, ktoré orgánom verejnej správy prinieslo nové Nariadenie (EÚ). **Takouto analýzou (informáciou) však štát nedisponuje a zvýšené finančné nároky na zabezpečenie ochrany osobných údajov, vyplývajúce pre prevádzkovateľov z Nariadenia (EÚ), štát zatiaľ ponechal výlučne na orgány verejnej správy, aby sa s tým vysporiadali vo vlastnej réžii a bez jeho pričinenia.**

Bez dostatočných finančných prostriedkov zabezpečovať akúkoľvek vysoko odbornú činnosť je spravidla nemožné, o to viac, ak ide o oblasť, ktorá si vyžaduje nielen neustále aktuálne a moderné hardvérové a softvérové vybavenie potrebné na zabezpečenie ochrany IS obsahujúcich osobné údaje, ale aj **na slovo vzatých odborníkov, špecialistov na ochranu osobných údajov**, ktorých si však verejná správa len ťažko udrží bez adekvátneho finančného ohodnotenia.

Najslabšie výsledky v oblasti ochrany osobných údajov dosiahli prevádzkovatelia v úrovni prijatých technických a organizačných opatrení na zabezpečenie ochrany osobných údajov v IS. Pri spracovávaní osobných údajov, pri ktorých sa prevádzkovateľ **musí riadiť podmienkami ustanovenými zákonom**, **kontrolované subjekty v praxi nemali podstatné problémy** a väčšina z nich na tento účel zaviedla opatrenia prostredníctvom pokynov alebo poučení pre oprávnené osoby.

NKÚ SR konštatuje, že dobrý zámer EK posilniť ochranu údajov a bezpečnosť spracúvania v IS prevádzkovateľov a sprostredkovateľov prostredníctvom povinného zavedenia funkcie *„Úradníka pre ochranu údajov“* v orgánoch verejnej

správy, sa po jednom roku od účinnosti Nariadenia (EÚ) v SR celkom nenaplnil. **Organizácie s väčším počtom zamestnancov nie sú veľmi ochotné akceptovať názory a rady tzv. zodpovedných osôb, odsúvajú ich na pozície na nižších stupňoch riadenia v organizácii.** Opomenúť nemožno nízke finančné ohodnotenie interných zodpovedných osôb, keďže štát priamo na ich činnosť zatiaľ neprispieva a väčšinou ju **v rámci organizácie tieto osoby vykonávajú kumulovane v súbehu s inými úlohami len ako doplnkovú činnosť**.

NKÚ SR vyhodnotením celkového stavu dodržiavania povinností ustanovených Nariadením (EÚ), zákonom č. 18/2018 Z. z., dospel k záveru, že **„subjekty verejnej správy nedostatočne zabezpečujú a dodržiavajú ochranu osobných údajov"**. Najčastejšie sa opakujúce pochybenia kontrolovaných subjektov sú uvedené v kapitole 3 tejto záverečnej správy.

Nesprávna aplikácia Nariadenia (EÚ) alebo zákona č. 18/2018 Z. z. v praxi môže mať pôvod aj v **nejasnej** alebo **nesprávne implementovanej legislatíve**. Viac ako **45 % kontrolovaných subjektov považuje prijatú legislatívu za čiastočne zrozumiteľnú**, pričom viacerí z nich zároveň uviedli, že s aplikáciou legislatívy v praxi majú problém a bez odbornej pomoci nemajú istotu, že konajú v súlade so zákonom a nariadením. **Až 28 % kontrolovaných subjektov sa vyjadrilo, že legislatíva v oblasti ochrany osobných údajov je náročná**, **nezrozumiteľná a ťažko aplikovateľná**.

NKÚ SR v rámci kontroly zistil, že MS SR na základe kompetencie, ustanovenej zákonom č. 18/2018 Z. z., vykonávať funkciu osobitného orgánu dozoru, **neprijalo opatrenia**, v súlade s ktorými **by bol v SR od 25. mája 2018 zavedený účinný kontrolný systém** dodržiavania pravidiel ustanovených v Nariadení (EÚ) **pri spracúvaní osobných údajov súdmi pri výkone ich súdnej právomoci. A zároveň zistil, že MS SR v tomto období na súdoch nevykonalo žiadnu kontrolu.**

Ďalej NKÚ SR v rámci kontroly skonštatoval, že ak nastavený model samotného výkonu dozoru na súdoch má fungovať v rámci MS SR, ktoré je orgánom výkonnej moci a ktoré prostredníctvom ministra riadi, koordinuje a kontroluje vláda SR, **potom nemožno hovoriť o nezávislom výkone právomocí členov osobitného orgánu dozoru kontrolovať spracúvanie osobných údajov na nezávislých súdoch pri výkone ich súdnej právomoci a MS SR by malo zvážiť jeho zmenu.** Na porovnanie, v Českej republike dozor nad ochranou osobných údajov na súdoch pri výkone ich súdnej právomoci zverili osobitným orgánom, ktoré zriadili priamo na nezávislých súdoch.

V minulosti EK pri rôznych rokovaniach viackrát upozornila SR a vyslovila vážne pochybnosti, že postavenie ÚOOÚ SR a výkon jeho právomocí v rozpočtovej a finančnej oblasti nie je úplne nezávislý a vo vnútroštátnom právnom poriadku SR nie je upravený v súlade s právom EÚ. Nariadenie (EÚ) výslovne ustanovuje požiadavku, aby členské štáty EÚ takéto nezávislé postavenie, ako aj rozpočtovú nezávislosť dozornej autorite priznali. **To sa však v rámci implementácie príslušných článkov nariadenia prostredníctvom nového zákona č. 18/2018 Z. z. o ochrane osobných údajov nestalo.**

Všetky kontrolované subjekty, u ktorých boli zistené porušenia právnych predpisov majú **zákonnú povinnosť prijať** v stanovených termínoch **opatrenia na odstránenie zistených nedostatkov a zaslať správu o ich plnení.** NKÚ SR zároveň **odporúča ÚOOÚ SR, aby v spolupráci so zodpovednými inštitúciami preskúmal obsah zákona č. 18/2018 Z. z. a čl. 51 ods.1 a čl. 52 ods. 6 Nariadenia (EÚ)** a prehodnotil, či požiadavky vyplývajúce z Nariadenia (EÚ) boli prevzaté v požadovanom rozsahu a spôsobom, ktorý je primerane zrozumiteľný pre prevádzkovateľov a dotknuté osoby a či požiadavky týkajúce sa nezávislosti postavenia dozorných orgánov na ochranu osobných údajov boli správne implementované do vnútroštátneho poriadku. NKÚ SR taktiež **ÚOOÚ SR odporúča**, aby využil zistenia zo Záverečnej správy ako zdôvodnenie pre **vypracovanie analýzy finančnej náročnosti** zabezpečenia ochrany osobných údajov vo verejnom sektore v **spolupráci s MF SR.**

1 ÚČEL KONTROLNEJ AKCIE

Účelom kontrolnej akcie bolo preveriť súlad konania orgánov verejnej správy so všeobecne záväznými právnymi predpismi platnými pre oblasť ochrany osobných údajov účinnými v SR od 25. mája 2018 a zriadenie nového orgánu dozerajúceho na spracúvanie osobných údajov na súdoch pri výkone ich súdnej právomoci.

Predmetom kontroly bolo zistiť:

- rozsah prijatých opatrení prevádzkovateľmi na uvedenie spracúvania osobných údajov do súladu s Nariadením (EÚ)
- stav zabezpečenia osobných údajov občanov v IS
- objem finančných prostriedkov vynaložených na implementáciu povinností podľa Nariadenia (EÚ)
- úroveň zrozumiteľnosti prijatej legislatívy pre oblasť ochrany osobných údajov, účinnej od 25. mája 2018 pre prevádzkovateľov
- zriadenie osobitného orgánu dozoru v rámci systému súdnictva.

2 RÁMEC KONTROLNEJ AKCIE

Kontrolná akcia **bola vykonaná v období od júna do decembra 2019,** t. j. **rok po nadobudnutí účinnosti Nariadenia (EÚ) a zákona č. 18/2018 Z. z.**

V rámci kontrolnej akcie bolo preverených **62 subjektov prevádzkovateľov IS** spracúvajúcich osobné údaje vo verejnom sektore **a MS SR**. Prevádzkovatelia IS boli vybraní tak, aby v rámci kontroly mali zastúpenie rôzne orgány verejnej správy a to plošne v rámci celej SR. Podstatným kritériom pri výbere orgánov štátu bol rozsah, obsah a dôležitosť IS, v ktorých prevádzkovatelia spracúvajú osobné údaje občanov SR. Kontrola na MS SR mala osobité zameranie.

Tabuľka č. 1: Kontrolované subjekty

Orgány verejnej správy	**Kontrolované subjekty**						
Orgány štátu	MPSVaR SR	ÚPSVaR SR	Sociálna poisťovňa	ÚGKK SR	DataCentrum	VšZP	**MS SR**
VÚC	BSK	KSK	NSK	ŽSK			
Krajské mestá	Banská Bystrica	Trenčín	Prešov				
Okresné mestá	Kysucké Nové Mesto	Michalovce	Považská Bystrica	Piešťany	Žarnovica	Zlaté Moravce	Sabinov
Obce od 1 do 500 obyvateľov	Dolné Otrokovce	Jalšové	Kotrčiná Lúčka	Nezbudská Lúčka	Čavoj	Dlžín	Zbrojníky
	Zalaba	Baláže	Moštenica	Babie	Petrovce	Belža	Bočiar
Obce od 501 do 3000 obyvateľov	Bojničky	Hermanovce nad Topľou	Pohronský Ruskov	Zemianske Kostoľany	Červeník	Lutiše	Krasňany
	Oslany	Hronovce	Podkonice	Trakovice	Šarovce	Bystré	Liešťany
	Staré Hory	Vyšný Žipov	Gbeľany	Povrazník	Geča	Ždaňa	Sokoľany
Obce od 3001 do 6000 obyvateľov	Leopoldov	Slovenská Ľupča	Čaňa	Želiezovce	Hanušovce nad Topľou	Varín	Nováky

Zdroj: NKÚ SR

Kontroly boli vykonané v súlade so zákonom o NKÚ SR a so štandardmi, ktoré vychádzajú zo základných princípov medzinárodných štandardov najvyšších kontrolných inštitúcií (ISSAI), ako kontroly súladu. **Kontrolovaným obdobím** boli **roky 2016 – 2019** a súvisiace predchádzajúce obdobia. **Hodnotiacimi kritériami** boli najmä právne normy – Nariadenie (EÚ), zákon č. 18/2018 Z. z. a výnos MF SR.

3 ZISTENIA A ODPORÚČANIA

3.1 OCHRANA OSOBNÝCH ÚDAJOV V EÚ A SR

V SR patrí právo na ochranu osobných údajov medzi základné práva a slobody zakotvené v Ústave SR. Predmetné právo upravuje Čl. 19 Ústavy SR, podľa ktorého každý má právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe, a je súčasťou ústavou garantovaného práva na rešpektovanie súkromného života.

