ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Č.j. UOOU-02491/20-8
Praha 30. září 2020

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „Úřad“). Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Kontrolující:

MVDr. František Bartoš – inspektor Úřadu**,** číslo průkazu inspektora XXXX.
JUDr. Roman Recman – pověřený zaměstnanec Úřadu, číslo služebního průkazu XXXX.
JUDr. Michal Jelínek – pověřený zaměstnanec Úřadu, číslo služebního průkazu XXXX.

Kontrolovaná osoba:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXXXXXXXXXXX.
(dále jen „kontrolovaná osoba“)

Předmět kontroly:

Předmětem kontroly je dodržování nařízení Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016 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) v systému BAKALÁŘI, se zaměřením na zásady zpracování osobních údajů podle čl. 5, zákonnost zpracování osobních údajů podle čl. 6, podmínky vyjádření souhlasu podle čl. 7, zákonnost zpracování zvláštních kategorií osobních údajů podle čl. 9, informační povinnost správce podle čl. 12 a 13, dodržování práv subjektů údajů podle čl. 15 – 23, zabezpečení osobních údajů podle čl. 32, včetně povinností dodavatelů systému BAKALÁŘI a jednotlivých aplikací. V průběhu kontroly může být předmět kontroly rozšířen.

První kontrolní úkon:

Kontrola byla zahájena Oznámením o zahájení kontroly č.j. UOOU-02491/20-2, ze dne 17. června 2020, které bylo kontrolované osobě doručeno přihlášením oprávněné osoby do datové schránky dne 18. června 2020.

Poslední kontrolní úkon:

Posledním úkonem předcházejícím vyhotovení protokolu je odpověď kontrolované osoby k žádosti o součinnost č.j. UOOU-02491/20-7, ze dne 23. září 2020.

I. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1) Pověření ke kontrole, ze dne 10. června 2020, č.j. UOOU-02491/20-1.
2) Oznámení o zahájení kontroly, ze dne 17. června 2020, č.j. UOOU-02491/20-2.
3) Zaslání požadovaných dokumentů a informací kontrolovanou osobou, ze dne 1. července 2020, č.j. UOOU-02491/20-3.
   Přílohy:
   - Kontrola zpracování údajů v systému Bakalář.
   - Směrnice – „XXXXXXXXXXXXXXXXXXXXXXXXX (pokud je zavedena ve škole počítačová síť“.
   - Licenční smlouva uzavřená mezi kontrolovanou osobou a společností XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.
4) Dopis Úřadu s požadavkem na doplnění kontrolních zjištění, ze dne 12. srpna 2020, č.j. UOOU-02491/20-4.
5) Odpověď kontrolované osoby, kterou Úřad obdržel dne 20. srpna 2020, čj. UOOU-02491/20-5.
6) Žádost o součinnost č.j. UOOU-02491/20-6, ze dne 16. srpna 2020.
7) Odpověď kontrolované osoby č.j. UOOU-02491/20-7, ze dne 23. září 2020.

V rámci kontroly bylo posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly, ledaže je níže uvedeno jinak a v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod kontroly:

Kontrola je provedena na základě kontrolního plánu Úřadu pro rok 2020. Kontrola je zaměřena na dodržování nařízení Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016 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), se zřetelem na zpracování osobních údajů dle základních zásad, zákonnost zpracování, informační povinnost, práva subjektů údajů podle nařízení (EU) 2016/679 a ochranu osobních údajů.

Oznámení o zahájení kontroly ze dne 17. června 2020, č.j. UOOU-02491/20-2, bylo kontrolované osobě doručeno přihlášením oprávněné osoby do datové schránky dne 18. června 2020. V oznámení o zahájení kontroly byla kontrolovaná osoba požádána o zaslání následujících informací a dokumentů:

