Holubová advokáti s.r.o.

Za Poříčskou bránou 21/365
CZ-186 00 Praha 8 (Florenc)
tel./fax: +420 224 914 050
e-mail: info@holubova.cz
http://www.holubova.cz/
ID datové schránky: eaqq73c

Základní umělecká škola Karla Malicha
Holubova 1234,
534 01 Holice

Vaše značka	Naše značka	Praha
-----	GDPR/2018/017	15. 6. 2018

ANALÝZA SOULADU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZÁKLADNÍ UMĚLECKÉ ŠKOLY KARLA MALICHA S POŽADAVKY TZV. GDPR

I. Účel analýzy

V souvislosti s přípravou na nařízení Evropského parlamentu a Rady (EU) č. 679/2016 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 (dále jen „GDPR“) zadalo město Holice advokátní kanceláři Holubová advokáti s.r.o. (dále jen „AK“) vypracování GAP analýzy neboli analýzy souladu stavu zpracování osobních údajů s požadavky GDPR pro ZUŠ Karla Malicha (dále jen „Klient“). Účelem této analýzy je tedy zjistit současný stav zpracování osobních údajů u Klienta a navrhnout změny k dosažení souladu zpracování osobních údajů s požadavky GDPR.

Tato zpráva vychází z právního stavu ke dni vyhotovení této GAP analýzy.

II. Úvod

GDPR je dosud nejvíce uceleným souborem pravidel na ochranu osobních údajů na světě. Jedná se o předpis schválený na půdě EU, který je závazný pro všechny státy EU a je bezprostředně použitelný. Má přednost před českými zákony. V České republice nahrazuje právní úpravu ochrany osobních údajů v podobě zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZOOÚ“). Práva a povinnosti v současném ZOOÚ jsou nahrazena právy a povinnostmi vyplývajícími z GDPR. ZOOÚ bude zcela zrušen a nahrazen novým zákonem, který bude již upravovat jen některé aspekty týkající se Úřadu pro ochranu osobních údajů (dále jen „úřad“) (např. jeho ustavení, organizaci) a některé dílčí záležitosti nutné k dotvoření celého rámce ochrany osobních údajů, které nejsou nařízením GDPR upraveny nebo které GDPR umožňuje upravit na vnitrostátní úrovni.

Nová právní úprava neznamená zásadní předěl v přístupu k ochraně osobních údajů, pouze nad rámec dosavadní praxe stanoví několik nových povinností pro správce a zpracovatele, dále GDPR aktualizuje některá práva subjektů, jejichž osobní údaje se zpracovávají. Základní principy spojené s nakládáním s osobními údaji, kterými je nutno se řídit v současné době,

např. zásada přiměřenosti a zásada transparentnosti, se nemění. Proto pokud byly osobní údaje zpracovávány v souladu s dosud platným zákonem o ochraně osobních údajů, pak nebude nutné příliš do zavedených postupů zasahovat.

Příslušným orgánem pro provádění kontrol a ukládání pokut bude stejně jako doposud Úřad pro ochranu osobních údajů. Přibudou mu ale pravomoci odrážející závažnost celé reformy a zároveň bude částečně podřízen Evropskému sboru pro ochranu osobních údajů. Evropský sbor pro ochranu osobních údajů bude plnit především koordinační funkci a dohlížet na to, aby GDPR bylo uplatňováno v celé EU stejným způsobem.

III. Metoda práce

Cílem této analýzy a implementace v oblasti ochrany osobních údajů je provést komplexní mapování zpracování osobních údajů, zejména popsat jednotlivé procesy ve fungování, při kterých dochází ke zpracování osobních údajů, odhalit nedostatky nastavení těchto procesů pohledem nároků obecného nařízení a představit seznam povinností, které pro správce osobních údajů toto nařízení přináší.

AK tímto prohlašuje, že při doporučování změn dokumentů upravovala Klientem dodané dokumenty pouze v rozsahu jejich souladu s GDPR. AK tak v žádném případě neodpovídá za jejich formální či věcnou správnost ve smyslu ostatních právních oblastí ani za jejich soulad s dalšími právními předpisy. AK dále upozorňuje, že při zpracování analýzy vycházela z výkladové praxe relevantních ustanovení GDPR a ZOOÚ ke dni zpracování této analýzy. AK upozorňuje, že tato výkladová praxe se může postupem času měnit.

Příprava této analýzy byla následující. Vycházeli jsme primárně z dokumentů, které nám dodal Klient, tzn. v rozsahu interních předpisů (zejm. směrnice), vlastních dokumentů a formulářů a dodavatelských smluv.

Dále jsme při přípravě této analýzy vycházeli z dotazníků, které vyplnil Klient, které se týkaly (i) procesů zpracování osobních údajů, (ii) informačních systémů používaných Klientem, (iii) úložišť používaných Klientem a (iv) zabezpečením používaným Klientem. Dalšími zdroji pro přípravu této analýzy bylo místní šetření, které proběhlo u Klienta v květnu 2018.