Osobné údaje sú prevádzkovateľmi spracúvané naprieč celým verejným aj súkromným sektorom a ochrana a spracúvanie osobných údajov sa týka všetkých občanov SR bez výnimky. Ochrana osobných údajov neznamená ich neposkytovanie zo strany občanov, ale znamená zabezpečenie nenarušenia vážnosti, dôstojnosti a bezpečnosti osôb, ktoré osobné údaje poskytli verejnému alebo súkromnému subjektu na účely ich ďalšieho spracovania. Bezpečnosť osobných údajov sú prevádzkovatelia povinní zabezpečiť **bez ohľadu na to, aký je prevádzkovateľ veľký a koľko osobných údajov a ako dôležitých o dotknutých osobách v IS spracúva.**

Každý orgán verejnej správy je s určitosťou prevádzkovateľom personálnej a mzdovej agendy a správy registratúry. Štát okrem toho prevádzkuje ďalšie stovky databáz, IS a registrov (matriku, kataster nehnuteľností, daňový IS, register trestov, evideciu obyvateľov, IS súdov, databázu občianskych preukazov, rezortný IS školstva, IS sociálnej poisťovne, národné zdravotné registre a ďalšie), **v ktorých spracúva osobné údaje v elektronickej a papierovej forme**, v mnohých prípadoch prostredníctvom samospráv v rámci preneseného výkonu štátnej správy.

V rámci predvstupových rokovaní SR do EÚ bola SR povinná zosúladiť svoj právny poriadok s právom EÚ a v oblasti ochrany osobných údajov prebrať do svojho právneho systému základné princípy Smernice 95/46/ES. Na tento účel bol prijatý zákon č. 428/2002 Z. z. o ochrane osobných údajov, ktorý s účinnosťou od 1. septembra 2002 nielen transponoval predmetnú smernicu do právneho poriadku SR, ale zákonom bola zriadená aj dozorná autorita pre oblasť ochrany osobných údajov v SR, ÚOOÚ SR.

Dňa 25. januára 2012 Európska komisia predstavila nový právny rámec ochrany osobných údajov, ktorý bol v rokoch 2012 – 2016 pripomienkovaný členskými štátmi EÚ. V júli 2013 zákon o ochrane osobných údajov z roku 2002 v SR nahradil zákon č. 122/2013 Z. z. **Princípy ochrany osobných údajov sú teda prevádzkovatelia IS povinní v SR aplikovať kontinuálne od septembra 2002,** čo znamená, že **ochrana osobných údajov nie je novou oblasťou, s ktorou by sa prevádzkovatelia začali len teraz zoznamovať.**

Finálne znenie **GDPR** (General Data Protection Regulation), t. j. všeobecného Nariadenia (EÚ) o ochrane údajov **nadobudlo platnosť 25. mája 2016**. Od tohto momentu začalo plynúť **dvojročné prechodné obdobie**, počas ktorého boli povinné všetky subjekty verejného aj súkromného sektora, spracúvajúce osobné údaje v IS (prevádzkovatelia), pripraviť sa na jeho **uplatňovanie v plnom rozsahu od 25. mája 2018**. Na základe Nariadenia (EÚ) bola SR **opätovne postavená pred úlohu zriadiť nezávislý orgán dozoru** na ochranu osobných údajov, **tentoraz v rámci systému súdnictva**.

Nariadenie (EÚ) má charakter európskeho zákona, ktoré je priamo účinné, vykonateľné a uplatniteľné na území každého členského štátu EÚ bez nutnosti prijatia vnútroštátnych vykonávacích predpisov. Nariadenie dáva členským štátom priestor upraviť len niektoré jeho články v zmysle národných špecifík. Dňom 25. mája 2018 teda došlo nielen k zrušeniu dovtedy platnej Smernice 95/46/ES, ale aj k zrušeniu zákona č. 122/2013 Z. z., ktorý s účinnosťou od 25. mája 2018 nahradil **nový zákon č. 18/2018 Z. z. a doplnil Nariadenie (EÚ) na národnej úrovni**.

Štát je povinný postarať sa v súlade s princípmi zakotvenými v Nariadení (EÚ) o bezpečnosť osobných údajov svojich občanov, ktoré od nich vyžaduje na rôzne účely a spracúva vo svojich IS.

3.2 SÚLAD PRIJATÝCH OPATRENÍ S NARIADENÍM (EÚ), ZÁKONOM Č.18/2018 Z. Z. A VÝNOSOM MF SR

Proces kontroly preverovania súladu prijatých opatrení s Nariadením (EÚ), zákonom č. 18/2018 Z. z. a výnosom MF SR bol **rozdelený do niekoľkých ucelených samostatných oblastí**, v rámci ktorých boli prevádzkovateľom s výnimkou MS SR kladené rovnaké otázky, ktorým bolo priradené bodové ohodnotenie (váha) a v závere boli vyhodnotené podľa jednotnej metodiky NKÚ SR s výsledkom na škále od známky 1 (najlepšie hodnotenie pre prevádzkovateľa) do 5 (najhoršie hodnotenie pre prevádzkovateľa). Otázky boli zoradené do oblastí:

- *analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ)* (3.2.1)
- *práva dotknutej osoby – pravidlá, postupy a oznámenia* (3.2.2)
- *výkon funkcie zodpovednej osoby* (3.2.3)
- *stav ochrany osobných údajov v oblasti bezpečnosti spracúvania údajov* (3.2.4)
- *zrozumiteľnosť legislatívy (nariadenia a zákona č. 18/2018 Z. z.), metodík a usmernení vydaných ÚOOÚ SR pre prevádzkovateľov* (3.3)
- *finančné prostriedky a ľudské zdroje vyčlenené na ochranu osobných údajov* (3.4)

Oblasť *zrozumiteľnosť legislatívy, metodík a usmernení vydaných ÚOOÚ SR pre prevádzkovateľov* sa od ostatných oblastí odlišovala v tom, že v rámci nej nebol hodnotený prevádzkovateľ, ale na základe vyjadrení prevádzkovateľa bola hodnotená **úroveň zrozumiteľnosti** Nariadenia (EÚ), zákona č. 18/2018 Z. z. a metodík a usmernení vydaných ÚOOÚ

SR pre prevádzkovateľa podľa jednotnej metodiky NKÚ SR s výsledkom na škále od známky 1 (legislatíva a metodika je zrozumiteľná) do 5 (legislatíva a metodika je nezrozumiteľná).

Niektoré ďalšie podrobnosti o zisťovaní podľa jednotnej metodiky NKÚ SR sú uvedené v Prílohe tejto záverečnej správy.

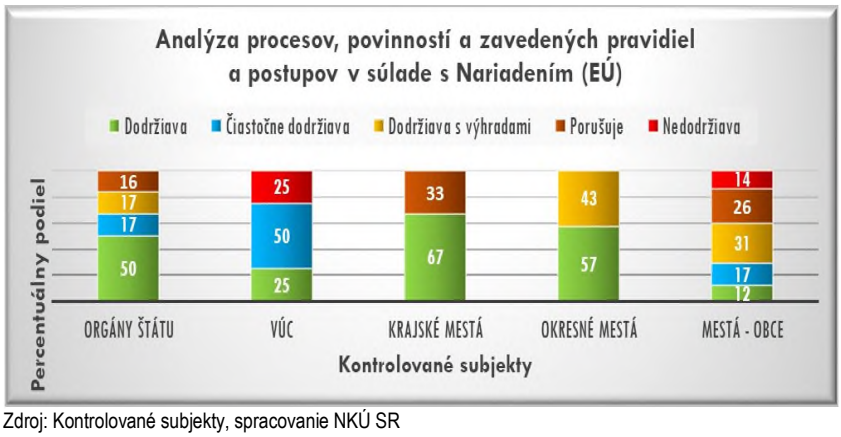
3.2.1 Analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ)

Pred nadobudnutím účinnosti Nariadenia (EÚ) bolo potrebné zo strany každého prevádzkovateľa: (**1**) analyzovať technické a organizačné opatrenia v oblasti ochrany osobných údajov, prijaté podľa zákona č. 122/2013 Z. z., (**2**) porovnať ich s požiadavkami kladenými na bezpečnosť spracúvania osobných údajov a zabezpečenie uplatňovania práv dotknutých osôb podľa Nariadenia (EÚ) a zákona č. 18/2018 Z. z., (**3**) identifikovať rozdiely, navrhnúť technické a organizačné opatrenia potrebné na elimináciu zistených nedostatkov a (**4**) prijať adekvátne opatrenia na plné zabezpečenie spracúvania osobných údajov v súlade s novým právnym stavom najneskôr do 25. mája 2018.

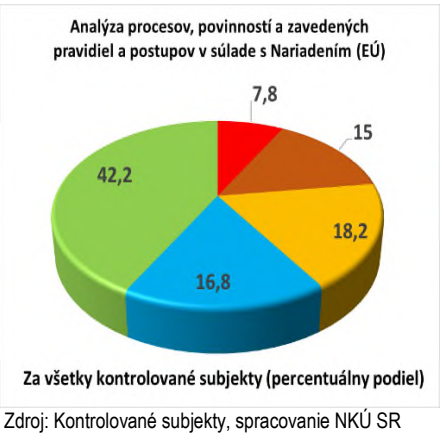
Kontrolou NKÚ SR bolo zistené, že **42 %** zo všetkých kontrolovaných subjektov túto **úlohu splnilo včas** a **17 %** ju **splnilo s oneskorením**. Ďalších **18 %** kontrolovaných subjektov síce **analýzu vykonalo oneskorene, avšak ani v čase kontroly**, t. j. po jednom roku od nadobudnutia účinnosti Nariadenia (EÚ), väčšina z nich **nevedela preukázať, že opatrenia identifikované v analýze na zosúladenie stavu spracúvania zaviedla do praxe**. Ostatných **23 %** kontrolovaných subjektov sa touto úlohou (analýzou) buď **nezaoberalo vôbec** alebo len veľmi **okrajovo**.

Graf č. 1: Analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ) podľa charakteru (typu) kontrolovaných subjektov

Graf č. 2: Analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ) komplexne za všetky kontrolované subjekty



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Podľa právnej úpravy, platnej do 25. mája 2018, boli prevádzkovatelia povinní v súvislosti s prijímaním technických, organizačných a personálnych opatrení na zabezpečenie ochrany osobných údajov v IS, vypracúvať **bezpečnostný projekt**. Viaceré kontrolované subjekty mali takéto bezpečnostné projekty vypracované, avšak **väčšina z nich bola staršieho dáta a niekoľko rokov neboli aktualizované**. Pozitívom je, že takmer **tri štvrtiny kontrolovaných subjektov podrobili celý svoj systém analýzam**, v ktorých sa často medzi navrhovanými opatreniami objavovalo odporúčanie, aby prevádzkovateľ existujúcu dokumentáciu vypracovanú na základe bezpečnostného projektu prepracoval, chýbajúcu dopracoval, alebo vypracoval úplne novú.

Viaceré analýzy taktiež odhalili, že niektoré opatrenia, ktoré mali byť formalizované už podľa zákona č. 122/2013 Z. z., **boli vykonávané len zaužívaným spôsobom a v závislosti od znalostí a skúseností zainteresovaných zamestnancov**. **Tento prístup bol NKÚ SR vyhodnotený ako neakceptovateľný najmä z toho dôvodu, že Nariadenie (EÚ) prináša nové povinnosti a požaduje zaviesť nové prístupy.** Znamená to najmä, aby oprávnené osoby (zamestnanci spracúvajúci osobné údaje) mali prevádzkovateľom jasné zadefinované pravidlá, boli o nich preukázateľne poučení, zaviazaní ich dodržiavaním a presne vedeli, na čo sú v súvislosti so spracúvaním údajov oprávnení, resp. čo nesmú, aby nezapríčinili porušenie ochrany osobných údajov. Preto analýzy spravidla prevádzkovateľom odporúčali vypracovať plán implementácie navrhovaných opatrení a ich postupnej realizácie.