1) Sdělte, jaké osobní údaje a v jakém rozsahu osobní údaje v systému BAKALÁŘI zpracováváte.
2) Sdělte, zda v systému BAKALÁŘI zpracováváte zvláštní kategorie osobních údajů podle čl. 9 nařízení (EU) 2016/679), v jakém rozsahu a za jakým účelem.
3) Sdělte jednotlivé účely zpracování osobních údajů v systému BAKALÁŘI a jeho aplikacích, včetně jejich odůvodnění (čl. 5 odst. 1 písm. b) nařízení (EU) 2016/679).
4) Sdělte dobu, po kterou jsou osobní údaje v systému uchovávány, za jakým účelem a způsob jejich likvidace (čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679).
5) Sdělte, právní titul pro zpracování osobních údajů v systému a počet přihlášených žáků (čl. 6 Nařízení (EU) 2016/679).
6) V případě, že zákonní zástupci vyslovili souhlas se zpracováním osobních údajů v systému BAKALÁŘ, zašlete jako příklad 5 kopií takto vyjádřených souhlasů. V případě, že osobní údaje zpracováváte z jiného právního titulu, sdělte jeho odůvodnění (čl. 6 nařízení (EU) 2016/679). Také uveďte, jak plníte podmínky vyjádření souhlasu a jeho odvolání (čl. 7 nařízení (EU) 2016/679).
7) Sdělte informace o dodavateli systému a zašlete kopie smluv, které máte s tímto dodavatelem uzavřené a sdělte informaci, zda dodavatel vykonává také servis systému a jeho aplikací. Pokud se na provozu systému BAKALÁŘI podílí také další subjekty, sdělte jejich název a zašlete kopie smluv, které máte s těmito subjekty uzavřeny.
8) Sdělte, jak jsou osobní údaje v systému BAKALÁŘI zabezpečeny proti neoprávněným přístupům, kdo osobní údaje do systému zadává, kdo má k uloženým údajům přístup, jak probíhá kontrola jednotlivých přístupů a jak často (logování přístupů).
9) Zašlete kopii interního předpisu, který upravuje technická a organizační opatření při zpracování a zabezpečení osobních údajů v systému BAKALÁŘI (čl. 32 nařízení (EU) 2016/679).
10) Zašlete seznam rizik, která jsou možná při zpracování osobních údajů v systému Zejména se jedná určeni míry pravděpodobnosti náhodného zničení uložených, resp. archivovaných osobních údajů, jejich ztrátě, neoprávněnému přístupu, jejich pozměňování (čl. 32 nařízení (EU) 2016/679). (Seznam rizik je zpracován správcem systému, zpravidla za pomocí dodavatele softwarového programu).

III. Kontrolní zjištění:

Kontrolní zjištění č. 1:

A. Ve svém vyjádření k oznámení o zahájení kontroly, kontrolovaná osoba uvedla, že osobní údaje v systému BAKALÁŘI zpracovává v níže uvedeném rozsahu:

- vedení docházky v rozsahu: – jméno a příjmení, docházka,
- vedení školní matriky v rozsahu: – jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, státní příslušnost, telefonní číslo, e-mailová adresa, zdravotní pojišťovna, údaje o zdravotním stavu, škola, kterou žák navštěvoval,

doporučení školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění, jméno a příjmení zákonného zástupce, jeho telefonní číslo, e-mail a adresa bydliště. Údaje o posouzení zdravotního stavu a zdravotní způsobilosti žáka ke vzdělání jsou zvláštní kategorií osobních údajů podle čl. 9 nařízení (EU) 2016/679),

- vedení žákovské knížky zpracovává škola osobní údaje žáka v rozsahu – jméno a příjmení, studijní výsledky.

B. Kontrolou bylo zjištěno, že kontrolovaná vede v systému BAKALÁŘI (matrika) osobní údaje za těmito účely:

- evidence žáků a splnění povinností podle zákona č. 651/2004 Sb., o předškolním, základním, vyšším odborném a jiném vzdělávání (školský zákon), - osobní údaje v rozsahu jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, státní příslušnost,
- evidence žáků a splnění povinností podle školského zákona – telefonní číslo a e-mail,
- za účelem potřeby komunikace s pojišťovnou v souvislosti s BOZP (např. úrazy), se souhlasem zákonných zástupců.
- evidence žáků a splnění povinností podle zákona č. 561/2004 Sb., školský zákon – posouzení zdravotního stavu a zdravotní způsobilosti žáka ke vzdělání,
- evidence žáků a splnění povinností podle školského zákona – název školy, kterou žák navštěvoval, doporučení školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění žáka,
- evidence žáků a splnění povinností podle školského zákona – jméno a příjmení zákonného zástupce žáka,
- evidence žáků a splnění povinností podle školského zákona – telefonní číslo, e-mail a bydliště zákonného zástupce, za účelem jeho kontaktování,
- za účelem informovat rodiče o prospěchu žáka záznamy v žákovské knížce – jméno a příjmení žáka.

C. Kontrolovaná osoba uchovává osobní údaje v systému BAKALÁŘI (matrika) podle zákona o archivnictví č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů a prováděcích předpisů po následující doby:

- jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, telefonní číslo, e-mail, údaje o zdravotním stavu, doporučení školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění, škola, kterou žák navštěvoval, a to po dobu 45 let,
- státní příslušnost a údaje týkající se zdravotní pojišťovny po dobu trvání docházky,
- údaje zákonného zástupce v rozsahu jméno a příjmení, telefonní číslo, e-mail a adresa bydliště, a to dobu 45 let.

