

ukládá podle zákona účinného v době, kdy byl čin spáchán, a pozdějšího zákona se použije, jestliže je to pro pachatele příznivější. S ohledem na dobu spáchání protiprávního jednání specifikovaného ve výroku tohoto příkazu, jakož i s ohledem na změny právních předpisů, ke kterým došlo v období mezi spácháním skutku a rozhodováním o něm, posoudil správní orgán obsah relevantních právních předpisů účinných v době spáchání činu a obsah později účinných právních norem a dospěl k závěru, že pozdější právní úprava obsažená v zákoně č. 110/2019 Sb. je pro pachatele příznivější, neboť na rozdíl od předchozí právní úpravy obsažené zejména v zákoně č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů, ukládá Úřadu, aby upustil od uložení správního trestu v případě, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení (EU) 2016/679.

Ze shromážděného spisového materiálu vyplývá, že dne 9. listopadu 2018 Úřad obdržel od ústředního školního inspektora oznámení o narušení bezpečnosti osobních údajů, ve kterém mimo jiné uvedl, že došlo k porušení zabezpečení osobních údajů žáků základních škol v inspekčním systému elektronického testování [REDAKCE], o němž se dozvěděl dne 7. listopadu 2018. K tomu uvedl, že incident se týká informačního systému [REDAKCE] který obviněná v souladu se svým zákonným zmocněním podle § 174 odst. 2 písm. a) a b) zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), využívá pro zjišťování výsledků žáků v rámci počátečního vzdělávání. Toto zjišťování probíhá každý školní rok vždy v odlišném vybraném vzorku škol a tříd, přičemž jsou elektronickou formou vždy testováni žáci vybraných tříd v rámci vybrané tematiky (předmětů a oblastí, která se rovněž v jednotlivých letech mění). K tomu uvedl, že příprava a realizace tohoto testování probíhá v modulu tzv. Certifikovaného testování systému [REDAKCE]. Příprava spočívá mimo jiné v tom, že ředitel školy nebo jím prověřená osoba disponující přístupovými údaji k webové části systému, popř. ředitelem školy přiřazeným oprávněním činit v systému příslušné kroky pro danou školu, kterými jsou uživatelské jméno a heslo, zaregistruje žáky tříd, jímž je testování určeno. [REDAKCE]

Porušení, které obviněná identifikovala dne 7. listopadu 2018 v ranních hodinách na základě oznámení od dvou osob, spočívalo v tom, že by osobní údaje zaregistrovaných žáků ze

systému mohla získat neoprávněná osoba. K tomu, aby k údajům měla přístup, by musela učinit tyto kroky:

1. [REDACTED]

[REDACTED]

Zástupce obviněné dále uvedl, že u případného úniku by se jednalo výhradně o kombinaci dat jméno a příjmení žáka, třída, škola a název testu, ke kterému je žák zaregistrován. Příkladem názvu testu je „[REDACTED]“. V případě, že ředitel školy rozhodne, že konkrétní žák bude absolvovat test s úlevou, může také rozhodnout, že žák se testování vůbec nezúčastní, je zobrazován tento název testu „[REDACTED]“. Tato poznámka ovšem neznamená, že daný žák má diagnostikované speciální vzdělávací potřeby, pouze ředitel školy rozhodl o úlevách. K tomu dodal, že v mediálních výstupech se k této věci objevily různé nepravdivé informace včetně obrázku ze systému [REDACTED] ze kterého vyplývá možnost kategorizace konkrétního hendikepu žáka. Tato možnost v systému

skutečně existuje, jedná se však o jeho webovou část chráněnou přístupem s uživatelským jménem a heslem, a nikoliv testovací aplikaci, přičemž tato funkčnost byla používána v některých historických zjišťováních. Pro toto aktuální testování nejenže ze strany škol nebylo nutné tyto detailní údaje zadávat, ale nebylo to ani možné.

Zástupce obviněné dále uvedl, že ihned po oznámení a rychlé analýze problému obviněná vydala telefonicky dne 7. listopadu 2018 v 8:51 hod. pokyn externímu provozovateli systému, společnosti [REDAKCE], k zastavení provozu systému v jeho dotčené části, která slouží k distribuci testových dávek pro jednotlivé školy. Následně tento dodavatel upravil všechny dávky tak, že z nich odebral údaj o jménu a příjmení žáka. Zároveň upravil testovací aplikaci tak, aby její další spuštění provedlo stejný úkon na počítačích, na které byla dávka stažena již dříve (před přijetím popsaných opatření). Implementace této změny aplikace je možná díky zabudované funkci automatického update; pokud se při spuštění aplikace zjistí existence novější verze, nejprve dojde k přeinstalaci aplikace a až následně je jí možné dále využívat.