V této analýze se nejprve zabýváme činnostmi, při kterých jsou zpracovávány osobní údaje. Pro přehlednost celé analýzy uvádíme pouze ty aspekty zpracování osobních údajů, které dle našeho názoru nejsou v souladu s požadavky GDPR, resp. je sporné, zda by při případné kontrole byly shledány legálními či nikoliv. Ve zbylých procesech zpracování osobních údajů odkazujeme na záznamy o činnostech zpracování osobních údajů, které tvoří přílohu této analýzy.

V další části analýzy se zabýváme požadavky, které GDPR klade na smlouvy se zpracovateli osobních údajů a předávání osobních údajů subjektům do třetích zemí. Velmi podstatnou povinností je způsob plnění informační povinnosti a zajištění práv subjektů údajů, kterému se věnujeme v části IX. Dále analýza obsahuje další povinnosti vyplývající z GDPR, a to záznamy o činnostech zpracování a interní analýzu nazvanou posouzení vlivu na ochranu osobních údajů. Zabezpečením a úložištím osobních údajů je věnována jedna kapitola. V závěru se věnujeme způsobu hlášení porušení zabezpečení osobních údajů a problematice pověřence pro ochranu osobních údajů.

IV. O klientovi

Klient je právnickou osobou veřejného práva, která dle rejstříku škol a školských zařízení vykonává činnost základní umělecké školy. Zřizovatelem Klienta je město Holice. Kapacita školy je 600 žáků.

V. Seznam zdrojů GAP analýzy

Vycházeli jsme z dodaných podkladů, tzn. vyplněných dotazníků, zaslaných dokumentů a místního šetření.

Seznam podkladů ZUŠ Karla Malicha:

- "Organizační řád školy" – seznam směrnic
- Organizační řád školy – školní řád (2016)
- Organizační řád školy (2017)
- podpisové vzory
- Organizační řád školy – školní řád (2015)
- Organizační řád školy – vnitřní platový předpis
- Organizační řád školy – evidence majetku
- Organizační řád školy – oběh účetních dokladů
- Organizační řád školy – ochrana majetku školy
- Organizační řád školy – směrnice inventarizace majetku
- Organizační řád školy – spolupráce s policií
- Organizační řád školy – hospodaření s přebytečným, neupotřebitelným majetkem
- Organizační řád školy – směrnice pro určení výše školného a pronájem nástrojů
- Organizační řád školy – směrnice – provozní řád
- Organizační řád školy – směrnice závodní lékařská péče
- Organizační řád školy – směrnice pracovní náplně
- Organizační řád školy – poskytování cestovních náhrad
- Organizační řád školy – finanční kontrola (vnitřní kontrolní systém na škole)
- Organizační řád školy – směrnice – vyřizování stížností
- Organizační řád školy – směrnice – traumatologický plán
- Organizační řád školy – směrnice – pokladna
- Organizační řád školy – směrnice na ochranu osobních údajů
- Organizační řád školy – směrnice k čerpání dovolené
- Organizační řád školy – směrnice porušení kázně
- Evidenční list stížností, potvrzení o převzetí stížnosti, oznámení, podnětu
- Organizační řád školy – spisový a skartační řád školy
- Organizační řád školy – BOZP
- Organizační řád školy – směrnice kontrola práce neschopných zaměstnanců
- Organizační řád školy – směrnice pro poskytování informací
- Organizační řád školy – směrnice náhradová komise
- Organizační řád školy – vymáhání pohledávek
- Organizační řád školy – směrnice pro zadávání veřejných zakázek
- Dlouhodobý plán DVPP
- Organizační řád školy – ochrana dat zpracovaných výpočetní technikou
- Organizační řád školy – pronájem prostor školy
- Organizační řád školy – řády odborných učeben
- Organizace mimoškolní umělecké výchovy a vzdělávání
- Organizační řád školy – doplňková činnost
- Organizační řád školy – FKSP

• Organizační řád školy – BOZP (2013)
• Přihláška do Základní umělecké školy
• Odhláška ze studia na Základní umělecké škole
• Osobní dotazník (s hlavičkou)
• Osobní dotazník
• Datová schránka
• Smlouva o poskytování telekomunikačních služeb (Omcom)
• Zápis – dohlídka v rámci pracovnělékařské péče
• Smlouva o poskytování pacovnělékařských služeb
• Přípis ČSOB – kryptografická čipová karta
• Smlouva o využívání služby ČSOB Bussinesbanking 24
• Smlouva o vydání a používání Twins
• Protokol o podání žádosti o vydání TWINS
• Obchodní podmínky pro poskytování služby ČSOB elektronického bankovnictví
• Smlouva o poskytnutí software iZUŠ – informační systém základních uměleckých škol
• Příloha č.1 ke Smlouvě o poskytnutí software – všeobecné obchodní podmínky služby Český hosting (2016)
• Licenční smlouva (Vema)
• platový výměr
• pracovní smlouva
• dohoda o provedení práce (DČ)
• dohoda o provedení práce (soutěž)
• pracovní smlouva (nově příchozí)
• přihláška do soutěže
• záznam o provedení identifikace klienta
• smlouva o vedení účetnictví (ESOP)