D. Právním titulem pro zpracování osobních údajů v systému BAKALÁŘI je zejména:

- plnění právní povinnosti správce osobních údajů podle školského zákona. Tento zákon určuje povinnost zpracovávat údaje v elektronicky vedené matrice v rozsahu: jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, státní příslušnost, údaje o zdravotním stavu, škola, kterou žák navštěvoval, doporučení

školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění, jméno a příjmení zákonného zástupce a adresa jeho bydliště,

- oprávněný zájem správce, na základě, kterého vede osobní údaje v rozsahu: telefonní číslo a e-mail žáka a jeho zákonného zástupce,
- souhlas zákonného zástupce ke zpracování osobních údajů v souvislosti se zdravotním pojištěním.

E. Informace o zpracování osobních údajů pro zákonné zástupce jsou kontrolovanou osobou zpracovány na webových stránkách kontrolované osoby, v systému BAKALÁŘI. Pro přihlášení do systému je zapotřebí zadat přihlašovací jméno, včetně přístupového hesla, které obdrží od kontrolované osoby.

F. Kontrolou bylo zjištěno, že k osobním údajům v sytému BAKALÁŘI mají přístup tyto osoby:

a) Ředitel kontrolované osoby jako správce systému (administrátor) má přístup k celé databázi, může číst i editovat všechny položky systému BAKALAŘI, přiděluje práva a hesla dalším uživatelům (vedení školy, třídní učitelé atd.), může tisknout vysvědčení, generovat sestavy pro kontrolní orgány atd.

b) Zástupce ředitele má právo zadávání údajů o nově přijatých žácích, může tisknout a odesílat údaje do škol, kam žáci přestoupili.

c) Hospodářka školy, administrativní pracovník má právo zadávat nově přijaté žáky, tisknout a scanovat údaje z matriky a odesílat je na instituce dle pokynu ředitele kontrolované osoby.

d) Výchovný poradce má právo zadávat údaje žáků o integraci, měnit, tisknout a doplňovat je, generovat výkaz s údaji o integrovaných žácích, zodpovídá za správnost zadaných údajů.

e) Třídní učitel má právo zadávat údaje o žácích a zákonných zástupcích, měnit a doplňovat je, tisknout, zodpovídá za správnost a aktuálnost údajů o žácích jemu přidělené třídy.

f) Učitel má právo číst a editovat údaje žáků a zákonných zástupců.

Povinnosti uživatelů systému BAKALÁŘI jsou určeny následovně:

- ředitel zavádí do databáze údaje žáků nastupujících do budoucí první třídy ihned po nabytí právní moci správního rozhodnutí o přijetí žáka a přiděluje třídy třídním učitelům na základě rozhodnutí vedení kontrolované osoby,
- správce, ředitel kontrolované osoby a zástupce ředitele využívají databáze k tvorbě sestav pro kontrolní orgány (UIV, zřizovatel), provádí tisk vysvědčení atd.,
- třídní učitelé jsou garanty přesnosti a aktuálnost údajů. Každý třídní učitel má povinnost na začátku školního roku zkontrolovat aktuálnost údajů o žácích a jejich zákonných zástupcích (např. změna bydliště během prázdnin, telefonního spojení apod.). Aktualizace údajů o žácích a jejich zákonných zástupcích je povinen provádět při každé změně i v průběhu školního roku.

Systém BAKALÁŘI je nainstalován na všech PC (ve sborovně, ředitelně, kancelářích a kabinetech), a je přístupný až po přihlášení uživatele ke školní počítačové síti. Pro spuštění programu je nezbytné přihlášení uživatele. Všichni uživatelé systému BAKALÁŘI jsou povinni dodržovat mlčenlivost o skutečnostech obsažených ve školní matrice i o přístupových heslech do školní počítačové sítě a systému BAKALÁŘI.

Kontrolovaná osoba předává osobní údaje z matriky vedené v BAKALÁŘI třetím subjektům podle vyhlášky č. 364/2005 Sb., o dokumentaci škol a školských zařízení (individuální údaje, agregované údaje, údaje týkajících se podpůrných opatření druhého až pátého stupně). Dále

jsou osobní údaje z matriky předávány podle § 28 odst. 4 školského zákona, a to soudům, Policii České republiky a dalším orgánům činným v trestním řízení, České školní inspekci, dalším kontrolním orgánům, zdravotním pojišťovnám apod., v rámci jejich zákonem vymezené působnosti. O předávání těchto údajů rozhoduje ředitel kontrolované osoby.
Přístup k osobním údajům zpracovávaným v matrice má v rámci servisní smlouvy (viz kontrolní zjištění č. 2) dodavatel a správce IT systému BAKALÁŘI.