Pri spracovávaní osobných údajov, pri ktorých sa prevádzkovateľ **musí riadiť podmienkami ustanovenými zákonom**, **kontrolované subjekty v praxi nemali podstatné problémy** a väčšina z nich na tento účel zaviedla opatrenia

prostredníctvom pokynov alebo poučení pre oprávnené osoby. Kontrolou NKÚ SR boli zistené nasledovné **príklady zlej praxe**:

- **kontrolované subjekty väčšinou nedisponovali pokynmi pre zamestnancov o postupoch poskytovania informácií o štátnom zamestnancovi na základe zákona o štátnej službe,** podľa ktorého *služobný úrad môže poskytovať informácie o štátnom zamestnancovi len na základe osobitného predpisu alebo s jeho písomným súhlasom*
- niektorí **prevádzkovatelia stále vyžadovali súhlas dotknutej osoby so spracúvaním jej osobných údajov na účel plnenia zmluvy, ktorej zmluvnou stranou bola dotknutá osoba (napr. pracovná zmluva)**, aj keď jeho vyžadovanie v tomto prípade je v rozpore s Nariadením (EÚ)
- **viaceré kontrolované subjekty nedisponovali pravidlami a pokynmi pre oprávnené osoby** v súvislosti s vedením evidencie o pracovných úrazoch (napr. záznam o registrovanom pracovnom úraze), pri spracovaní údajov o členstve v odborovej organizácii, pri výkone kontrolnej činnosti na základe zákona o BOZP (zisťovanie prítomnosti omamných alebo psychotropných látok u zamestnanca v pracovnej dobe).

*Podľa jednotnej metodiky NKÚ SR je stav ochrany osobných údajov v oblasti analýzy procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ) v SR v rámci kontrolovanej vzorky ohodnotený **v priemere známkou 2,65**.*

3.2.2 *Práva dotknutej osoby – pravidlá, postupy a oznámenia*

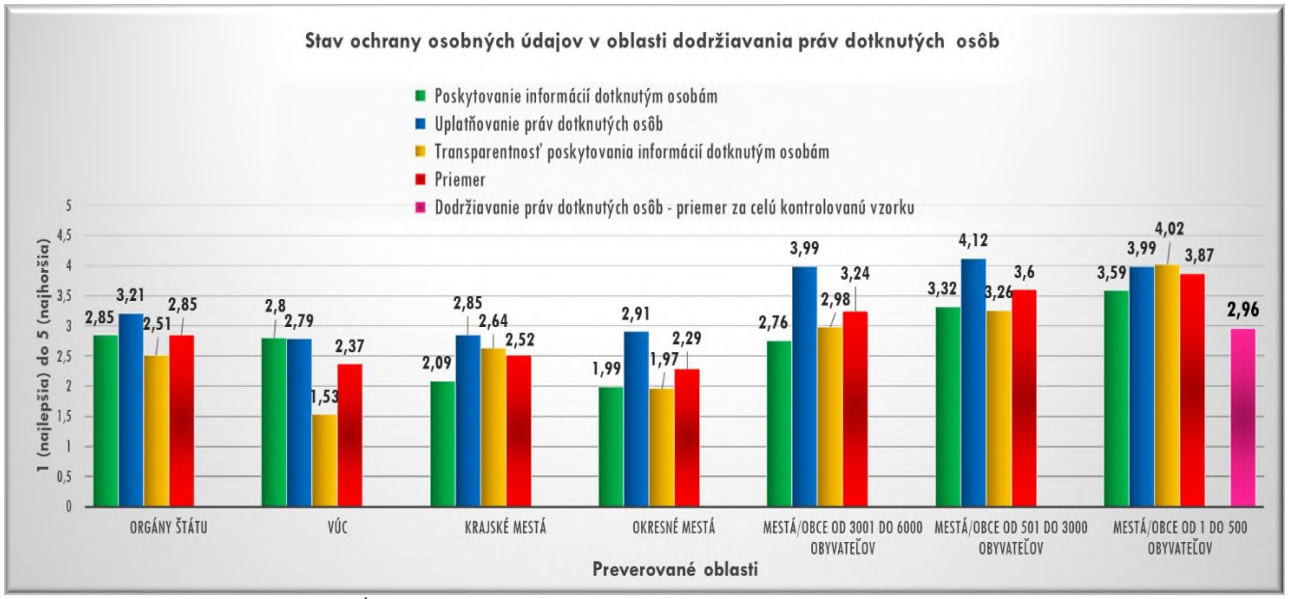
Do 25. mája 2018 bol každý prevádzkovateľ povinný prijať primerané interné smernice upravujúce zákonný, jednotný a transparentný postup jeho zamestnancov pri komunikácii s dotknutými osobami.

Poskytovanie informácií dotknutým osobám

Ak prevádzkovateľ získava osobné údaje priamo od dotknutej osoby, musí ju vopred oboznámiť s podmienkami ich spracúvania, pričom, ak osoba danými informáciami už disponuje, takéto oboznámenie nie je potrebné. Väčšina prevádzkovateľov vykonala opatrenia a v pokynoch formálne zadefinovala zamestnancom povinnosti, ktoré by mali viesť k informovaniu osôb, avšak pokyny neboli spravidla tak podrobné, aby pokrývali celý rozsah požiadaviek Nariadenia (EÚ). Ani komunikácia zamestnancov pri získavaní osobných údajov sa často nezačínala oboznámením osoby s možnosťami uplatnenia si jej práv podľa nariadenia a ani tým, za akých okolností a v akých prípadoch sa informácie osobám neposkytujú.

Z grafu č. 3 vyplýva, že z vyhodnotenia poskytovania informácií dotknutým osobám **najlepšie obstáli okresné mestá** a **najhoršie skončili mestá/obce od 1 – 500 obyvateľov**, pričom zo vzorky 14 obcí, tri z nich dosiahli hodnotenie *„nedodržiava“*.

Graf č. 3: Stav ochrany osobných údajov v oblasti dodržiavania práv dotknutých osôb



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Uplatňovanie práv dotknutých osôb

Na základe Nariadenia (EÚ) si **dotknuté osoby môžu u prevádzkovateľa uplatniť viacero práv,** medzi ktoré patrí napríklad **právo na prístup k svojim osobným údajom, právo „na zabudnutie", právo na obmedzenie spracúvania údajov, právo na prenosnosť údajov**, alebo môže osoba využiť **právo na odvolanie súhlasu**, prípadne **namietať proti rozhodnutiu** založenom výlučne na automatizovanom spracúvaní osobných údajov alebo proti profilovaniu.

Na tento účel je nevyhnutné, aby mal prevádzkovateľ vypracované usmernenia a zdokumentované pokyny pre zamestnancov, ako majú postupovať v konkrétnych prípadoch, keď si osoba uplatní dané právo.

Ak dotknutá osoba prevádzkovateľovi oznámi alebo ten na základe vlastnej činnosti zistí, že spracúva nesprávne alebo neúplné osobné údaje, ktoré je nútený opraviť, vymazať alebo obmedziť ich spracúvanie, prevádzkovateľ je povinný to oznámiť každému, komu predmetné osobné údaje poskytol. Zamestnanci musia byť poučení o tejto povinnosti a zodpovednosti za jej nesplnenie, pretože neoznámenie môže znamenať pre prevádzkovateľa sankčný postih.

Pri uplatňovaní práv dotknutých osôb najlepšie obstáli VÚC a najhoršie dopadli mestá/obce od 501 – 3 000 obyvateľov. Z nich zo vzorky 21 obcí až desať dosiahlo hodnotenie *„porušuje alebo nedodržiava"* a len štyri obce sa pohybovali v oblasti hodnotenia *„dodržiava"*. Zo vzorky 14 miest/obcí od 1 – 500 obyvateľov sa až polovica z nich nachádzala v pásmach hodnotenia *„porušuje alebo nedodržiava"* povinnosti ustanovené Nariadením (EÚ).

Transparentnosť poskytovania informácií dotknutým osobám

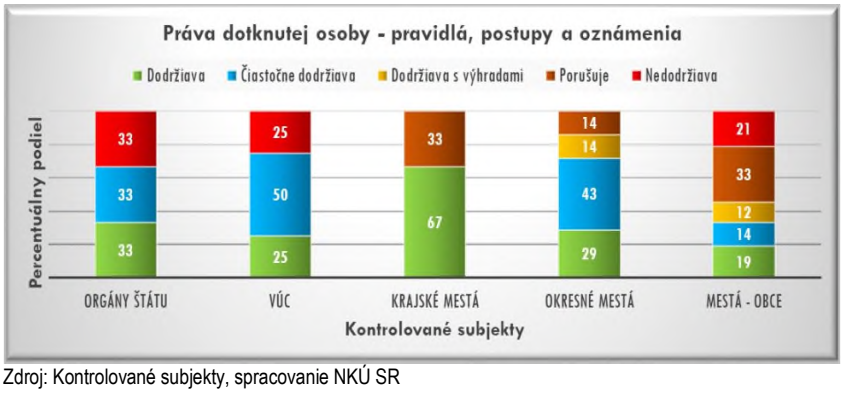
Zásada transparentnosti si vyžaduje, aby všetky informácie určené dotknutým osobám a verejnosti boli stručné, ľahko prístupné, pochopiteľné, dobre viditeľné a formulované jasne a jednoducho. **Zákonné, spravodlivé a transparentné spracúvanie si vyžaduje, aby osoba bola informovaná úplne a včas o existencii všetkých spracovateľských operácií a o ich účele v súvislosti so spracúvaním jej osobných údajov**.

Informácie pre verejnosť o jednotlivých právach, ktoré si dotknutá osoba môže u prevádzkovateľa uplatniť, vrátane odkazu na právo podať sťažnosť dozornému orgánu, informáciách o IS, právnom základe a účele spracúvania osobných údajov, **kontrolované subjekty zverejňovali na svojich webových sídlach, aj keď nie vždy v požadovanom rozsahu**. Na webovej stránke sú povinní v súlade s Nariadením (EÚ) zverejňovať aj kontaktné údaje na zodpovednú osobu organizácie.

Najlepšie hodnotenie dosiahli VÚC. Dobré výsledky dosiahli aj okresné mestá a orgány štátu. Najhoršie výsledky v súvislosti s transparentným poskytovaním informácií verejnosti dosiahli mestá/obce od 1 do 500 obyvateľov, pričom zo vzorky 14 obcí skončilo s hodnotením *„nedodržiava"* až šesť obcí.

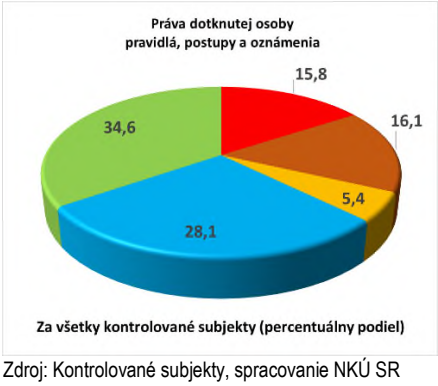
Alarmujúcim zistením je, že až tretina kontrolovaných subjektov vôbec alebo len vo veľmi obmedzenej forme plnila povinnosti ustanovené Nariadením (EÚ) v oblasti dodržiavania práv dotknutých osôb a ďalšia tretina z nich dodržiavala ich len čiastočne.

Graf č. 4: Práva dotknutej osoby – pravidlá, postupy a oznámenia podľa charakteru (typu) kontrolovaných subjektov



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Graf č 5: Práva dotknutej osoby – pravidlá, postupy a oznámenia komplexne za všetky kontrolované subjekty



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

*Podľa jednotnej metodiky NKÚ SR je stav ochrany osobných údajov v oblasti dodržiavania práv dotknutých osôb v rámci kontrolovanej vzorky ohodnotený **v priemere známkou 2,96**.*

3.2.3 Výkon funkcie zodpovednej osoby

Orgány verejnej moci a verejnoprávne subjekty spracúvajúce osobné údaje boli povinné na základe Nariadenia (EÚ) od 25. mája 2018 určiť tzv. zodpovednú osobu. Inštitút zodpovednej osoby nie je pre prevádzkovateľov novou

povinnosťou, veď pomenovanie ako dohľad nad ochranou osobných údajov platilo už podľa zákona č. 428/2002 Z. z., pričom zákonom č. 122/2013 Z. z. bolo rozšírené aj na sprostredkovateľov a platilo až do 25. mája 2018.