VI. Agendy, při nichž dochází ke zpracování osobních údajů, a zákonnost jejich zpracování

Tato část je rozdělena podle jednotlivých činností Klienta. Těmi jsou:

- Umělecká výchova v oboru hudebním, tanečním, výtvarném a literárně-dramatickém
- Zapůjčování hudebních nástrojů žákům v rámci jejich výuky
- Prezentace vlastních zájmových uměleckých souborů a jejich veřejná vystoupení
- Pronájem prostor pro podnikání
- Organizování žákovských soutěží
- Provozování vydavatelské a polygrafické činnosti, knihařské a kopírovací práce v rámci výuky
- Organizování mimoškolní umělecké výchovy a vzdělávání, kurzy, školení, lektorské činnosti, pořádání konferencí, vlastní hudební produkce
- Výjezdy vlastních uměleckých souborů

a dále je zde zařazena také zaměstnanecká agenda, prezentace Klienta a kamerový systém.

Pro přehlednost celé analýzy uvádíme pouze ty aspekty zpracování osobních údajů, které dle našeho názoru nejsou v souladu s požadavky GDPR, resp. je sporné, zda by při případné kontrole byly shledány legálními či nikoliv. Ve zbylých (tzn. stoprocentně legálních) procesech zpracování osobních údajů odkazujeme na záznamy o činnostech zpracování osobních údajů, které tvoří přílohu této analýzy.

1. **Umělecká výchova v oboru hudebním, tanečním, výtvarném a literárně-dramatickém**

Přihláška ke studiu
Doporučujeme upravit přihlášku ke studiu a odstranit údaje o pracovišti a povolání zákonného zástupce, jelikož je tím porušena zásada minimalizace.

Součástí poučení by nemělo být udílení souhlasu se zpracováním. Právním důvodem pro běžné zpracování osobních údajů je již samotné přihlášení žáka.

Pro zveřejňování fotek a výsledků soutěží na internetu doporučujeme připojit souhlas k přihlášce. Vzor souhlasu tvoří přílohu této analýzy. Více v bodu 10. prezentace Klienta.

2. **Zapůjčování hudebních nástrojů žákům v rámci jejich výuky**

Nebyly dodány podklady pro evidenci výpůjček. Ve smlouvách by mělo být uvedené pouze jméno, příjmení, adresa trvalého bydliště, datum narození a kontaktní údaje nájemce.

3. **Prezentace vlastních zájmových uměleckých souborů a jejich veřejná vystoupení**

Pro zveřejňování fotek a výsledků soutěží na internetu doporučujeme připojit souhlas k přihlášce. Vzor souhlasu tvoří přílohu této analýzy. Více v bodu 10. prezentace Klienta.

4. **Pronájem prostor pro podnikání**

Nebyly dodány smlouvy pro pronájem prostorů k podnikání. Ve smlouvách by mělo být uvedené pouze jméno, příjmení, adresa trvalého bydliště a datum narození, popř. IČO a kontaktní údaje nájemce resp. identifikační a kontaktní údaje společnosti.

5. **Organizování žákovských soutěží**

Na základě místního šetření a dodaných podkladů se domníváme, že přihláška do soutěže splňuje zásadu minimalizace zpracování osobních údajů.

Ne vždy jsou účastníky pouze žáci školy, od nichž má Klient zajištěné souhlasy se zveřejněním výsledků a fotografií ze soutěží. Pro zveřejnění výsledků či fotografií ze soutěží mimo prostory školy (např. na internetu) doporučujeme zajistit souhlasy od účastníků, kteří nejsou žáky školy. Je možné je získat např. zaškrtnutím na účastnické listině.

6. **Provozování vydavatelské a polygrafické činnosti, knihařské a kopírovací práce v rámci výuky**

K této činnosti nebyly dodané podklady. Co se kronik či historických záznamů týká, tak prvně je nutné podotknout, že GDPR se nevztahuje na osoby zemřelé. Co se týče ostatních osob, kdy není možné si souhlas obstarat, domníváme se, že lze údaje zpracovat bez souhlasu dotčené osoby, jelikož za účel by se dle GDPR dala považovat archivace ve veřejném zájmu, příp. vědecký a historický výzkum dle čl. 9 odst. 2 písm. j) GDPR, avšak za dodržení podmínky přiměřenosti.