Na závěr zástupce obviněné uvedl, že po implementaci těchto opatření byl kompletní provoz systému ve všech jeho částech obnoven dne 7. listopadu 2018 v 17:49 hod. Zároveň byly podle čl. 34 odst. 3 písm. c) nařízení (EU) 2016/679 informovány dotčené subjekty osobních údajů, a to prostřednictvím informace na webových stránkách obviněné publikované dne 8. listopadu 2018 a e-mailovou zprávou odeslanou téhož dne ředitelům všech škol, které se účastní příslušného zjišťování. K tomu dodal, že tento způsob byl zvolen s ohledem na to, že obviněná nedisponuje kontaktními údaji žáků ani jejich zákonných zástupců. Tato informace byla poskytnuta, i přestože obviněná má za to, že nedošlo k naplnění podmínek uvedených pro takový krok v čl. 34 odst. 1 nařízení (EU) 2016/679, tedy k situaci, která bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Pokud by však situace takto klasifikována byla, byla dle obviněné naplněna podmínka uvedená v čl. 34 odst. 3 písm. b) nařízení (EU) 2016/679. Skutečnost, že tato informace byla skutečně zveřejněna, je doložena ve spisovém materiálu.

Ze spisového materiálu dále vyplývá, že Úřad obdržel od obviněné dne 5. prosince 2018 vnitřní předpis nazvaný Nařízení ústředního školního inspektora, kterým se upravuje systém zpracování a ochrany osobních údajů v České školní inspekci (9/2018) ze dne 24. května 2018, které mimo jiné obecně formuluje základní cíle a zásady zpracování osobních údajů obviněnou, dále upravuje technická a organizační opatření k zajištění zpracování a ochrany osobních údajů. Součástí dokumentu jsou přílohy, a to záznam o činnosti zpracování a dále souhlas se zpracováním osobních údajů, včetně poučení o právech subjektu údajů. Další přílohou je záznamový list k žádosti subjektu údajů podle čl. 15 až 22 nařízení (EU) 2016/679.

Z úředního záznamu ze dne 19. prosince 2018 vyplývá, že dne 8. listopadu 2018 byl prověřen program obviněné [REDAKCE] v testovací verzi, která byla stažena z webových stránek obviněné, a to z internetové adresy [REDAKCE]

[REDAKCE]
[REDAKCE]
[REDAKCE]
[REDAKCE] Z úředního záznamu vyplývá, že program se choval tak, jak bylo deklarováno obviněnou.

K předmětu řízení lze konstatovat, že dle čl. 4 bodu 1 nařízení (EU) 2016/679 se osobním údajem rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Obviněná nepochybně za účelem testování v informačním systému ██████████ zpracovává osobní údaje v rozsahu jméno a příjmení žáka, třída a název testu, ke kterému je žák zaregistrován, a v některých případech informace, že daný žák bude mít dle rozhodnutí ředitele školy nějakým způsobem test upraven, neboť tyto informace je možné zcela zjevně vztáhnout ke konkrétnímu subjektu údajů.

Dle čl. 4 bodu 2 nařízení (EU) 2016/679 se zpracováním rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Obviněná ve svém informačním systému InspIS SET nakládala s osobními údaji testovaných žáků a nepochybně je tak zpracovávala, neboť je shromažďovala a používala za účelem jejich testování.

Dále je nezbytné uvést, že obviněná je správcem osobních údajů žáků škol ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť určila účel (provádění inspekční činnosti, evidence, evidence úrazů dětí, žáků a studentů, komunikace se školami a školskými zařízeními, zajištění interních procesů) a prostředky (informační systém ██████████) zpracování osobních údajů.

Obviněná je proto povinna dodržet veškeré relevantní povinnosti stanovené nařízením (EU) 2016/679 správcům osobních údajů. Jedna z těchto povinností je vyjádřena v zásadě integrity a důvěrnosti stanovené v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, podle které musí být osobní údaje zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Na tuto zásadu pak navazuje čl. 32 odst. 1 nařízení (EU) 2016/679, dle kterého s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) tohoto článku.

Správní orgán konstatuje, že v daném případě zcela zjevně nebyly osobní údaje žáků obviněnou zpracovávány způsobem, který by zajistil jejich náležité zabezpečení před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Jak vyplývá ze shromážděné spisové dokumentace, obviněná dostatečně nezabezpečila v době specifikované ve výroku tohoto příkazu osobní údaje žáků v informačním systému ██████████ a tím umožnila jejich zpřístupnění neoprávněným osobám.

Podle § 5 zákona č. 250/2016 Sb. je přestupkem škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.

Z čl. 83 odst. 7 nařízení (EU) 2016/679 vyplývá, že aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2 tohoto nařízení, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě. Podle § 62 odst. 5 zákona č. 110/2019 Sb. Úřad upustí od uložení správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení (EU) 2016/679. S ohledem na skutečnost, že obviněná je orgán veřejné moci, tedy správce uvedený v čl. 83 odst. 7 nařízení (EU) 2016/679, upustil správní orgán od uložení správního trestu.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že obviněná spáchala svým jednáním přestupek podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., a proto rozhodl podle § 150 odst. 1 správního řádu ve spojení s § 90 odst. 1 zákona č. 250/2016 Sb. ve věci příkazem.

Poučení: V souladu s § 150 odst. 3 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto příkazu podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen dnem převzetí stejnopisu, nejpozději ale desátým dnem od jeho uložení na poště. V případě doručování do datové schránky je dnem doručení okamžik přihlášení oprávněné osoby do datové schránky, nejpozději ale desátý den ode dne dodání příkazu do datové schránky.

Praha 11. června 2019

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru kontrolního