

Vyjádření k problematice osobních údajů žáků v rámci přípravy výběrového zjišťování 2018

Ve středu 7. 11. 2018 v ranních hodinách obdržela Česká školní inspekce e-mailovou a telefonickou informaci o chybě administrační části testovací aplikace systému InspIS SET. V této souvislosti Česká školní inspekce upřesňuje, že identifikovaný problém se netýká inspekčního systému elektronického testování InspIS SET jako takového, ale týká se pouze jeho dílčí samostatné aplikace umístěné mimo prostředí vlastního systému InspIS SET.

Chyba se týkala možnosti neautorizovaného stažení testové dávky do této aplikace a následné přístupnosti vybraných osobních údajů v této aplikaci, popř. v souboru testové dávky.

Ihned po obdržení těchto oznámení zajistila Česká školní inspekce okamžité odstavení dotčené části systému (která testovacím aplikacím poskytuje testové dávky) a ve spolupráci s dodavatelem systému byly neprodleně zahájeny práce na analýze problému a jeho řešení. Během velmi krátké doby bylo potvrzeno, že vybrané osobní údaje se po stažení dávky v aplikaci skutečně mohou za určitých okolností zobrazit i osobám, kterým se zobrazit nemají.

Identifikovaná chyba byla následně ještě ten den odstraněna a dotčená dílčí část systému byla téhož dne v 17:49 hod. znovu uvedena do provozu.

Chyba, která se vyskytla a která byla velmi krátce po upozornění odstraněna, souvisela s masivnějšími úpravami, které byly v celém systému InspIS SET (a zejména v modulu tzv. certifikovaného testování, kde je realizováno výběrové zjišťování výsledků žáků) provedeny v uplynulém období, a které byly motivovány výrazným zjednodušením jeho obsluhy na straně škol. Jednalo se zejména o úpravy spojené se zavedením nového průvodce přípravy (registrace žáků apod.) a realizace testování, díky kterému je možné na straně školy administrovat celý proces testování a jeho přípravy zcela bez znalosti uživatelských příruček. Část těchto úprav se soustředila také na dotčenou samostatnou aplikaci, která je určena pro instalaci na školní počítače s operačními systémy Windows.

Zde došlo k odstranění zjednodušeného procesu autentifikace školy (nejednalo se však o jediný mechanismus zabezpečení, jak bude uvedeno dále a jak se zcela nesprávně objevuje v různých mediálních výstupech), který byl doprovázen změnou struktury testové dávky, jež nově neměla obsahovat osobní údaje, které dříve byly v aplikaci určeny k tomu, aby osoba ve škole odpovědná za přípravu testování mohla ověřit, že testová dávka obsahuje testy pro všechny registrované žáky. S ohledem na to se z testové dávky stal pouze zašifrovaný soubor (bez jakýchkoli osobních údajů), k jehož získání není třeba žádné autentifikace. K tomuto rozhodnutí Českou školní inspekci vedly dlouholeté zkušenosti s provozováním celého systému a četné podněty škol zahrnující a popisující situace, kdy osoba, která ve škole tuto část přípravy vykonává (často externí administrátor), nedisponuje uživatelským účtem v systému InspIS SET a často ani základními informacemi, které pro přípravu testování obdržel ředitel školy.

A právě náležitost odstranění osobních údajů z testových dávek v tomto případě selhala. Po zjištění problému a následném odstavení systému byly z testových dávek všechny osobní údaje automaticky odstraněny a byla učiněna adekvátní opatření pro to, aby k obdobným situacím již nemohlo dojít.

Administrační část testové aplikace tak nyní, v souladu s původním záměrem úprav, nadále nevyžaduje autentifikaci, avšak v tabulce detailů o stažené dávce již neobsahuje osobní údaje jednotlivých žáků,

ale pouze bezvýznamové identifikátory jejich testů. Osobní údaje žáků se zde naplní až ve chvíli, kdy některý z žáků (vybavený přístupovými kódy, které mu předá pracovník školy po stažení z plně autentifikované části systému) na daném počítači vyplní test.

Osobní údaje, které díky výše popsané chybě mohly být zobrazeny i nepovolanou osobou, obsahovaly jméno a příjmení žáka, třídu a název testu, ke kterému je žák zaregistrován. V některých případech byla u názvu testu uvedena i poznámka „SVP“. Ta znamená, že daný žák bude mít dle rozhodnutí ředitele školy nějakým způsobem test upraven (např. delší čas na jeho realizaci apod.). Tato informace neumožňuje určit konkrétní důvody, proč tomu tak je, a už vůbec neposkytuje informaci o nějakém konkrétním postižení nebo znevýhodnění u daného žáka. Není tedy pravda, že se nepovolané osoby mohly dostat k informacím o konkrétním typu speciálních vzdělávacích potřeb, jak se objevovalo v některých médiích. Taková podrobnější data ke speciálním vzdělávacím potřebám sice mohou být v systému evidována (tohoto zjišťování výsledků se to však netýká a žádné podrobnosti k typu speciálních vzdělávacích potřeb nebylo v rámci přípravy na podzimní testování vůbec možné zadat, natož jakkoli zobrazit), nikdy však nebyla obsahem testových dávek ani uživatelského rozhraní testovací aplikace a s popsaným incidentem nijak nesouvisí!

Dalším údajem, který Česká školní inspekce jednoznačně vyvrací, je informace, že se mohlo jednat o únik osobních údajů až 140 tisíc žáků. Skutečnost je taková, že distribuované testové dávky, kterých se popisovaný problém týkal, obsahovaly informace pouze o aktuálně připravovaném testování, pro které je registrováno 49.606 žáků, přičemž problém se mohl týkat max. 31.361 z nich. Jednalo se však téměř bezvýhradně o dávky stažené přímo ve školách.

Hypotetická možnost rozsáhlejšího úniku vybraných osobních údajů (o max. 31.361 žácích) se nepotvrdila, což prokazují interní záznamy kontrolních a bezpečnostních prvků systému a celé hostující infrastruktury, jejichž analýzu dodavatel systému právě dokončil.

Tyto mechanismy, které bezpečnostně doplňují veškeré uživatelské přístupy včetně těch neautentifikovaných, neidentifikovaly žádné nestandardní situace, které by jinak nutně musely být spojeny se záměrem masivnějšího neoprávněného přístupu ke zmíněným datům (stahování dávek více škol z jednoho místa, popř. v uceleném časovém období nebo vyšší frekvenci, pokusy o stažení dávky pomocí nevalidních údajů apod.). V takovém případě by již dávno implementované mechanismy zajistily nemožnost provedení takových úkonů.

Nelze však vyloučit to, že v některých jednotlivých případech skutečně mohlo dojít ke stažení testové dávky a přístupu k výše uvedeným vybraným osobním informacím žáků (jméno, příjmení, třída a název testu). I proto v souladu s ustanovením článku 33 Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), připravuje Česká školní inspekce oznámení Úřadu pro ochranu osobních údajů.

Česká školní inspekce samozřejmě velmi lituje této situace a přijala veškerá možná opatření, aby k něčemu takovému v budoucnu již nemohlo dojít. Zároveň Česká školní inspekce konstatuje, že systém InspIS SET a všechny jeho komponenty jsou v tuto chvíli plně připraveny na maximální zajištění ochrany veškerých osobních údajů, a tím i plně připraveny k realizaci výběrového zjišťování výsledků žáků.

V Praze dne 8. 11. 2018