**MINISTERSTVO ŠKOLSTVA,
VEDY, VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY**
Stromová 1, 813 30 Bratislava 1
manažér informačnej bezpečnosti

**priamo riadené organizácie MŠVVaŠ SR
vysoké školy
školy a školské zariadenia**

| Váš list číslo/zo dňa | Naše číslo | Vybavuje/linka | Bratislava |
|---|---|---|---|
| | 2017-17650:1-66AA | Ing. Juraj Kobela/371 | 15.12.2017 |

**Vec**
**Metodické usmernenie k zabezpečeniu ochrany osobných údajov vo svojich informačných systémoch v zmysle nariadenia EPaR EÚ 2016/679 (GDPR) a nového zákona o ochrane osobných údajov**

Vážení kolegovia,

v nadväznosti na prijatie nariadenia Európskeho parlamentu a Rady EÚ 2016/679 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 - GDPR) a nového zákona o ochrane osobných údajov (ďalej len „ZOOÚ“), ktorý nahrádza pôvodný zákon č. 122/2013 Z. z., stojí pred každou organizáciou úloha zosúladenia súčasného stavu ochrany osobných údajov vo svojich informačných systémoch s požiadavkami, ktoré im v tejto oblasti predpisujú vyššie spomínané záväzné právne normy. Účinnosť oboch týchto právnych noriem nadobúda dňom 25. mája 2018.

**Najdôležitejšie definície**:
„osobné údaje“ sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (dotknutá osoba - ďalej len „DO“); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;
„spracúvanie“ osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami;

„informačný systém“ (ďalej len „IS“) akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe;
„prevádzkovateľom“ každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných;
„šifrovaním“ transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra ako je kľúč alebo heslo;
„pseudonymizáciou“ spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej alebo identifikovateľnej fyzickej osobe;

Pre zabezpečenie spomínaných úloh Ministerstvo školstva, vedy, výskumu a športu slovenskej republiky (ďalej len „MŠVVaŠ SR“) odporúča vykonať minimálne tieto kroky:

1. vo všetký IS zmapovať spracúvanie osobných údajov s priradením atribútu, či sa daný osobný údaj spracúva na základe osobitného zákona, alebo na základe súhlasu DO; ak je spracúvanie osobných údajov založené na súhlase DO, prevádzkovateľ je povinný kedykoľvek vedieť preukázať, že DO poskytla súhlas so spracúvaním svojich osobných údajov; súhlas so spracúvaním osobných údajov udelený podľa doterajšieho zákona, ktorý je v súlade s GDPR sa považuje za súhlas so spracúvaním osobných údajov podľa predpisov účinných od 25. mája 2018;
2. v rámci organizácie ustanoviť zodpovednú osobu – Data Protection Officer (ďalej len „DPO“); DPO by mala byť zriadená na každej vysokej škole a na každej priamo riadenej organizácii MŠVVaŠ SR; v rámci regionálneho školstva odporúča zriaďovateľom škôl a školských zariadení (ďalej len ŠaŠZ“) zriadiť jednu DPO pre všetky ŠaŠZ vo svojej zriaďovateľskej pôsobnosti; organizácia je povinná zverejniť (napr. na ich webovom sídle) údaje o ustanovení DPO v rozsahu, kontaktné údaje zodpovednej osoby, ak je určená a oznámiť ich Úradu na ochranu osobných údajov (ďalej len „ÚOOÚ“); zodpovedná osoba poverená podľa doterajšieho zákona, ktorá spĺňa podmienky podľa GDPR sa považuje za zodpovednú osobu podľa predpisov účinných od 25. mája 2018;
3. pri spracúvaní osobných údajov treba mať na zreteli najmä tieto zásady: zásada zákonnosti, zásada obmedzenia účelu, zásada minimalizácie osobných údajov, zásada správnosti, zásada minimalizácie uchovávania, zásada integrity a dôvernosti, zásada zodpovednosti;
4. zosúladiť vnútorné akty riadenia týkajúce sa ochrany osobných údajov s novými legislatívnymi normami (GDPR, ZOOÚ);

5. zaviesť vedenie záznamov o spracovateľských činnostiach; ako podklad môžu slúžiť súčasne vedené Evidenčné listy IS;
6. prijať primerané technické a organizačné opatrenia na zaistenie požadovanej úrovne bezpečnosti spracúvaných osobných údajov, najmä ich šifrovaním a pseudonymizáciou, zabezpečením trvalej dôvernosti, integrity, dostupnosti a odolnosti systémov; tu je možnosť, aby združenie zastupujúce kategóriu prevádzkovateľov alebo sprostredkovateľov prijalo kódex správania na preukázanie súladu prijatých opatrení s požiadavkami uvedenými v GDPR a ZOOÚ (§ 85 ZOOÚ);
7. pre IS, v ktorých sa spracúvajú osobné údaje vykonať posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov; ako podklad môže slúžiť bezpečnostný projekt IS;
8. zabezpečiť implementáciu detekovania bezpečnostných rizík;
9. schopnosť plniť požiadavku na oznamovanie porušenia ochrany osobných údajov úradu; v prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín oznámi porušenie ochrany osobných údajov ÚOOÚ;

**Ďalšie upozornenia:**

1. pri spracúvaní osobných údajov detí mladších ako 16 rokov na základe súhlasu DO je potrebné mať na zreteli, že takéto spracúvanie osobných údajov je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas poskytol alebo schválil zákonný zástupca dieťaťa;
2. pri spracúvaní osobných údajov na základe súhlasu si je treba uvedomiť značné rozšírenie práv priznaných DO vo vzťahu k ich spracúvaným osobným údajom v IS, najmä právo na opravu osobných údajov, právo na výmaz osobných údajov, právo na obmedzenie spracúvania osobných údajov, právo na prenosnosť osobných údajov, právo namietať spracúvanie osobných údajov, automatizované individuálne rozhodovanie vrátane profilovania; ak organizácia zbiera od DO osobné údaje na základe súhlasu, musí zabezpečiť, aby ich IS bol schopný pri využití svojich práv DO takéto úkony zabezpečiť;

S pozdravom

Ing. Juraj Kobela
manažér informačnej bezpečnosti
MŠVVaŠ SR