7. **Organizování mimoškolní umělecké výchovy a vzdělávání, kurzy, školení, lektorské činnosti, pořádání konferencí, vlastní hudební produkce**

V dohodách o provedení práce doporučujeme odstranit z požadovaných údajů zdravotní pojišťovnu. Toto doporučení je platné pro dohody, v rámci kterých je vyplácena odměna do 10.000 Kč, jelikož z nich není nutné odvádět zdravotní ani sociální pojištění. Pro dohody s odměnou nad 10.000 Kč doporučujeme údaj o zdravotní pojišťovně ponechat, případně zvážit použití dohody o pracovní činnosti nebo případně standardní pracovní poměr.

8. Výjezdy vlastních uměleckých souborů

K této činnosti nebyly dodány podklady. Obecně pro účely výjezdů je nutné rozlišovat zda se jedná o výjezd v rámci EU či mimo EU. Pokud pořádáte výjezd do zemí EU, jsou podmínky předání osobních údajů stejné jako v případě předání v rámci České republiky (především se jedná o informační povinnost). Pouze je navíc nezbytné v rámci informační povinnosti informovat o předávání do zahraničí.

Pokud se výjezd týká zemí mimo EU, pak je vhodné situaci konzultovat s pověřencem pro ochranu osobních údajů. Je nutné minimálně zjistit, zda existuje rozhodnutí Evropské komise o odpovídající ochraně osobních údajů a o tom žáky informovat.

Souhlasy se zpracováním osobních údajů v tomto případě nejsou potřeba. Samotným přihlášením na výjezd bere dotyčný na vědomí, že jím uvedené osobní údaje budou předány dále. Doporučujeme v rámci poučení na webových stránkách informovat subjekty údajů o tom, že údaje budou v nezbytné míře předány ubytovateli resp. pořadateli soutěže, výstavy, festivalu apod. Vzor poučení tvoří přílohu této analýzy.

9. Zaměstnanecká agenda

Doporučujeme upravit vstupní dotazníky zaměstnanců a to následovně:

- V dotazníku zaměstnance s ohledem na zásadu minimalizace zpracování os. údajů doporučujeme nevyžadovat rodinný stav.
- U dětí jako vyživovaných osob doporučujeme vyžadovat pouze jméno, příjmení a rodné číslo dítěte.
- U manžela/manželky jako vyživované osoby postačuje jméno, příjmení a identifikace zaměstnavatele.
- Z důvodu dodržení zásady minimalizace doporučujeme nekopírovat rodné listy dětí zaměstnanců.
- Zákon č. 328/1999 Sb. o občanských průkazech též neumožňuje kopírování občanských průkazů bez prokazatelného souhlasu. Z důvodu minimalizace zpracování osobních údajů OP též doporučujeme nekopírovat.

Pro bližší informace o tom, jaké údaje je možné zpracovávat a jaké nikoliv doporučujeme navštívit stránky Úřadu pro ochranu osobních údajů: https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171 .

10. Prezentace Klienta

Klient nezveřejňuje portrétní fotografie zaměstnanců na svých internetových stránkách. Klient zveřejňuje fotografie dětí a pedagogů na svých internetových stránkách jako individuální i skupinové fotografie z akcí Klienta. Klient v současné době nezveřejňuje na svých webových stránkách osobní údaje dětí, resp. fotografie se jmenným popiskem. Dle současného názoru Úřadu pro ochranu osobních údajů zveřejňování skupinových fotografií z výuky, resp. z akcí Klienta, není zpracováním osobních údajů ve smyslu zákona o ochraně osobních údajů a zřejmě ani podle GDPR.

Nicméně jelikož je situace v oblasti zveřejňování fotografií značně nepřehledná a nejistá, a navíc se může jednat též o fotografie malých dětí, doporučili bychom i tak si souhlas od zákonných zástupců vyžádat. Vzor souhlasu, který je použitelný nejen na fotografie, ale i uložení údajů o zdravotní pojišťovně, tvoří přílohu této analýzy.

11. Kamerový systém

Klient provozuje kamerový systém se záznamem. Zpracování osobních údajů v tomto rozsahu je řádně nahlášeno na ÚOOÚ. Kamery jsou umístěny na chodbách a na obvodu domu. Kamery slouží k zajištění bezpečnosti dětí a majetku Klienta. Kamery reagují pouze na pohyb. Délka uložení je proto zpravidla 10-14 dní, přes letní prázdniny až měsíc. Záznam je

uložen na vlastním serveru. K záznamům má přístup pouze správce budovy.
Pro soulad s požadavky GDPR je nezbytné označit prostory, že jsou snímány kamerovým systémem. Dále doporučujeme uzavřít se správcem zpracovatelskou smlouvu podle čl. 28 GDPR.

VII. Smlouvy se zpracovateli

Správce osobních údajů je ten, kdo určuje účel a prostředky zpracování osobních údajů. V běžných situacích je to Klient.

Zpracovatel je ten, kdo zpracování za správce provádí. Zpracovatelem však není zaměstnanec. Typickými zpracovateli jsou poskytovatelé cloudových nebo jiných IT řešení nebo externí účetní firmy.