Zodpovedná osoba poverená podľa zákona č. 122/2013 Z. z. priamo rozhodovala o účeloch a prostriedkoch spracúvania a za plnenie úloh niesla zodpovednosť. Prevádzkovateľ ju mohol kedykoľvek bez udania dôvodu odvolať a dokonca podľa vyhláseného znenia zákona č. 122/2013 Z. z., ÚOOÚ SR mal oprávnenie zodpovednej osobe uložiť pokutu do 3 000 eur, ak si povinnosti podľa zákona neplnila.

Podľa Nariadenia (EÚ) sú však postavenie a pôsobnosť zodpovednej osoby úplne iné. Úlohou zodpovednej osoby je vykonávať permanentný dohľad nad spracovaním osobných údajov u prevádzkovateľa. Na zistené nedostatky môže len upozorňovať, informovať o nich najvyššie vedenie organizácie a poskytovať prevádzkovateľovi poradenstvo. Zodpovedná osoba nesmie plniť úlohy spojené s rozhodovaním o účeloch a prostriedkoch spracúvania osobných údajov, a prevádzkovateľ ju nesmie odvolať alebo postihovať za výkon jej úloh, t. z., že **musí podliehať najvyššiemu vedeniu prevádzkovateľa alebo sprostredkovateľa, ba v súvislosti s plnením úloh nesmie dostávať žiadne pokyny.** Zodpovedná osoba síce môže plniť aj iné úlohy alebo povinnosti v rámci organizácie, avšak žiadna z nich nesmie viesť ku konfliktu záujmov.

Kontrolou výkonu funkcie zodpovednej osoby bolo zistené toto.

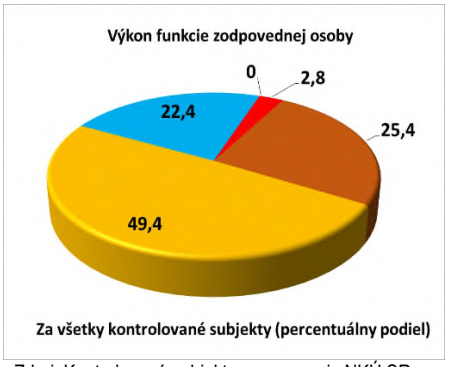
- **Výkon činnosti zodpovednej osoby bol vo väčšine prípadov formálny.** Viaceré interné zodpovedné osoby nevedeli predložiť záznamy o plnení svojich úloh (neviedli ich na týždňovej, ani na mesačnej báze), nemali vypracovanú výročnú správu o svojej činnosti, neviedli výstupy z monitorovania svojej činnosti pri praktickom výkone ochrany údajov v teréne, viacerí nevedeli doložiť dôkaz o vykonaní odbornej prípravy (školení) personálu a zvyšovaní povedomia oprávnených osôb a pod. V zmluvách uzatváraných s obcami sa externé spoločnosti síce zaviazali k plneniu úloh uložených Nariadením (EÚ), avšak podľa vyjadrení viacerých obcí sa toto plnenie **neuskutočňuje zo strany externej zodpovednej osoby systematicky a kontinuálne,** ale spravidla podľa princípu ***„ak vznikne problém, zavolajte alebo pošlite email“***.
- **Interná zodpovedná osoba** bola najčastejšie zaradená do odboru krízového manažmentu a bezpečnosti, odboru informatiky, odboru bezpečnosti IS, odboru kybernetickej bezpečnosti, či do sekcie koordinácie výkonu štátnej správy, t. z., že **priamo nepodliehala najvyššiemu vedeniu prevádzkovateľa.**
- **Zodpovedné osoby sa vo väčšine kontrolovaných subjektov nezúčastňovali zasadaní najvyššieho vedenia organizácie, na ktorých sa riešili otázky ochrany údajov a informačnej bezpečnosti.** Svoje návrhy, rady a odporúčania týkajúce sa ochrany údajov väčšinou delegovali interné zodpovedné osoby najvyššiemu vedeniu **len sprostredkovane, cez riaditeľov,** pričom o takýchto návrhoch zodpovedných osôb neexistovali na kontrolovaných subjektoch žiadne relevantné záznamy, dôkazy, napríklad z porady odboru, z rokovania najvyššieho vedenia a pod. Niektoré mestá a obce **neudelili externým zodpovedným osobám prístupové práva do potrebných IS** a **neprizývali ich na zasadania mesta**, ale problémy s nimi konzultovali separátne.
- **Nepochopenie inštitútov *„sprostredkovateľ“ a „zodpovedná osoba“.*** Podľa Nariadenia (EÚ) platí, že **sprostredkovateľ spracúva osobné údaje v mene prevádzkovateľa výlučne na základe jeho pokynov**, a to v rozsahu a za podmienok dohodnutých v zmluve. Naproti tomu **zodpovedná osoba nesmie dostávať od prevádzkovateľa žiadne pokyny a plniť úlohy** spojené s rozhodovaním o účeloch a prostriedkoch spracúvania osobných údajov. **Zodpovedná osoba nesmie svoju funkciu vykonávať v postavení sprostredkovateľa.**
- **Všetky kontrolované subjekty financovali činnosť výlučne z prostriedkov svojho rozpočtu bez poskytnutia dodatočných finančných prostriedkov zo strany štátu.** Kontrolované subjekty, u ktorých **výkon funkcie zodpovednej osoby vykonával interný zamestnanec**, nemali priamo určenú odmenu za výkon jej činnosti. Odmena bola spravidla súčasťou celkovej mzdy zamestnanca a reálne náklady bolo možné určiť len približne po konzultáciách s kontrolovaným subjektom. Jej výška sa pohybovala v rozmedzí cca od 350 do 550 eur vrátane odvodov zamestnávateľa mesačne. **Odmena za výkon funkcie zodpovednej osoby, ktorú vykonávala externá osoba (spoločnosť)**, bola značne rozdielna. Výška odmeny rástla s veľkosťou obce a mesta. Malé obce sa zväčša pohybovali v rozmedzí cca od 30 do 90 eur mesačne s DPH, a okresné a krajské mestá od 120 do 1 100 eur s DPH mesačne.

Napriek tomu, že inštitút zodpovednej osoby nie je nový, len 22,4 % zo všetkých kontrolovaných subjektov ho zaviedlo v rámci organizácie relatívne v súlade s požiadavkami ustanovenými Nariadením (EÚ). Polovica zo všetkých subjektov povinnosti síce dodržiava, ale s určitými výhradami a cca 25 % subjektov povinnosti viac porušuje než dodržiava.

Graf č. 6: Výkon funkcie zodpovednej osoby podľa charakteru (typu) kontrolovaných subjektov

Graf č. 7: Výkon funkcie zodpovednej osoby komplexne za všetky kontrolované subjekty

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Potvrdil sa predpoklad NKÚ SR o nevhodnosti zachovania pôvodného názvu *„zodpovedná osoba“* podľa predchádzajúcej právnej úpravy. Z vyjadrení kontrolovaných subjektov a ďalších zistení pri kontrole vyplynulo, že slabšie výsledky zavedenia inštitútu *zodpovednej osoby* do praxe idú na vrub aj nesprávneho prekladu názvu tejto osoby označenej ako **„zodpovedná“, ktorá vlastne podľa Nariadenia (EÚ) už „zodpovednou“ nie je**. Tomuto názvu totiž nezodpovedá ani preklad originálu textu Nariadenia (EÚ) tejto osoby v anglickom jazyku *„Data protection officer“*. Jeho doslovný preklad je *„Úradník pre ochranu údajov“*. **Vo viacerých prípadoch si kontrolovaný subjekt až po vysvetlení NKÚ SR uvedomil, že postavenie a pôsobnosť *zodpovednej osoby* pochopil nesprávne** a kreoval ju v intenciách, ako na to bol zvyknutý podľa zákona č. 122/2013 Z. z. a nie ako mu to ukladá Nariadenie (EÚ).

Vyhodnotenie podľa jednotnej metodiky NKÚ SR je uvedené na konci podkapitoly 3.2.4. Stav ochrany osobných údajov v oblasti bezpečnosti spracúvania údajov.

3.2.4 Stav ochrany osobných údajov v oblasti bezpečnosti spracúvania údajov

Do 25. mája 2018 bol prevádzkovateľ povinný prijať vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie údajov vykonáva v súlade s Nariadením (EÚ). Na tento účel mal prijať primerané politiky ochrany údajov (smernice) a zabezpečiť, aby každá fyzická osoba, ktorú poveril spracúvaním a tá získala prístup k osobným údajom vrátane sprostredkovateľa, spracúvala tieto údaje len na základe pokynov prevádzkovateľa.

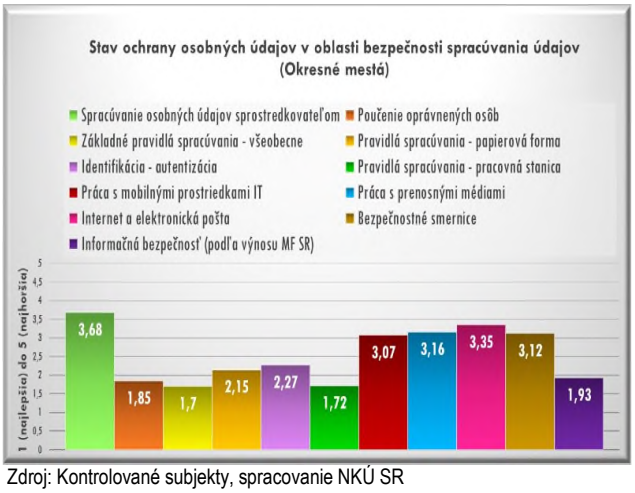
Všeobecné základné pravidlá platné pre oprávnené osoby – zamestnancov pri spracúvaní osobných údajov v papierovej forme a ich poučenie o povinnostiach pri spracúvaní údajov v zodpovedajúcom rozsahu prijala podstatná väčšia kontrolovaných subjektov. Tieto povinnosti v relatívne prijateľnej miere plnili aj menšie mestá a obce.

Grafy č. 8 až 11: Vyhodnotenie stavu ochrany osobných údajov v oblasti bezpečnosti spracúvania údajov (Orgány štátu, VÚC, Krajské mestá, Okresné mestá)

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Najčastejšie sa opakujúce pochybenia kontrolovaných subjektov v oblasti bezpečnosti spracúvania údajov, zistené v priebehu výkonu kontroly NKÚ SR, boli tieto.