Kontrolní zjištění č. 2:
Kontrolovaná osoba (uživatel) má se společností XXXXXXXXXXXXXXXXXXXX (poskytovatel) uzavřenou Licenční smlouvu ze dne 1. listopadu 2019 (dále jen „smlouva"), jejímž předmětem je dodávka a servis systému BAKALÁŘI. V úvodu smlouvy strany shodně prohlašují, že poskytovatel nemá na základě této smlouvy bez předchozího svolení samostatný přístup k osobním údajům, jejichž je uživatel správcem. Smluvní strany shodně prohlašují, že uživatel může v ojedinělých případech poskytovateli umožňovat přístup do systému BAKALÁŘI prostřednictvím aplikace XXXXXXXXXXXX, za účelem servisu software. Podobně může uživatel ojediněle zasílat poskytovateli data k reklamaci systému.
Obsahem smlouvy jsou licenční ujednání, záruka a odstranění vad v systému BAKALÁŘI, sankční ustanovení, doba trvání smlouvy a ochrana osobních údajů, včetně závěrečných ustanovení.
V části „další ujednání smluvních stran" jsou uvedeny povinnosti uživatele v souvislosti s provozem systému BAKALÁŘI. Uživatel se ve smlouvě zavazuje:

- dodržovat veškeré pokyny k užívání software uvedené v přiložené dokumentaci;
- instalovat software pouze na koncová zařízení s takovým hardwarovým a softwarovým vybavením, které je plně kompatibilní se software, a udržovat koncová zařízení v kompatibilním stavu;
- udržovat koncová zařízení v řádném stavu, který umožňuje bezproblémové a řádné fungování software, zejména se zavazuje provádět nezbytné aktualizace softwarového vybavení koncových zařízení a odstraňovat nežádoucí software (jakékoliv viry či jiné škodlivé programy);
- pravidelně zálohovat a archivovat či jinak řádně uchovávat data;
- bez předchozího výslovného souhlasu poskytovatele sám nebo prostřednictvím třetích osob nebude zasahovat, upravovat nebo měnit software, a to ani v souvislosti s funkčním propojením software s jinými softwarovými aplikacemi smluvní strany.
- bez předchozího výslovného souhlasu poskytovatele neměnit data nebo jejich části, nezasahovat do dat jinak než prostřednictvím funkcí software způsobem popsaným v dokumentaci;
- chránit přístupové kódy (hesla), sdělit přístupové kódy pouze koncovým uživatelům v rozsahu, který je nutný pro využití software pro plnění pracovních povinností takových uživatelů;

Ochrana osobních údajů je upravena v části 10. smlouvy. V této části smlouvy kontrolovaná osoba a společnost XXXXXXXXXXXXXXXX konstatují, že data ve smyslu smlouvy obsahují osobní údaje o koncových uživatelích, jakož i o žácích studentech uživatele či jiných osobách v obdobném postavení, a to veškerá data, se kterými školy a školská zařízení přichází do styku v průběhu poskytování vzdělávání. Uživatel prohlašuje, že data mohou obsahovat i citlivé osobní údaje. Uživatel je správcem osobních údajů ve smyslu čl. 4., odst. 7 nařízení (EU) 2016/679) a poskytovatel je zpracovatelem osobních údajů ve smyslu 4., odst. 8. nařízení (EU) 2016/679). Smlouva je také smlouvou o zpracování osobních údajů ve smyslu čl. 28., odst. 3 nařízení (EU) 2016/679).

V části 10. smlouvy se také poskytovatel systému zavazuje, že v případech, kdy uživatel umožní poskytovateli přístup k osobním údajům, bude:
a) zpracovávat osobní údaje výlučně za účelem řádného provozu a užívání systému ze strany uživatele;
b) zpracovávat osobní údaje pouze na základě této smlouvy a doložených pokynů uživatele,
c) zabezpečit po technické a organizační stránce údaje tak, že bude minimalizována možnost přístupu neoprávněných osob k osobním údajům obsaženým v systému, jakož i možnost jejich ztráty, změny či poškození;
d) přistupovat k údajům pouze se souhlasem uživatele, přičemž zaměstnanci poskytovatele jsou pro takový případ vázáni poskytovatelem k povinnosti mlčenlivosti; případné užití osobních údajů ze strany poskytovatele je možné jen pro nezbytný servisní úkon a přístup je možný jen v nezbytně nutném rozsahu;
e) poskytnout uživateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v čl. 28 nařízení (EU) 2016/679), a dále umožní uživateli audity, včetně inspekcí prováděné uživatelem nebo jiným auditorem ve smyslu ustanovení čl. 28., odst. 3. nařízení (EU) 2016/679), a k těmto auditům přispěje;
f) vrátit po ukončení servisních služeb veškerá data uživateli;
g) poskytnout uživateli veškerou potřebnou součinnost pro případ výkonu jiných povinností správce podle nařízení (EU) 2016/679). např. realizace práv subjektů údajů na přístup k osobním údajům či povinnosti ohlašovat porušení zabezpečení osobních údajů.