Význam dělení na správce a zpracovatele spočívá v tom, že mezi nimi musí být vždy uzavřena písemná smlouva, přičemž za písemnou se považuje i elektronická podoba.

Zpracovatelská smlouva, aby vyhovovala GDPR, by měla obsahovat následující náležitosti:

- Předmět a doba trvání zpracování osobních údajů, povahu a účel zpracování, typ osobních údajů a kategorii subjektů údajů.
- Ustanovení, že zpracovatel osobních údajů nesmí do zpracování osobních údajů zapojit žádného dalšího zpracovatele bez předchozího konkrétního či obecného souhlasu správce.
- Ustanovení, že zpracovatel bude zpracovávat osobní údaje pouze v rozsahu stanoveném smlouvou mezi ním a správcem, případně na základě doložených pokynů správce.
- Ustanovení, že na osoby zpracovatele, které zpracovávají osobní údaje, se vztahuje zákonná povinnost mlčenlivosti nebo je zpracovatel k této mlčenlivosti smluvně zaváže.
- Ustanovení, že se zpracovatel zaváže přijmout taková technická, organizační a jiná potřebná opatření, spočívající např. v šifrování, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití.
- Ustanovení, že zpracovatel je povinen správci poskytnout součinnost pro případ výkonu jiných povinností správce podle GDPR, např. realizace práv subjektů údajů na přístup k osobním údajům či povinnosti ohlašovat porušení zabezpečení osobních údajů.
- Ustanovení, že zpracovatel je povinen vrátit správci po ukončení zpracování osobních údajů všechny osobní údaje, pokud to není v rozporu s jinými právními předpisy.
- Ustanovení, že zpracovatel poskytne správci veškeré informace potřebné k doložení splnění povinností podle GDPR a umožní správci kontrolu zákonnosti zpracování osobních údajů, pokud to neodporuje právnímu předpisu.

Klient je ve vztazích se všemi dotčenými subjekty údajů (zaměstnanci, žáci) správcem osobních údajů. V prostředí Klienta považujeme za zpracovatele též osoby, kteří Klientovi poskytují licenci k určitému programu, ve kterém jsou zpracovány osobní údaje, a současně poskytují Klientovi servisní služby k tomuto programu. To znamená, že za zpracovatele ve smyslu GDPR považujeme též třetí osoby, které mají bez dohledu Klienta přístup k jeho osobním údajům, ačkoliv spíše nahodilý. Upozorňujeme, že toto je striktní pojetí zpracovatelského vztahu a některé dozorové orgány obdobné situace nepovažují za vztah mezi správcem a zpracovatelem ve smyslu GDPR.

Na základě místního šetření a dodaných smluv uvádíme subjekty, které z hlediska GDPR mohou být považovány za subjekty s nimiž je nezbytné vyřešit smluvní vztah mezi správcem a zpracovatelem osobních údajů:

Sensio.cz s.r.o.
Dodatek smlouvy se společností Sensio.cz s.r.o. odpovídá požadavkům dle čl. 28. Doporučujeme pouze vyjasnit otázku předávání osobních údajů do třetích zemí, jelikož formulace odst. 1 v kapitole VIII je značně nejasná. S ohledem na smlouvu společnosti Sensio.cz s.r.o. se společností THINline s.r.o., kde je předávání do třetích zemí zmiňováno na několika místech, lze doporučit zajistit závazek zpracovatele, že osobní údaje Klienta nebudou předávány do třetích zemí mimo EU.
Pokud osobní údaje do třetích zemí budou předávány, tak musí tak být činěno na základě vhodných záruk ve smyslu příslušných ustanovení GDPR. V takovém případě je nutné upravit odpovídajícím způsobem informační povinnost (příloha č. 3).

Vema a.s.
Ze smlouvy se společností Vema a.s. přímo nevyplývá způsob spravování softwaru ze strany poskytovatele licence. Pokud spravuje software na základě vzdáleného přístupu, pak doporučujeme uzavřít dodatek k této smlouvě obsahující ustanovení podle čl. 28 GDPR. Vzor dodatku tvoří přílohu č. 5 této analýzy.

ESOP účetní a daňová kancelář s.r.o.
Ze smlouvy se společností ESOP účetní a daňová kancelář s.r.o. nelze zjistit, zda zpracovává osobní údaje zaměstnanců Klienta (např. výši mezd). Pokud ano, pak doporučujeme uzavřít dodatek k této smlouvě obsahující ustanovení podle čl. 28 GDPR. Vzor dodatku tvoří přílohu č. 5 této analýzy.

VIII. Předávání osobních údajů cizím subjektům, do třetích zemí

Klient nepředává v rámci své běžné činnosti osobní údaje do třetích zemí, tzn. do zemí mimo EU. V případě jednorázového předání do třetí země v budoucnu doporučujeme konzultovat toto předání s pověřencem pro ochranu osobních údajů.