Spracúvanie osobných údajov sprostredkovateľom

Väčšina kontrolovaných subjektov mala najväčšie rezervy v oblasti spracúvania osobných údajov sprostredkovateľmi. **Prevádzkovatelia buď nepreverovali sprostredkovateľov, či poskytujú dostatočné záruky, že prijmú primerané technické a organizačné opatrenia, alebo ak aj potvrdili, že ich preverovali, nevedeli preukázať ani popísať, ako ich preverovali.** Kontrolované subjekty väčšinou:

- **nemali vypracovanú internú smernicu pre prípravu sprostredkovateľských zmlúv** v rozsahu podmienok požadovaných podľa článku 28 Nariadenia (EÚ).
- **nemali upravené pravidlá a pokyny pre oprávnené osoby**, ako majú postupovať **pri preverovaní osôb** (potenciálnych sprostredkovateľov), **či poskytujú dostatočné záruky**.
- **oprávnené osoby neboli usmernené, ako majú vybrať a poveriť externého audítora**, resp. ako majú postupovať pri kontrole/audite u sprostredkovateľa, pri ktorom je sprostredkovateľ povinný prevádzkovateľovi alebo externému audítorovi preukázať, že plní/splnil všetky povinnosti ustanovené v článku 28 Nariadenia (EÚ). Napr., že dodržiava dohodnuté podmienky upravené v zmluve, že spracúva osobné údaje na základe a v súlade so zdokumentovanými pokynmi prevádzkovateľa, že všetky oprávnené osoby sprostredkovateľa spracúvajú osobné údaje výlučne na základe jeho pokynov, že plní podmienky bezpečného spracúvania osobných údajov vo svojich IS a pod.

Bezpečnostné smernice

Absencia bezpečnostných smerníc sa netýkala len oblasti spracúvania osobných údajov sprostredkovateľom. Prevádzkovatelia v SR si zrejme nie celkom správne vysvetlili informáciu, že podľa Nariadenia (EÚ) už nie je potrebné vypracúvať bezpečnostné projekty, ktoré boli povinní zabezpečiť podľa predchádzajúcej právnej úpravy. **Podľa článku 24 Nariadenia (EÚ) sú však povinní prijať vhodné technické a organizačné opatrenia a zabezpečiť, aby boli kedykoľvek schopní preukázať, že spracúvanie osobných údajov vykonávajú v súlade s nariadením a na tento účel prijať (zaviesť) primerané politiky ochrany údajov (smernice, pokyny, usmernenia).**

Spracúvanie osobných údajov v elektronickej forme

- *Práca s počítačom*

Najčastejším nedostatkom prevádzkovateľov bolo, že zamestnancov neupozornili, resp. im nezakázali používanie ich pracovnej stanice osobami, ktoré nie sú v postavení oprávnených osôb, nezaviazali ich povinnosťou nahlasovať administrátorovi akékoľvek zlyhanie alebo neštandardné správanie sa systému, ani povinnosťou preverovať antivírovým programom súbory ukladané na pevný disk počítača, nezasahovať do bezpečnostnej konfigurácie nainštalovaného softvéru, ani neinštalovať a nepoužívať na hardvérovom vybavení pridelených prostriedkov IT neautorizovaný (nelegálny) softvér.

- *Identifikácia a autentizácia*

Prevádzkovatelia pre používateľov zaviedli viaceré ochranné opatrenia. **Avšak niektoré pokyny mali len veľmi všeobecný charakter alebo boli používateľom oznamované len ústne** (napr. pri preberaní autentizačného prostriedku,

hesla a pod.). Prevádzkovatelia často nesplnili požiadavky na zložitosť hesla, počet znakov a zaužívaným pravidlom nebola ani povinnosť meniť heslo v pravidelných intervaloch. Oprávnené osoby neboli zaviazané povinnosťou zmeniť si heslo bezodkladne po jeho vyzradení, a tiež nebolo len výnimkou, že im nebolo obmedzené ani používanie funkcionality „zapamätať heslo". Prevádzkovatelia používateľom len výnimočne zakázali posielať autentizačné prostriedky (užívateľský účet, PIN a pod.) elektronickou poštou, faxom alebo SMS správou vo forme voľne čitateľného textu.

- *Práca s mobilnými prostriedkami IT*

Okrem nedostatkov, ktoré boli identifikované pri práci s pracovnou stanicou, **prevádzkovatelia vo väčšine prípadov** od používateľov nevyžadovali ani im nezakazovali ponechávať mobilné prostriedky IT voľne odložené bez dozoru, ani pripájať mobilný prostriedok do nezabezpečených verejných dátových sietí.

- *Práca s prenosnými médiami*

Len zriedkavo kontrolované subjekty uložili používateľom povinnosť pri odovzdaní/pridelení prenosného média inej osobe údaje z prenosného média bezpečne softvérovo skartovať (údaje niekoľkonásobne prepísať s využitím autorizovaného softvéru), ak nemajú byť na médiu zachované. **Častým nedostatkom** bolo, že používatelia neboli upozornení na to, aby neponechávali prenosné médiá vložené do mobilného prostriedku IT (napr. notebooku) alebo PC bez dozoru (voľne prístupné) po ich vypnutí, a tiež aby neumožnili v prostriedkoch IT organizácie použiť neoprávneným osobám ich prenosné médium bez jeho náležitej kontroly a osobnej asistencie. **Skôr pravidlom než výnimkou** bolo zistenie, že subjekty nepoužívali prenosné médiá (USB kľúče) s možnosťou zašifrovania údajov na médiu, a používateľom neukladali povinnosť údaje na prenosných médiách prenášaných mimo organizácie zašifrovať.

- *Internet a elektronická pošta*

Častým nedostatkom bolo, že prevádzkovatelia neuložili používateľom povinnosť:

- ✓ neotvárať súbory alebo makrá pripojené k správe elektronickej pošty od neznámeho odosielateľa, resp. súbory uložené v priečinku *nevyžiadaná pošta* (tzv. spam),
- ✓ bezodkladne mazať reťazové a iné podozrivé e-mailové správy a spamy,
- ✓ nepoužívať oficiálne poštové konto organizácie na súkromné alebo komerčné účely.

Niektoré z vyššie uvedených činnosti prevádzkovatelia (spravidla tí väčší) obmedzili doménovou politikou, na vstupe do prostredia nasadili FortiGate firewall, používateľom zamedzili hrať veľké hry, na vstupe zaviedli kontrolu (blacklist) nevhodných stánok, alebo prílohy kontrolovali politikou Exchange servera, takže napr. súbory s príponou *„exe"* systém blokoval. Aj tu však platilo, že zavedené bezpečnostné mechanizmy nemuseli mať a ani nemali stopercentnú účinnosť.

V rámci kontroly boli zistené aj **prípady, kedy dôvody a spôsob monitorovania zamestnancov** pri odosielaní/prijímaní elektronickej pošty z/do pracovnej elektronickej adresy a pri prezeraní webových stránok nesúvisiacich s výkonom ich činnosti **neboli prerokované so zástupcami zamestnancov v súlade so zákonom** a to napriek tomu, že zamestnanci boli o monitorovaní vopred informovaní.

- *Informačná bezpečnosť zavedená podľa výnosu MF SR*

Z relevantných ustanovení výnosu MF SR sa NKÚ SR pri kontrole zameral najmä na tie *bezpečnostné štandardy* – štandardy pre architektúru riadenia a štandardy minimálneho technického zabezpečenia, ktoré sa týkali aj ochrany osobných údajov.

V oblasti informačnej bezpečnosti organizácie najčastejšie

- ✓ nemali schválenú alebo aktuálnu bezpečnostnú politiku a neustanovili osobu zodpovednú za informačnú bezpečnosť,
- ✓ nedisponovali postupom pre disciplinárne konanie v prípade porušenia bezpečnostnej politiky alebo súvisiacich právnych predpisov o ochrane osobných údajov,
- ✓ nepriradili zodpovednosť za bezpečnosť a obsah každého významného aktíva konkrétnemu vlastníkovi (gestorovi).

Zámerom kontroly bolo komplexne a objektívne zistiť úroveň prijatých bezpečnostných opatrení prevádzkovateľom. Kvalitu prijatých technických a organizačných opatrení, ako aj celkovú úroveň bezpečnosti spracúvaných údajov v IS prevádzkovateľa priamo ovplyvňuje odbornosť dohľadu vykonávaného zodpovednou osobou. Tá musí byť chápaná ako súčasť zavedených bezpečnostných opatrení organizačného charakteru. Zistené výsledky v oblasti bezpečnosti spracúvania údajov a výkonu funkcie zodpovednej osoby bolo preto potrebné vyhodnotiť vo vzájomnej súvislosti.

*Podľa jednotnej metodiky NKÚ SR, úroveň prijatých bezpečnostných opatrení za celú kontrolovanú vzorku dosiahla známku 2,68 a inštitút zodpovednej osoby bol ohodnotený známkou 3,31**. Celková známka charakterizujúca bezpečnosť spracúvania údajov v IS prevádzkovateľov v rámci celej kontrolovanej vzorky je 3,00.***

3.3 ZROZUMITEĽNOSŤ LEGISLATÍVY A METODÍK PRE PREVÁDZKOVATEĽOV

Dôvodom problémov aplikácie Nariadenia (EÚ) v praxi môže byť jeho priama uplatniteľnosť, keďže *„právny jazyk"* nariadenia je značne zložitý a prevádzkovatelia sú povinní ho aplikovať priamo. Vnútroštátnu právnu úpravu, **nový zákon č. 18/2018 Z. z. o ochrane osobných údajov**, už v jeho návrhu v rámci MPK viaceré pripomienkujúce subjekty vyhodnotili ako **nezrozumiteľný a vnútorne rozporný**. Za najzávažnejšie negatívum považovali takmer doslovné prevzatie celého znenia Nariadenia (EÚ) do zákona. Po zverejnení zákona č. 18/2018 Z. z. dotknuté subjekty smerovali na ÚOOÚ SR množstvo otázok týkajúcich sa najmä pôsobnosti zákona a nariadenia. ÚOOÚ SR vypracoval v júni 2018 metodické usmernenie *„Kedy Nariadenie a kedy zákon o ochrane osobných údajov"*, v ktorom musel vysvetľovať, kedy pri spracúvaní osobných údajov treba použiť zákon o ochrane osobných údajov a kedy Nariadenie (EÚ). Podľa usmernenia *nie je chybou, ak sa prevádzkovateľ bude riadiť a postupovať len podľa zákona č. 18/2018 Z. z., aj ak by sa na jeho činnosť malo vzťahovať Nariadenie (EÚ)*.

Názory prevádzkovateľov na úroveň legislatívy, Usmernenia ÚOOÚ SR a metodík vydaných ÚOOÚ SR a zverejnených na jeho webovom sídle reprezentuje tabuľka č. 2.