Kontrolní zjištění č. 3:
Kontrolovaná osoba má zpracovanou směrnici „XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX“ (dále jen „směrnice“). Cílem směrnice je stanovit základní bezpečnostní pravidla, která zajistí přístup k datům poskytovaných dílčími informačními systémy správce, a zároveň zajistí patřičnou ochranu poskytovaných a uchovávaných údajů s ohledem na zachování jejich důvěryhodnosti.
Podle směrnice mají všichni uživatele počítačového systému povinnost v případě zjištění nebo podezření na výskyt bezpečnostního incidentu, tuto skutečnost ohlásit. Oznámení výskytu bezpečnostního IT incidentu se provádí vyplněním formuláře „Evidence GDPR“ v elektronické podobě na společném úložišti. Veškeré bezpečnostní incidenty jsou evidovány a kontrolovány. V případě vyhodnoceného vysokého rizika průběžně informuje správce o stavu řešení příp. požádá o spolupráci.
Hlavním cílem směrnice je stanovit základní bezpečnostní pravidla, která zajistí přístup k údajům poskytovaných dílčími informačními systémy kontrolované osoby, a zároveň zajistí patřičnou ochranu poskytovaných a uchovávaných dat s ohledem na zachování jejich důvěryhodnosti.

Směrnice upravuje jednotlivé postupy při ochraně nosičů informací, archivačních médií, zabezpečení přenosných zařízení. Dále směrnice upravuje postupy při využívání počítačového systému kontrolované osoba v souvislosti se vznikem pracovního poměru a jeho ukončení. Směrnice také upravuje tvorbu přístupového účtu, který je tvořen XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX. Zaměstnanec, který má přístup do systému BAKALÁŘI, nebo zpracovává osobní údaje je povinen o těchto zachovávat mlčenlivost. Povinnost mlčenlivosti trvá i po skončení pracovního poměru nebo příslušných prací. Podle směrnice musí být systém BAKALÁŘI nastaven tak, aby v systémových událostech byly dostupné minimálně informace o přihlášení a odhlášení uživatele a informace o neúspěšných pokusech přístupu k informačnímu systému. Záznamy musí být pravidelně kontrolovány. Přístupová

práva veškerých uživatelů musí být pravidelně revidována. Revize bude zaměřena na neplatné přístupové účty, nesprávně nastavená oprávnění a na změny vlastností informačního systému. Jako základní ochranná opatření před zavedením škodlivého programového kódu jsou XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Ve směrnici je dále uvedeno, že v případě že se jsou v rámci informačního a počítačového systému, případně mimo tento informační systém šířeny osobní údaje nebo chráněné informace, musí být na jejich ochranu použita přídavná ochranná opatření. V případě zasílání dat prostřednictvím elektronické pošty může být jako vhodné ochranné opatření použito XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

Kontrolou bylo zjištěno, že směrnice obsahuje také tabulku s riziky při zpracování osobních údajů, která se mohou v informačním systému kontrolované osoby vyskytnout. U každé hrozby je uveden možný způsob výskytu hrozby.

- Úmyslná — hrozba, která může nastat úmyslným jednáním za účelem poškodit IS
- Náhodná — hrozba, která může nastat náhodným jednáním lidské aktivity, a která může způsobit náhodné poškození IS
- Přírodní— hrozba, které nemá souvislost s lidským jednáním a je způsobena vlivy přírody nebo okolního prostředí

Tabulka obsahuje 40 rizik, která mohou při zpracování osobních údajů prostřednictvím informačního systému nastat. Směrnice je v závěru podepsána 7 zaměstnanci kontrolované osoby, včetně ředitele.

Kontrolovaná osoba má také samostatně zpracovaný seznam rizik, která mohou vzniknout při zpracování jednotlivých osobních údajů vedených v matrice. V tabulce jsou uvedena rizika, pravděpodobnost jejich výskytu a způsoby jejich omezení (prevence). Ve všech případech kontrolovaná osoba uvedla, že pravděpodobnost výskytu rizik je výjimečná a jejich výskyt je zabezpečen ochranou informačního systému.