IX. Plnění informační povinnosti a zajištění práv subjektů údajů

GDPR upravuje v článku 13 a 14 informační povinnost správce, resp. tomu odpovídající právo subjektu údajů být informován o zpracování svých osobních údajů. Správce či zpracovatel by měl subjektu údajů, jehož osobní údaje zpracovává, sdělit svoje identifikační údaje, dále informaci o tom, zda jmenoval pověřence pro ochranu osobních údajů a kdo jím je, pro jaký účel osobní údaje zpracovává a na jakém právním základě. Dále by měl subjekty údajů informovat o případných příjemcích či kategoriích příjemců osobních údajů a o případném úmyslu předat osobní údaje do třetí země a o existenci či neexistenci rozhodnutí Evropské komise o odpovídající ochraně.

Ačkoliv se informační povinnost jeví jako další administrativní zátěž, tyto informace není nutné sdělovat, pokud subjekt údajů již uvedené informace má.

Informační povinnost správce osobních údajů však zdaleka není bezbřehá. Není potřebné ani vhodné, aby správce, jestliže to není v jeho případě aktuální, informoval subjekt údajů o všech okolnostech uvedených v čl. 14 GDPR. To samé platí o poučení subjektů údajů o jejich

právech. Nicméně zpravidla každý správce a zpracovatel by měl subjekt údajů poučit o možnosti (i) uplatit právo na přístup k osobním údajům, (ii) uplatnit právo být zapomenut, (iii) uplatnit právo na opravu osobních údajů a (iv) uplatnit právo na omezení osobních údajů.

Klient bude plnit informační povinnost podle čl. 13 až 14 GDPR vůči svým zaměstnancům prostřednictvím Interní směrnice o ochraně osobních údajů, resp. jejích příloh, která všechny potřebné informace obsahuje.

Nicméně Klient je povinen plnit tuto informační povinnost též vůči jiným osobám, zejm. žákům. Jelikož lze tuto povinnost splnit i způsobem zajišťujícím dálkový přístup, doporučujeme zřídit nový interaktivní odkaz na webových stránkách nazvaný „ochrana osobních údajů“, který doporučujeme umístit do záložky dokumeny v menu (URL http://www.zusholice.cz/dokumenty). Zde je vhodné uveřejnit obsah dokumentu nazvaného „Informační povinnost správce“, jež tvoří přílohu této analýzy.

Klient je dále povinen zveřejnit informace týkající se pověřence pro ochranu osobních údajů na svých webových stránkách, kdy nejlépe v kontaktech bude zveřejněno jméno pověřence, sídlo/adresa, e-mail, telefon, údaj o dostupnosti, příp. ID datové schránky. Tuto povinnost již Klient splnil.

X. Záznamy o činnostech zpracování

Záznam o činnostech zpracování je písemný dokument, který definuje, jakým způsobem daná organizace zpracovává osobní údaje. Pro každý typ zpracování musí být veden samostatný záznam. Není tedy nutné zaznamenávat každé jednotlivé zpracování osobních údajů konkrétního člověka. Jinými slovy, správce má záznam o činnostech zpracování nazvaný „personální agenda“, ve kterém je obecně popsáno, se kterými údaji zaměstnanců se pracuje. Při přijetí nového zaměstnance se nový záznam o činnostech zpracování připravovat nebude, nicméně by správce osobních údajů měl postupovat v souladu se záznamem o činnostech zpracování. Záznam o činnostech zpracování je jakousi náhradou za oznamovací povinnost vůči Úřadu pro ochranu osobních údajů, která byla GDPR zrušena. Záznamy je nutné na žádost zpřístupnit Úřadu pro ochranu osobních údajů. Záznam totiž primárně slouží úřadu jako vodítko k tomu, aby se zorientoval v tom, jak v dané organizaci probíhá zpracování osobních údajů. Úřad pro ochranu osobních údajů bude také posuzovat, zda faktické zpracování v organizaci probíhá tak, jak je popsáno v záznamech o činnostech zpracování.
Záznamy o činnostech zpracování je nutné vést písemně, přičemž za písemnou podobu se považují i záznamy vedené v elektronické podobě.

Povinnost vést záznamy o činnostech zpracování osobních údajů dopadá prakticky na všechny subjekty, které osobní údaje zpracovávají. Není rozhodující, jestli se jedná o správce či zpracovatele osobních údajů. Nicméně GDPR stanovuje výjimku, a to, že záznamy o činnostech zpracování nemusejí vést společnosti a organizace, které zaměstnávají méně než 250 zaměstnanců. Nicméně výjimka má další výjimky, protože je zároveň nutné s počtem zaměstnanců splnit další tři podmínky. Těmi jsou:

- zpracování nesmí představovat riziko pro práva a svobody subjektů údajů;
- zpracování nesmí být příležitostné a
- zpracování nesmí zahrnovat zvláštní kategorie osobních údajů.