Tabuľka č. 2: Úroveň zrozumiteľnosti Nariadenia (EÚ), zákona č. 18/2018 Z. z., Usmernenia ÚOOÚ SR a metodík

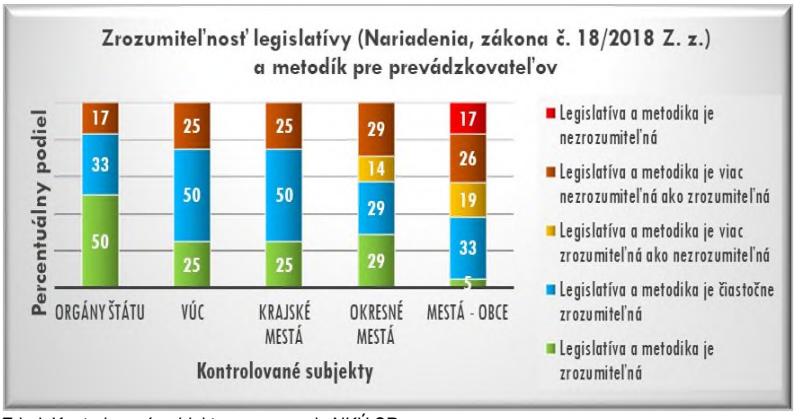
Úroveň zrozumiteľnosti podľa prevádzkovateľov	Orgány štátu / VÚC Krajské mestá / Okresné mestá (20 kontrolovaných subjektov)				Mestá / Obce od 1 – 6000 obyvateľov (42 kontrolovaných subjektov)			
	Nariadenie (EÚ)	Zákon č. 18/2018 Z. z.	Usmernenie ÚOOÚ SR	Metodiky vydané ÚOOÚ SR	Nariadenie (EÚ)	Zákon č. 18/2018 Z. z.	Usmernenie ÚOOÚ SR	Metodiky vydané ÚOOÚ SR
Zrozumiteľné / Čiastočne zrozumiteľné	13	9	5	11	26	24	15	21
Zrozumiteľnosť je obmedzená	6	6	3	8	0	0	4	11
Nejasné / Nezrozumiteľné	1	5	12	1	16	18	23	10

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

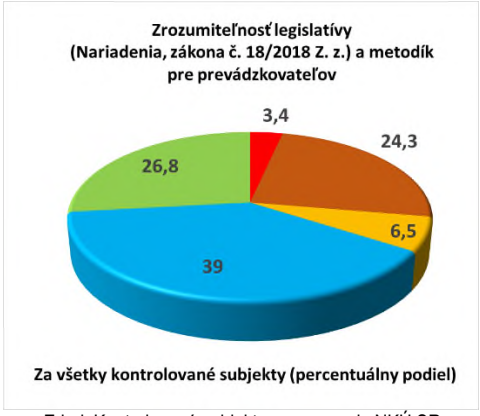
Podľa vyhodnotení **26,8 %** kontrolovaných subjektov prijatú legislatívu a vydané metodiky aplikuje **bez väčších problémov**. Len **45,5 %** subjektov považuje legislatívu **za čiastočne zrozumiteľnú**. Niektorí tiež uviedli, že s aplikáciou legislatívy a metodiky v praxi mávajú problém a bez odbornej pomoci nemajú istotu, že konajú v úplnom súlade so zákonom a nariadením. Nejasnosti by potrebovali konzultovať s ÚOOÚ SR alebo odborníkom na ochranu osobných údajov. **Takmer 28 % kontrolovaných subjektov sa vyjadrilo, že legislatíva v oblasti ochrany osobných údajov je náročná, nezrozumiteľná a ťažko aplikovateľná**.

Graf č. 12: Zrozumiteľnosť legislatívy (Nariadenie, zákon č. 18/2018 Z. z.) a metodík pre prevádzkovateľov podľa charakteru (typu) kontrolovaných subjektov

Graf č. 13: Zrozumiteľnosť legislatívy (Nariadenie, zákon č. 18/2018 Z. z.) a metodík pre prevádzkovateľov komplexne za všetky kontrolované subjekty



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Zo 62 kontrolovaných subjektov 10 z nich uviedlo, že ÚOOÚ SR požiadali o konzultáciu. ÚOOÚ SR zareagoval na žiadosť a konzultáciu poskytol. **Prevádzkovatelia však spravidla zároveň poznamenali, že ÚOOÚ SR v rámci vyjadrenia k riešenému problému nezaujal/nedal jednoznačné stanovisko a súčasne ho označil len za právne nezáväzné a odporúčacie. Nájsť správne riešenie a zodpovednosť za zákonnosť spracúvania tak v plnenej miere aj naďalej zostalo na prevádzkovateľovi. Tri subjekty sa vyjadrili, že doteraz na svoju žiadosť odpoveď ÚOOÚ SR nedostali.**

Štatisticky vyjadrené: 13 % kontrolovaných subjektov (8 zo 62) potvrdilo, že ÚOOÚ SR v minulosti u nich vykonal kontrolu spracúvania osobných údajov.

3.4 FINANČNÉ PROSTRIEDKY A ĽUDSKÉ ZDROJE VYČLENENÉ NA OCHRANU OSOBNÝCH ÚDAJOV

ÚOOÚ SR koncom roka 2016 oslovil ministerstvá a ústredné orgány štátnej správy, aby vyčíslili dosah na svoj rozpočet z dôvodu zavedenia novej legislatívy, Nariadenia (EÚ); napr. na výkon funkcie zodpovednej osoby a na zabezpečenie nových povinností s tým, že následne si orgán verejnej moci tieto prostriedky uplatní v roku 2017 pri príprave rozpočtu na roky 2018, 2019 a 2020. V doložke vplyvov k zákonu č. 18/2018 Z. z. však predkladateľ deklaroval, že plnenie úloh vyplývajúcich z predmetného zákona bude zabezpečené v rámci schválených limitov výdavkov ÚOOÚ SR, bez zvýšených požiadaviek na rozpočet verejnej správy.

MF SR sa vyjadrilo, že ako tvorca ŠR **nedisponuje požadovanými informáciami** ostatných orgánov verejnej správy, a teda **nevie poskytnúť** vierohodný obraz o tom, ktoré subjekty verejnej správy pri príprave rozpočtu na roky 2018, 2019 a 2020 boli schopné vyčísliť vplyv na svoj rozpočet v súvislosti so zavedením nových pravidiel pri ochrane osobných údajov.

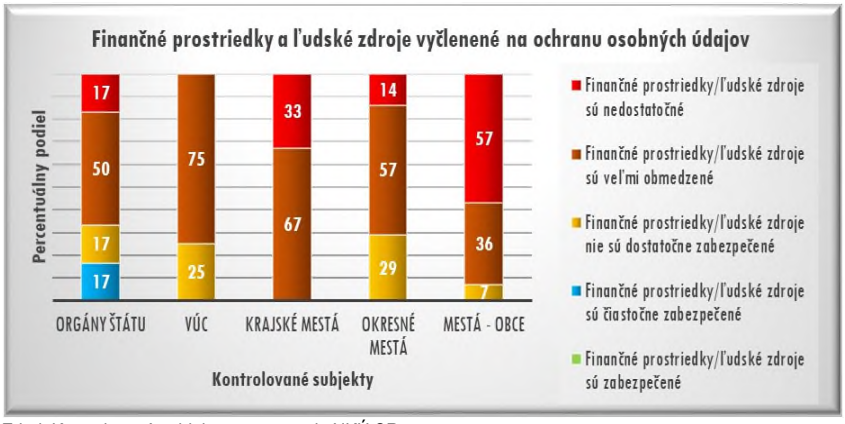
Kontrolované subjekty buď vôbec nevedeli vyčísliť finančné prostriedky, ktoré vynaložili na ochranu osobných údajov, alebo ich vedeli vyčísliť len veľmi nepresne, a to najmä z týchto dôvodov:

1. **v rámci rozpočtov orgánov verejnej správy neexistuje osobitná položka**, ktorá by sa priamo týkala výdavkov na ochranu osobných údajov v IS prevádzkovaných orgánom verejnej správy,
2. **orgány verejnej správy nemajú povinnosť a ani samé nevyčísľujú**, koľko finančných prostriedkov ročne potrebujú na pokrytie nákladov spojených s prevádzkou IS obsahujúcich osobné údaje a nevyčísľujú ani prostriedky potrebné na ľudské zdroje zabezpečujúce plnenie povinností a úloh vyplývajúcich z právnych predpisov týkajúcich sa ochrany osobných údajov.

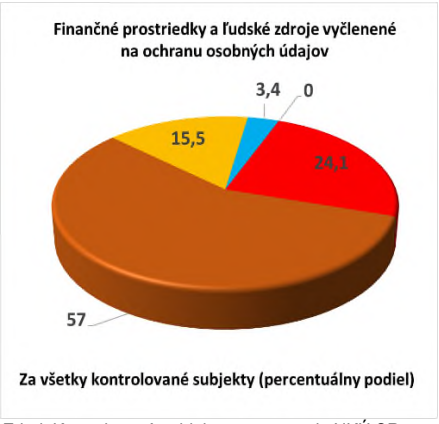
Vyhodnotenie vynakladania finančných prostriedkov na ochranu osobných údajov je spracované v nasledovných grafoch, ktoré zachytávajú dostupnosť a dopad reálne vynaložených finančných prostriedkov u kontrolovaných subjektov.

Graf č. 14: Finančné prostriedky a ľudské zdroje vyčlenené na ochranu osobných údajov podľa charakteru (typu) kontrolovaných subjektov

Graf č. 15: Finančné prostriedky a ľudské zdroje vyčlenené na ochranu osobných údajov komplexne za všetky kontrolované subjekty



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Ako vidieť z grafu, žiadny zo vzorky 62 kontrolovaných subjektov nemá zabezpečené finančné prostriedky na veľmi dobrej úrovni. Naopak, až **81,2 % z kontrolovaných subjektov** pracuje v oblasti ochrany osobných údajov **s veľmi obmedzenými až nedostatočnými finančnými prostriedkami**.

Graf č. 16: Stav finančných prostriedkov a ľudských zdrojov vyčlenených v kontrolovaných súboroch subjektov na plnenie povinností podľa Nariadenia (EÚ) / priemer za všetky kontrolované subjekty

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

*Podľa jednotnej metodiky NKÚ SR dosiahla vzorka kontrolovaných subjektov v priemere známku **4,31***. Najlepšie priemerné hodnotenie dosiahli orgány štátu a, naopak, najhoršie hodnotenie dosiahli mestá a obce s počtom obyvateľov od 1 do 500, čo potvrdzuje pravidlo, že **úroveň kvality zabezpečenia osobných údajov** vo verejnom sektore **klesá s veľkosťou orgánu verejnej správy**, ktorý zodpovedá za bezpečnosť spracúvaných osobných údajov v IS obsahujúcich osobné údaje.

MF SR sa ďalej vyjadrilo, že **nevykonalo žiadne analýzy týkajúce sa stavu ochrany osobných údajov v SR** a považuje spôsob vynakladania finančných prostriedkov na ochranu osobných údajov za plne v kompetencii jednotlivých orgánov verejnej správy. **Uvedený stav predstavuje riziko, že budúce požiadavky zo strany orgánov verejnej správy** o navýšenie rozpočtových prostriedkov na zabezpečenie adekvátnej ochrany osobných údajov **budú zo strany štátu zamietnuté, keďže ich relevantná oprávnenosť nie je podložená analytickými štúdiami, ktoré by to potvrdzovali.**

3.5 CELKOVÉ VYHODNOTENIE DODRŽIAVANIA POVINNOSTÍ USTANOVENÝCH NARIADENÍM (EÚ)

Výsledný stav ochrany osobných údajov v rámci celej kontrolovanej vzorky subjektov podľa jednotnej metodiky NKÚ SR **bol vyhodnotený známkou 2,87**, čo znamená, že **ochrana osobných údajov** podľa Nariadenia (EÚ), zákona č. 18/2018 Z. z. a súvisiacich právnych predpisov platných pre oblasť ochrany osobných údajov, **je orgánmi verejnej správy zabezpečovaná a dodržiavaná s výhradami**.

Tabuľka č. 3: Vyhodnotenie stavu dodržiavania povinností ustanovených Nariadením (EÚ) a zákonom č. 18/2018 Z. z.