Kontrolní zjištění č. 4:
V dopise ze dne 12. srpna 2020 byla kontrolovaná osoba vyzvána k doplnění kontrolních zjištění o následující informace:

- sdělte přesný odkaz na webové stránky, kde se informace dle čl. 12 nařízení (EU) 2016/679 nacházejí. Zašlete Úřadu písemnou verzi těchto informací;

- sdělte, jak škola postupuje v případě přihlášení nových žáků a jejich zákonných zástupců do systému BAKALÁŘI;

- sdělte, jak škola postupuje v případech, kdy se žáci nebo jejich zákonní zástupci do systému BAKALÁŘI přihlásili a později systém nevyužili;

- sdělte, jak nakládáte s osobními údaji žáků a jejich zákonných zástupců zpracovávaných v systému BAKALÁŘ v případě ukončení školní docházky a po jaké době jsou jim přístupy zrušeny.

K výše uvedeným dotazům Úřadu kontrolovaná osoba v dopise ze dne 20. srpna 2020 sdělila, že se informace pro zákonné zástupce žáků nacházejí na webových stránkách kontrolované osoby XXXXXXXXXXXX v dokumentu „XXXXXXXXXXXXXXXXXXXXXXXXXXX“ Na uvedených webových stránkách jsou tyto informace:

1) Kontaktní údaje o správci osobních údajů, statutárním zástupci a pověřenci pro ochranu osobních údajů.
2) Účely, v rámci, kterých budou osobní údaje správcem zpracovávány.
3) Právní tituly pro zákonnost zpracování osobních údajů, kterými jsou:
    a) zákon č. 561/2004 Sb., školský zákon,
    b) zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních,
    c) zákon č. 563/1991 Sb., O účetnictví,
    d) zákon č. 262/2006 Sb., Zákoník práce,
    e) souhlas zákonného zástupce.
4) Zpracovatelé, kterými jsou: poskytovatel software – XXXXXXXXXXXXXXXXX, správce IT (XXXXXXXXXXXX), XXXXXXXXXXXXXXXXXXX, případně další poskytovatelé software a služeb, kteří by v budoucnu nahradili poskytovatele pod písm. a) až c).
5) Doba uložení osobních údajů s odkazem na Spisový a skartační řád.
6) Dále jsou v dokumentu uvedená práva subjektů údajů při zpracování osobních údajů. Jedená se o právo požadovat přístup k osobním údajům týkajících se subjektu údajů, právo na jejich opravu, právo na omezení zpracování, právo vznést námitku proti zpracování, podat stížnost u Úřadu a právo na výmaz osobních údajů, u kterého je poznámka s textem *„Toto Vaše právo je omezeno některými platnými zákony ČR (viz bod „Právní základ pro zpracování Vašich osobních údajů“ v kapitole 2.). Vaše osobní údaje proto nemusí být vymazány, popř. mohou být vymazány jen částečně, přestože právo na jejich výmaz uplatníte“*
7) Dokument obsahuje také postup při uplatnění výše uvedených práv.

Kontrolní zjištění č. 5:

K dotazu kontrolujících, jakým způsobem postupuje škola v případě přihlášení nových žáků a jejich zákonných zástupců do systému BAKALÁŘI, kontrolovaná osoba ve svém sdělení ze dne 20. srpna 2020 uvedla, že na základě písemné přihlášky, která vytváří vstup do systému BAKALÁŘI je pověřenými zaměstnanci v systému BAKALÁŘI vytvořena karta žáka a automaticky je vytvořen i přístup do systému pro žáka a zákonného zástupce. Prvotní přihlašovací údaje jsou zaslány na email žáka a zákonného zástupce. Tyto údaje jsou následně uživatelem změněny na vlastní přihlašovací údaje. K dotazu, jak škola postupuje v případech, kdy se žáci nebo jejich zákonní zástupci do systému BAKALÁŘI přihlásili a později systém nevyužili, kontrolovaná osoba uvedla, že po vytvoření karty a automatickém zaslání údajů na e-mail žáka a zákonného zástupce škola dále nemanipuluje s přihlašovacími údaji. Tyto jsou automaticky obnovovány na konci školního roku. K otázce jak kontrolovaná osoba nakládá s osobními údaji žáků a jejich zákonných zástupců zpracovávaných v systému BAKALÁŘI v případě ukončení školní docházky, a po jaké době jsou jim přístupy zrušeny kontrolovaná osoba uvedla, že se osobní údaje archivují i po ukončení školní docházky v modulu XXXXXXXXX podle § 3 odst. 1 písm. j) zákona č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů a záznamů o činnostech uvedených na webových stránkách Ministerstva školství mládeže a tělovýchovy https://www.msmt.cz/dokumenty-3/strucny-navod-na-zabezpeceni-procesu-souvisejicich-s-gdpr. Přístupy do systému BAKALÁŘI jsou žákům a zákonným zástupcům zrušeny s ukončením školní docházky.