Z výše uvedeného lze dovodit, že Klient, který nezpracovává osobní údaje příležitostně a taktéž zpracovává osobní údaje ze zvláštní kategorie osobních údajů, musí vést záznamy o činnostech zpracování.

GDPR stanovuje minimální rozsah údajů, které musí záznamy o činnostech zpracování obsahovat. Jedná se o:

- Kontaktní údaje správce osobních údajů.
- Údaje o pověřenci pro ochranu osobních údajů.
- Účel zpracování osobních údajů.
- Popis činnosti zpracování.
- Kategorie subjektů údajů dotčených předmětným zpracováním
- Popis kategorií osobních údajů.
- Kategorie příjemců, kterým budou nebo byly osobní údaje sděleny nebo jinak zpřístupněny.
- Předávání osobních údajů do třetích zemí nebo mezinárodní organizaci. Třetími zeměmi se rozumí nečlenské státy EU.
- Plánovaná lhůta pro výmaz osobních údajů, je-li to možné. Některé lhůty pro výmaz vyplývají přímo ze zákona, resp. ze spisového a skartačního řádu.
- Obecný popis technických a organizačních bezpečnostní opatření.

Záznamy o činnostech zpracování pro Klienta tvoří přílohu interní směrnice a přílohu č. 2 této analýzy.

XI. Posouzení vlivu na ochranu osobních údajů

Z článku 35 odst. 1 GDPR vyplývá, že posouzení vlivu na ochranu osobních údajů, tzv. DPIA musí být provedeno v případě, kdy určitý druh zpracování údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, a to zejména při využití nových technologií. Nicméně vypracování DPIA zpravidla nebude nutné, i když je splněna výše uvedená podmínka, pokud je zpracování upravené právním předpisem (§ 9 návrhu zákona o ochraně osobních údajů).

Článek 35 odst. 3 GDPR dále uvádí demonstrativní výčet operací s osobními údaji, které vyžadují posouzení vlivu na ochranu osobních údajů. DPIA je nutné zejména v těch případech, kdy správce či zpracovatel realizuje:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
- rozsáhlé zpracování zvláštních kategorií údajů (např. údajů o rasovém či etnickém původu, politických názorech či zdravotním stavu anebo biometrických údajů atd.) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů;
- rozsáhlé systematické monitorování veřejně přístupných prostorů.

Navíc dle návrhu adaptačního zákona (pravděpodobně nebude schválen do účinnosti GDPR) není nutné provádět posouzení vlivu na ochranu osobních údajů v případě, že zpracování vyžaduje/výslovně povoluje právní předpis.

Dle dodaných podkladů by přicházelo v úvahu pouze posouzení vlivu na ochranu osobních údajů v případě provozování kamerového systému. Nicméně jelikož se nejedná o rozsáhlé systematické monitorování veřejně přístupných prostor a nadto bylo toto monitorování schváleno ÚOOÚ, není nutné posouzení vlivu na ochranu osobních údajů vypracovávat.

XII. Úložiště a zabezpečení osobních údajů

Dle požadavků GDPR je nutné zpracovávané osobní údaje vhodně zabezpečit, přičemž vhodné zabezpečení je věc individuální pro každou organizaci. Zejména je nutné vzít v potaz povahu, rozsah, kontext a účel zpracování a také riziko, které potenciálně hrozí subjektům údajů v případě jejich zneužití. Z toho vyplývá, že citlivé osobní údaje (např. údaje o zdravotním stavu) je zásadně nutné chránit více a lépe než běžné osobní údaje (např. seznamy osob).

Dle informací, které jsme obdrželi, jsou dokumenty v listinné podobě uchovávány mimo dosah žáků v uzamykatelných prostorách, čímž je zajištěna bezpečnost těchto údajů.

V elektronické podobě jsou uloženy v systému iZUŠ na cloudu, kdy Klient má nastavená odlišná přístupová oprávnění podle pracovního zařazení. Údaje o zaměstnancích jsou taktéž velmi dobře zabezpečeny s tím, že k nim má přístup pouze ředitel a zástupce ředitele školy a správce systému.

Úroveň technického a organizačního zabezpečení hodnotíme jako dobrou a profesionálně zpracovanou a nemáme k nim výtek. Doporučujeme pouze aktualizovat část 33 organizačního řádu školy – ochrana dat zpracovaných výpočetní technikou a odstranit odkaz na zákon č. 101/2000 Sb. o ochraně osobních údajů.

XIII. Hlášení porušení zabezpečení osobních údajů

Pokud dojde z jakéhokoli důvodu k porušení zabezpečení osobních údajů, musí na to správce osobních údajů bez zbytečného odkladu, zpravidla však do 72 hodin, upozornit Úřad pro ochranu osobních údajů. Ohlášení případu není nutné, pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob (čl. 33 odst. 1 nařízení). Jelikož v současnosti neexistuje formulář na stránkách Úřadu pro ochranu osobních údajů pro případy hlášení porušení, měl by správce oznámení podat nejlépe prostřednictvím datové schránky.