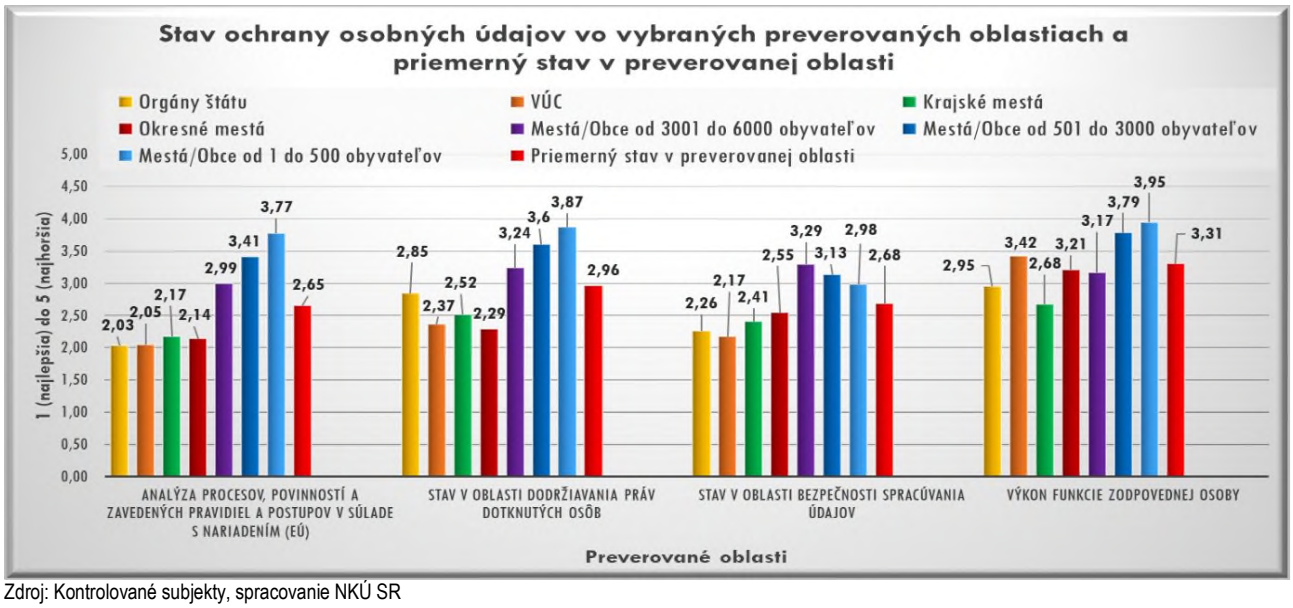
Preverovaná oblasť	Priemerné hodnotenie podľa jednotnej metodiky NKÚ SR
Analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ)	2,65
Dodržiavanie práv dotknutých osôb	2,96
Bezpečnosť spracúvania údajov a výkon funkcie zodpovednej osoby*	3,00
Celkové vyhodnotenie dodržiavania povinností ustanovených Nariadením (EÚ)	2,87

Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

** Celková úroveň bezpečnosti spracúvaných údajov v IS bola vo výsledku vyhodnotená komplexne vo vzájomnej súvislosti s výsledkom charakterizujúcim úroveň výkonu dohľadu zodpovednými osobami.*

***Poznámka:** Celkové vyhodnotenie stavu dodržiavania povinností ustanovených Nariadením (EÚ) a zákonom č. 18/2018 Z. z. nezahŕňa hodnotenie stavu finančných prostriedkov a ľudských zdrojov vyčlenených na ochranu osobných údajov a ani hodnotenie úrovne zrozumiteľnosti legislatívy (nariadenia a zákona) a metodík vydaných ÚOOÚ SR pre prevádzkovateľov. Tieto oblasti kontroly boli v predchádzajúcich kapitolách vyhodnotené samostatne.*

Graf č. 17: Stav ochrany osobných údajov v preverovaných oblastiach / priemer v preverovaných oblastiach

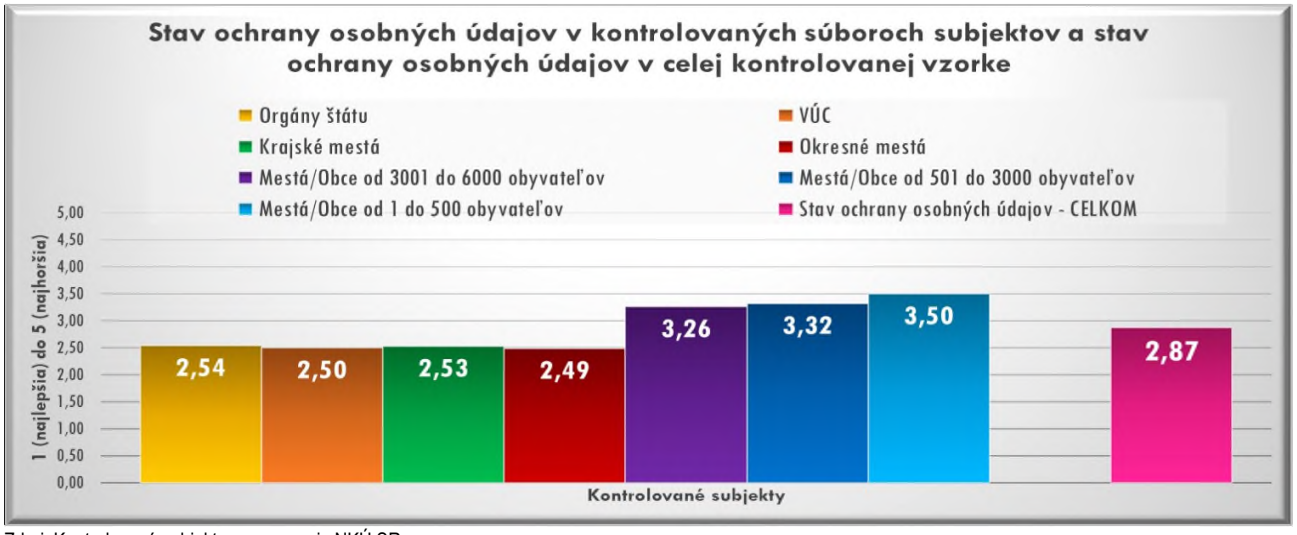


Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

Zhrnutie najvýznamnejších záverov kontroly NKÚ SR:

- **úroveň kvality zabezpečenia osobných údajov vo verejnom sektore** klesá s veľkosťou orgánu verejnej správy a priamo súvisí najmä s nedostatočnými finančnými prostriedkami vyčlenenými na zavedenie technických a organizačných opatrení a na ľudské zdroje v oblasti ochrany osobných údajov,
- Nariadenie (EÚ), a **najmä nižšiu zrozumiteľnosť prijatej legislatívy v oblasti ochrany osobných údajov na národnej úrovni (zákon č. 18/2018 Z. z.)** prevádzkovatelia označili za druhý vážny dôvod (po nedostatočných financiách), prečo nevedeli aplikovať a neaplikovali právnu úpravu v oblasti ochrany osobných údajov správne alebo v plnom rozsahu,
- **ochrana osobných údajov nefunguje dostatočne, nefunguje efektívne**, resp. povinnosti sú prevádzkovateľmi často plnené skôr formálne ako účinne, najmä v oblasti nedostatočnej úrovne zabezpečenia osobných údajov v IS prevádzkovaných orgánmi verejnej správy, a **to aj rok po nadobudnutí účinnosti Nariadenia (EÚ) a zákona č. 18/2018 Z. z.,**
- **MS SR** na základe kompetencie ustanovenej zákonom č. 18/2018 Z. z. od 25. mája 2018 v SR **nezaviedlo účinný kontrolný systém dodržiavania pravidiel** zavedených v Nariadení (EÚ) **pri spracúvaní osobných údajov súdmi v rámci výkonu ich súdnej právomoci**.

Graf č. 18: Stav ochrany osobných údajov v kontrolovaných súboroch subjektov / priemer v celej kontrolovanej vzorke



Zdroj: Kontrolované subjekty, spracovanie NKÚ SR

3.6 ZRIADENIE OSOBITNÉHO ORGÁNU DOZORU V RÁMCI SYSTÉMU SÚDNICTVA

Podľa Nariadenia (EÚ) výkon **dozoru nad spracovateľskými operáciami na súdoch pri výkone ich súdnej právomoci** musí byť od 25. mája 2018 **zverený osobitnému orgánu, zriadenému v rámci systému súdnictva**.

MS SR už v rámci MPK k návrhu nového zákona o ochrane osobných údajov v roku 2017 navrhovalo riešenie – zriadiť osobitný orgán dozoru pri Súdnej rade SR, ktoré sa oveľa viac približovalo k požiadavke plynúcej z primárneho práva EÚ. **Napokon, kompetencia vykonávať dozor v rozsahu kontroly nad spracúvaním osobných údajov na súdoch pri výkone ich súdnej právomoci, bola od 25. mája 2018 zverená zákonom č. 18/2018 Z. z. MS SR**.

NKÚ SR v rámci kontroly zistil, že MS SR na základe kompetencie ustanovenej zákonom č. 18/2018 Z. z. – vykonávať funkciu osobitného orgánu dozoru, **neprijalo opatrenia**, na základe ktorých **by bol v SR od 25. mája 2018 zavedený účinný kontrolný systém** dodržiavania pravidiel ustanovených v Nariadení (EÚ) **pri spracúvaní osobných údajov súdmi pri výkone ich súdnej právomoci**, keďže výkonom týchto povinností v mene MS SR do 21. augusta 2019 oficiálne nepoverilo žiadny útvar MS SR ani osobu/osoby, ba na tento účel nezabezpečilo ani personál s potrebnou kvalifikáciou, skúsenosťami a zručnosťami, a to predovšetkým v oblasti ochrany osobných údajov. **NKÚ SR zároveň zistil, že MS SR v tomto období na súdoch nevykonalo žiadnu kontrolu.**

Ďalej NKÚ SR v rámci kontroly skonštatoval, že ak nastavený model samotného výkonu dozoru na súdoch má fungovať v rámci MS SR, ktoré je orgánom výkonnej moci a ktoré prostredníctvom ministra riadi, koordinuje a kontroluje vláda SR, **potom nemožno hovoriť o nezávislom výkone právomocí členov osobitného orgánu dozoru kontrolovať spracúvanie osobných údajov na nezávislých súdoch pri výkone ich súdnej právomoci, takže MS SR by malo zvážiť jeho zmenu.** Na porovnanie, v Českej republike dozor nad ochranou osobných údajov na súdoch pri výkone ich súdnej právomoci zverili osobitným orgánom, ktoré zriadili priamo na nezávislých súdoch.

3.7 NEZÁVISLOSŤ POSTAVENIA DOZORNÝCH ORGÁNOV NA OCHRANU OSOBNÝCH ÚDAJOV

EK začala v roku 2011 voči SR konanie vo veci EÚ Pilot, prípad č. 2044/11/JUST, ktorý sa týkal vážnych pochybností EK o tom, že postavenie ÚOOÚ SR a výkon jeho právomocí v rozpočtovej a finančnej oblasti nie je úplne nezávislý a vo vnútroštátnom právnom poriadku SR nie je upravený v súlade s právom EÚ. Na tieto skutočnosti SR v rokoch 2003 až 2010 pri rôznych rokovaniach EK viackrát upozornila.

EK v právnom stanovisku misie Sch-Eval, ktoré uviedla vo svojej Hodnotiacej správe 6898/06 (Uznesenie vlády SR č. 558 z 21. júna 2006), žiadala zaručiť úplnú nezávislosť ÚOOÚ SR ako nezávislého orgánu s oporou v ústave a požadovala zabezpečiť aj jeho prevádzkovú a rozpočtovú nezávislosť.

NKÚ SR konštatuje, že nezávislé postavenie nebolo ÚOOÚ SR priznané ani v Ústave SR, ani zákonom č. 428/2002 Z. z., neskôr ani zákonom č. 122/2013 Z. z., a nebolo mu priznané ani zákonom č. 18/2018 Z. z. na základe článku 51 Nariadenia (EÚ), ktorý nezávislosť pre všeobecný dozorný orgán, ktorým je v SR ÚOOÚ SR, požaduje.