Kontrolní zjištění č. 6:
V žádosti o součinnost, ze dne 16. září 2020, byla kontrolovaná osoba požádána o sdělení, zda obdržela v posledních dvou letech žádost dle čl. 15 nařízení (EU) 2016/679 (právo subjektu údajů na přístup k osobním údajům), čl. 16 (právo na opravu), čl. 17 (právo na výmaz) a čl. 18 (právo na omezení zpracování), týkající se systému BAKALÁŘI. Pokud ano, měla sdělit bližší informace a zaslat kopii alespoň jedné podané žádosti a její vyřízení u každého z uvedených práv. Dále měla sdělit, zda v posledních dvou letech obdržela žádost dle čl. 21 nařízení (EU) 2016/679 (právo vznést námitku), týkající se systému BAKALÁŘI. V případě, uplatnění práva vznést námitku, měla sdělit k této skutečnosti bližší informace a zaslat kopii alespoň jedné podané námitky, včetně jejího vyřízení.

Dne 23. září 2020, zaslala kontrolovaná osoba datovou zprávou odpověď k žádosti o součinnost, ve které uvedla, že v posledních dvou létech neobdržela žádnou žádost ve věci ochrany osobních údajů, týkající se systému BAKALÁŘI.

Kontrolní zjištění č. 7:
Podle čl. 4 odst. 1) nařízení (EU) 2016/679 se pro účely tohoto nařízení osobními údaji 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“.*

Kontrolovaná osoba vede v systému BAKALÁŘI osobní údaje v rozsahu: jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, státní příslušnost, telefonní číslo, e-mailová adresa, zdravotní pojišťovna, údaje o zdravotním stavu, škola, kterou žák navštěvoval, doporučení školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění, jméno a příjmení zákonného zástupce, jeho telefonní číslo, e-mail a adresa bydliště.
Podle výše uvedených údajů se dá konkrétní fyzická osoba přímo nebo nepřímo identifikovat, jedná se tedy o osobní údaje ve smyslu čl. 4 odst. 1) nařízení (EU) 2016/679.

Kontrolovaná osoba dále vede údaje o posouzení zdravotního stavu a zdravotní způsobilosti žáka ke vzdělání**.** Uvedené údaje jsou vedeny dle školského zákona a jsou zvláštní kategorií osobních údajů ve smyslu čl. 9 nařízení (EU) 2016/679.

Kontrolní zjištění č. 8:
Podle čl. 4. odst. 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“*
Kontrolovaná osoba shromažďuje, zaznamenává a ukládá osobní údaje systematicky pomocí automatizovaných postupů a manuálně. Jedná se tedy o zpracování osobních údajů ve smyslu čl. 4. odst. 2 nařízení (EU) 2016/679.

Kontrolní zjištění č. 9:

Podle čl. 4 odst. 7) nařízení (EU) 2016/679 se správcem rozumí **„***fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho jmenování".*

Kontrolovaná osoba zpracovává osobní údaje v elektronické verzi matriky (systém BAKALÁŘI) za účelem vedení evidence žáků a další dokumentace za účelem právní povinnosti dle § 28 školského zákona.

Kontrolovaná osoba má určeny účely zpracování osobních údajů, je tedy správcem osobních údajů ve smyslu čl. 4 odst. 7) nařízení (EU) 2016/679.

Kontrolní zjištění č. 10:

Podle čl. 5 písm. e) nařízení (EU) 2016/679. musí být osobní údaje „*uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů".*

Kontrolovaná osoba uchovává osobní údaje v systému BAKALÁŘI (matrika) podle zákona o archivnictví č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů a prováděcích předpisů po následující doby:

1) jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, telefonní číslo, e-mail, údaje o zdravotním stavu, doporučení školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění, škola, kterou žák navštěvoval, a to po dobu 45 let,
2) státní příslušnost a údaje týkající se zdravotní pojišťovny po dobu trvání docházky,
3) údaje zákonného zástupce v rozsahu jméno a příjmení, telefonní číslo, e-mail a adresa bydliště, a to dobu 45 let.

Kontrolní zjištění č. 11:

Podle čl. 6 odst. 1 nařízení (EU) 2016/679, je zpracování zákonné, „*pokud je splněna nejméně jedna z níže uvedených podmínek a pouze v odpovídajícím rozsahu"*

a) *Subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;*
b) *Zpracování je nezbytné pro splnění smlouvy, jejíž stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;*
c) Zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
d) *Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;*
e) *Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;*
f) *Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě*."

Za účelem plnění právní povinnosti vede kontrolovaná osoba osobní údaje žáků podle § 28 školského zákona. Tento zákon určuje povinnost zpracovávat údaje vedené matrice v rozsahu: jméno a příjmení, datum narození, třída, rodné číslo, místo narození, adresa bydliště, státní příslušnost, údaje o zdravotním stavu, škola, kterou žák navštěvoval, doporučení školského poradenského zařízení, specifické potřeby jako zdravotní nebo sociální znevýhodnění, jméno a příjmení zákonného zástupce a adresa jeho bydliště,
Na základě oprávněného zájmu, vede kontrolovaná osoba telefonní číslo a e-mail žáka a jeho zákonného zástupce.
Se souhlasem zákonného zástupce vede osobní údaje v souvislosti se zdravotní pojišťovnou.
Údaje o posouzení zdravotního stavu a zdravotní způsobilosti žáka ke vzdělání jsou vedeny dle školského zákona a jsou zvláštní kategorií osobních údajů ve smyslu čl. 9 nařízení (EU) 2016/679.

Kontrolní zjištění č. 12:
Podle čl. 12 nařízení (EU) 2016/679), přijme správce *„vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby“.*
Kontrolovaná osoba informuje zákonné zástupce žáků o zpracování osobních údajů ve smyslu čl. 12 nařízení (EU) 2016/679) na webových stránkách kontrolované osoby XXXXXXXXXXXXXXXXXXXXXXXXXX, v dokumentu „XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.“
V dokumentu jsou uvedeny kontaktní údaje správce osobních údajů, statutárního zástupce a pověřence pro ochranu osobních údajů, účely zpracovávání, právní tituly pro zákonnost zpracování osobních údajů, zpracovatelé, doba uchovávání osobních údajů. V dokumentu jsou také podrobněji uvedena jednotlivá práva subjektů údajů při zpracování osobních údajů (právo přístupu, opravu, omezení zpracování, právo vznést námitku, podat stížnost u Úřadu, včetně práva na výmaz osobních údajů, ke kterému kontrolovaná osoba uvedla, že toto právo je omezeno některými platnými zákony České republiky, proto osobní údaje oprávněných žadatelů nemusí být vymazány, popř. mohou být vymazány jen částečně, a to přesto, že je toto uplatněno. Kontrolovaná osoba neobdržela v posledních 2 létech žádnou žádost tykající se práv subjektů údajů při zpracování osobních údajů v systému BAKALÁŘI.

Kontrolní zjištění č. 13:
Čl. 32 odst. 1 nařízení (EU) 2016/679 – *„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.“*
Čl. 32 odst. 2 nařízení (EU) 2016/679 – *„Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.“*

Technicko-organizační opatření kontrolované osoby, jsou ve vztahu k ochraně osobních údajů zpracována ve směrnici „XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX“

(viz. kontrolní zjištění č. 3). Směrnice obsahuje také tabulku s riziky při zpracování osobních údajů, která se mohou v informačním systému kontrolované osoby vyskytnout. U každé hrozby je uveden také možný způsob výskytu hrozby. Tabulka obsahuje 40 rizik, která mohou při zpracování osobních údajů prostřednictvím informačního systému nastat.
Kontrolovaná osoba má také samostatně zpracovaný seznam rizik, která mohou vzniknout při zpracování jednotlivých osobních údajů vedených v matrice. V tabulce jsou uvedena rizika, pravděpodobnost jejich výskytu a způsoby jejich omezení (prevence). Ve všech případech kontrolovaná osoba uvedla, že pravděpodobnost výskytu rizik je výjimečná a jejich výskyt je zabezpečen informačním systémem, který chrání osobní údaje vedené v systému BAKALÁŘI.

Kontrolou, provedenou na XXXXXXXXXXXXXXXX, nebylo zjištěno porušení kontrolovaných ustanovení nařízení (EU) 2016/679.

Poučení o opravném prostředku:
Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.
Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Podpisová doložka:

Otisk
úředního
razítka

MVDr. František Bartoš		(podepsáno elektronicky)
Titul, jméno a příjmení	Inspektor Úřadu	……..
		podpis
JUDr. Roman Recman		(podepsáno elektronicky)
Titul, jméno a příjmení	pověřený zaměstnanec Úřadu	……
		podpis
JUDr. Michal Jelínek		(podepsáno elektronicky)
Titul, jméno a příjmení	pověřený zaměstnanec Úřadu	……
		podpis