Problémom EÚ Pilot bol aj nedostatočný výkon právomocí ÚOOÚ SR v rozpočtovej a finančnej oblasti, pretože úrad nedisponoval samostatnou rozpočtovou kapitolou v rámci ŠR. Článok 52 Nariadenia (EÚ) však už výslovne požaduje, aby členské štáty EÚ prostredníctvom vnútroštátneho práva ustanovili, že všeobecné orgány dozoru budú v rámci ŠR disponovať samostatnou rozpočtovou kapitolou. Avšak SR prostredníctvom zákona č. 18/2018 Z. z. túto požiadavku v zákone neustanovila. Na rozpočtovú politiku ÚOOÚ SR má naďalej priamy vplyv MF SR, keďže od 1. januára 2009 návrh rozpočtu ÚOOÚ SR predkladá ako súčasť kapitoly Všeobecná pokladničná správa, ktorej správcom je MF SR.

Napriek tomu, v decembri 2018 (t. z. už v čase účinnosti zákona č. 18/2018 Z. z.) došlo k uzavretiu prípadu EÚ Pilot na základe iniciatívy ÚOOÚ SR, ktorý EK informoval, že problém s nezávislosťou ÚOOÚ SR a jeho finančným zabezpečením bol odstránený, a preto žiada prípad uzavrieť. **NKÚ SR na základe informácie ÚV SR, ktorý je pre systém EÚ Pilot na území SR kontaktným bodom, zistil, že EK na základe žiadosti ÚOOÚ SR v decembri 2018 prípad uzavrela. EK však zároveň slovenské orgány upozornila, že to nebráni EK jej rozhodnutie o zastavení konania voči SR prehodnotiť, ak sa do jej pozornosti dostane nový vývoj situácie alebo sa vyskytnú nové skutočnosti v predmetnej veci.**

ODPORÚČANIA

ÚOOÚ SR:

- **v spolupráci so zodpovednými inštitúciami –** preskúmať obsah zákona č. 18/2018 Z. z. a prehodnotiť, či požiadavky vyplývajúce z Nariadenia (EÚ), ktoré bolo potrebné implementovať do nášho právneho poriadku, boli prevzaté v požadovanom rozsahu a spôsobom, ktorý je primerane zrozumiteľný pre prevádzkovateľov a dotknuté osoby;
- **v spolupráci so zodpovednými inštitúciami –** preskúmať ustanovenia čl. 51 ods. 1 a čl. 52 ods. 6 Nariadenia (EÚ) a prehodnotiť, či požiadavky týkajúce sa nezávislosti postavenia dozorných orgánov na ochranu osobných údajov boli správne implementované do vnútroštátneho poriadku v súlade s Nariadením (EÚ);
- **v spolupráci s MF SR –** využiť zistenia zo Záverečnej správy ako zdôvodnenie pre vypracovanie analýzy, ktorá by poskytla ucelený obraz o tom, koľko finančných prostriedkov by mal štát reálne vynakladať ročne na ľudské zdroje, technické a organizačné opatrenia pre zabezpečenie ochrany osobných údajov v IS orgánov verejnej správy, a to v súlade s Nariadením (EÚ) a zákonom č. 18/2018 Z. z.

4 REAKCIA KONTROLOVANÉHO SUBJEKTU

Kontrolované subjekty vytvorili primerané podmienky na výkon kontroly. Výstupné materiály z kontrol boli predložené kontrolovaným subjektom na oboznámenie. Možnosť vzniesť námietky využili MPSVaR SR, MS SR a Sociálna poisťovňa. V prípade MPSVaR SR a MS SR nebola u vznesených námietok preukázaná ich opodstatnenosť voči pravdivosti, preukázateľnosti a úplnosti kontrolných zistení. Námietky vznesené Sociálnou poisťovňou boli zo strany NKÚ SR plne akceptované a bol vypracovaný dodatok k protokolu. Zostávajúcich 60 kontrolovaných subjektov námietky nevznieslo. Na základe výsledkov kontroly boli kontrolované subjekty **povinné prijať opatrenia** na odstránenie zistených nedostatkov v **celkovom počte 398**. Najviac boli zastúpené opatrenia týkajúce sa **základných pravidiel a pokynov pre bezpečné spracúvanie osobných údajov oprávnenými osobami (22 %) a informačnej bezpečnosti a bezpečnostných štandardov (19 %)**. Naopak najmenej opatrení na odstránenie zistených nedostatkov mali prijať kontrolované subjekty v oblastiach týkajúcich sa **sprostredkovateľov (7 %), právneho základu spracúvania osobných údajov (5 %) a práv dotknutých osôb (5 %)**. V priebehu roka 2020 musia kontrolované subjekty informovať NKÚ SR o plnení alebo splnení prijatých opatrení **zaslaním správy**.

5 TÍM KONTROLÓROV

Kontroly v rámci kontrolnej akcie vykonalo 8 kontrolórov z ústredia NKÚ SR a 27 kontrolórov z expozitúr NKÚ SR (Trnava, Trenčín, Nitra, Žilina, Banská Bystrica, Prešov a Košice). Kontrolóri majú dlhoročné skúsenosti v oblasti kontrolnej činnosti. S problematikou ochrany osobných údajov boli oboznámení v rámci prípravy kontroly a boli vyškolení v rozsahu potrebnom priamo na výkon kontrol tejto kontrolnej akcie. Odborný dohľad pri kontrole zabezpečoval a koordinoval kontrolór s dlhoročnými skúsenosťami v oblasti ochrany osobných údajov.

ZÁVER

Ochrana a spracúvanie osobných údajov sa týka všetkých občanov SR bez výnimky. **Nedostatočná alebo často len formálne deklarovaná bezpečnosť spracúvaných osobných údajov v IS verejnej správy môže byť v budúcnosti zneužitá v neprospech štátu**, a to vzhľadom na rastúce útoky neetických hackerov na IS verejnej správy, ktoré sú vedené s jediným cieľom – neoprávnene získať spracúvané osobné údaje (osobné údaje sa stali mimoriadne cenným predmetom obchodu). Ukázalo sa, že tento stav v rámci systému ochrany údajov existuje najmä z toho dôvodu, že **na účel zabezpečenia osobných údajov spracúvaných v IS orgánov verejnej správy nie sú vyčlenené a ani systematicky vyčleňované potrebné finančné prostriedky**, a to ani na odborníkov, ktorí by mali ochranu osobných údajov riadiť a správne implementovať potrebné opatrenia.

V prvom rade je preto nevyhnutné **analyzovať stav ochrany osobných údajov vo verejnom sektore z hľadiska finančných nárokov**, ktoré je potrebné „naliať“ do rozpočtov orgánov verejne správy, aby sa čo najskôr v oblasti financovania odstránil takmer havarijný stav.

V druhom kroku je potrebné **zintenzívniť osvetovú činnosť kompetentných orgánov a subjektov, ktoré majú vo svojej náplni dohľad nad ochranou osobných údajov**, či už priamo alebo nepriamo. Rovnako **pomôcť by mohli (rýchle) kontroly spracúvania osobných údajov, ktorých prvoradým cieľom by nebola represia, ale skôr prevencia** a pomoc kontrolovaným subjektom problémy odstrániť a čo najskôr napraviť.

Značná časť prevádzkovateľov sa vyjadrila, že nesprávna aplikácia Nariadenia (EÚ) a zákona č. 18/2018 Z. z. v praxi má pôvod aj v nejasnej alebo nesprávne implementovanej legislatíve.Toto slabé miesto verejnej správy, ktoré sa dá jednoducho odstrániť novelou právneho predpisu, možno zbytočne **ohrozuje bezpečnosť spracúvaných osobných údajov** v rámci celého systému. Preto, v treťom kroku je potrebné zvážiť, či by sa štát nemal začať zaoberať aj zmenami vnútroštátnej legislatívy platnej pre ochranu osobných údajov.

Nedostatočná úroveň nezávislosti ÚOOÚ SR podľa požiadaviek primárneho a sekundárneho práva EÚ v oblasti ochrany osobných údajov môže mať **negatívny vplyv na verejné financie SR,** keďže zo strany EK nemusí byť vylúčené konanie pre priame porušenie povinnosti podľa článku 288 Zmluvy o fungovaní EÚ v spojitosti s článkom 4 ods. 3 Zmluvy o EÚ **s následnou hrozbou uplatňovania si paušálnej pokuty**.

KONTAKT

Najvyšší kontrolný úrad Slovenskej republiky
Priemyselná 2
824 73 Bratislava 26
☎ +421 2 501 14 911
✉ info@nku.gov.sk

PRÍLOHA

Proces kontroly preverovania súladu prijatých opatrení s Nariadením (EÚ) a zákonom 18/2018 Z. z., ktorý bol doplnený o kontrolu bezpečnostných (štandardov) opatrení prijatých podľa výnosu MF SR, bol rozdelený do samostatných ucelených oblastí, ktoré NKÚ SR preveroval komplexne, a to prostredníctvom 300 kontrolných otázok a cca 150 doplňujúcich otázok. 62 prevádzkovateľom boli kladené rovnaké kontrolné otázky (a doplňujúce otázky), ktorým bolo priradené bodové ohodnotenie (váha) od 1 do 5 so slovným hodnotením:

1 – dodržiava, 2 – čiastočne dodržiava, 3 – dodržiava s výhradami, 4 – porušuje, 5 – nedodržiava.

Podľa tejto jednotnej metodiky NKÚ SR boli vyhodnotené oblasti:

- ***analýza procesov, povinností a zavedených pravidiel a postupov v súlade s Nariadením (EÚ)***
- ***práva dotknutej osoby – pravidlá, postupy a oznámenia***
- ***výkon funkcie zodpovednej osoby***
- ***stav ochrany osobných údajov v oblasti bezpečnosti spracúvania údajov***
- ***celkové vyhodnotenie dodržiavania povinností ustanovených Nariadením (EÚ);***

následne boli percentuálne vyhodnotené v skupinách:

- Orgány štátu
- VÚC
- Krajské mestá
- Okresné mestá
- Mestá/obce od 1 do 6 000 obyvateľov (mestá/obce od 1 do 500, mestá/obce od 501 do 3 000, mestá/obce od 3 001 do 6 000).

V rámci oblasti

- ***zrozumiteľnosť legislatívy (nariadenia a zákona č. 18/2018 Z. z.), metodík a usmernení vydaných ÚOOÚ SR pre prevádzkovateľov,***

nebol hodnotený prevádzkovateľ, ale na základe vyjadrení prevádzkovateľa bola hodnotená **úroveň zrozumiteľnosti Nariadenia (EÚ), zákona č. 18/2018 Z. z. a metodík a usmernení vydaných ÚOOÚ SR pre prevádzkovateľa,** a zisteniam bolo priradené bodové ohodnotenie (váha) od 1 do 5 so slovným hodnotením:

1 – legislatíva a metodika je zrozumiteľná
2 – legislatíva a metodika je čiastočne zrozumiteľná
3 – legislatíva a metodika je viac zrozumiteľná ako nezrozumiteľná (zrozumiteľnosť je obmedzená)
4 – legislatíva a metodika je viac nezrozumiteľná ako zrozumiteľná
5 – legislatíva a metodika je nezrozumiteľná.

Oblasť:

- ***finančné prostriedky a ľudské zdroje vyčlenené na ochranu osobných údajov***

podľa jednotnej metodiky NKÚ SR zachytáva dostupnosť a dopad reálne vynaložených finančných prostriedkov u kontrolovaných subjektov na ochranu osobných údajov. Zisteniam bolo priradené bodové ohodnotenie (váha) od 1 do 5 so slovným hodnotením:

1 – finančné prostriedky / ľudské zdroje sú zabezpečené
2 – finančné prostriedky / ľudské zdroje sú čiastočne zabezpečené
3 – finančné prostriedky / ľudské zdroje nie sú dostatočne zabezpečené
4 – finančné prostriedky / ľudské zdroje sú veľmi obmedzené
5 – finančné prostriedky / ľudské zdroje sú nedostatočné.