Postup hlášení porušení osobních údajů a odpovědnost u Klienta je detailně popsána v interní směrnici pro ochranu osobních údajů, která tvoří přílohu č. 1 této analýzy.

XIV. Pověřenec pro ochranu osobních údajů

V souvislosti s GDPR se často mluví o tzv. pověřenci na ochranu osobních údajů. Pověřenec pro ochranu osobních údajů je institut přejatý z německého práva. Osoba, kterou správce osobních údajů jmenuje pověřencem, má na starosti poskytovat informace a poradenství správcům osobních údajů nebo zpracovatelům osobních údajů a monitorovat soulad s GDPR. Další jeho povinností je spolupracovat s ÚOOÚ a zároveň pro tento úřad působit jako kontaktní místo.

V čl. 37 GDPR jsou definovány subjekty, které musí jmenovat pověřence pro ochranu osobních údajů. Jsou to:

- orgány veřejné moci nebo veřejné subjekty;
- subjekty, jejichž hlavní činnost spočívá ve zpracování osobních údajů prostřednictvím systematického monitorování subjektů údajů a
- subjekty, které rozsáhle zpracovávají osobní údaje ze zvláštní kategorie údajů, dříve známé jako citlivé údaje (údaje o zdravotním stavu, etnickém původu, sexuální orientaci apod.).

Stanovisko skupiny WP29[1] v nejasných případech doporučuje, aby správci a zpracovatelé vytvořili interní analýzu provedenou s cílem určit, zda by pověřenec pro ochranu osobních údajů měl, či neměl být jmenován, a aby tuto analýzu uchovali a byli tak schopni prokázat, že byly řádně zohledněny relevantní faktory. Pověřence pro ochranu osobních údajů je však případně možné jmenovat i dobrovolně, a vyhnout se tak zbytečným komplikacím.

Klient se rozhodl jmenovat pověřence pro ochranu osobních údajů. Pověřenec ze své pozice musí mít přístup k informacím důležitým pro jeho činnost. Správce či zpracovatel musí pověřenci zajistit přístup k potřebným podkladům a zdrojům. Jelikož pověřenec bude často potřebovat podklady od konkrétních zaměstnanců, je nutné, aby zaměstnanci byli informováni o existenci pověřence a o povinnosti poskytnout mu potřebnou součinnost. Toto by měl Klient zajistit proškolením zaměstnanců o GDPR a interní směrnici.

Ať již je pověřencem zaměstnanec nebo podnikající osoba, odpovědným za dodržování předpisů ohledně osobních údajů je vždy Klient. Pověřenec je pouhým pozorovatelem, který dává doporučení, jak zajistit soulad s GDPR. Klient by se jeho doporučeními měl řídit. Na druhou stranu pověřenec není od toho, aby případná porušení či nedodržování doporučení správcem dále hlásil. Pověřenec splnil své povinnosti tím, že správci doporučil změnu, a své doporučení si zaznamenal.

XV. Shrnutí základních doporučení

Základním mapováním zpracování osobních údajů bylo zjištěno, že nedochází k zásadnímu porušování GDPR. Naopak Klient má velmi dobře propracované interní dokumenty, které jsou relevantní v oblasti ochrany osobních údajů. Vesměs veškeré nedostatky jsou způsobeny přechodem na novou právní úpravu a je na ně adekvátně reagováno.

Na základě této analýzy doporučujeme implementovat povinnosti z GDPR v následujících dokumentech:

- přijetí a dodržování nové Interní směrnice o ochraně osobních údajů a tím zároveň provést nahrazení staré směrnice;
- zajištění souhlasu pro zpracování osobních údajů vždy po dobu docházky od zákonného zástupce žáka: vzorový souhlas tvoří přílohu č. 2 Interní směrnice pro ochranu osobních údajů;
- vést a aktualizovat záznamy o činnostech zpracování osobních údajů: tyto záznamy tvoří přílohu č. 3 Interní směrnice pro ochranu osobních údajů;
- plnění informační povinnost vůči veřejnosti na webových stránkách Klienta;
- pozměnit interní dokumenty (přihlášky, dotazníky apod.) s ohledem na zásadu minimalizace zpracování osobních údajů;
- doporučujeme aktualizovat část 33 organizačního řádu školy – ochrana dat zpracovaných výpočetní technikou a odstranit odkaz na zákon č. 101/2000 Sb. o ochraně osobních údajů.

Všechny doporučené změny (kromě změn v interních dokumentech, které nebyly dodány v elektronické podobě) tvoří přílohu této analýzy. Pro změny v interních dokumentech Klienta předkládáme doporučení v rámci analýzy, na základě kterých lze tyto dokumenty upravit.

Přílohy:

1. Interní směrnice o ochraně osobních údajů
2. Záznamy o činnostech zpracování osobních údajů ZUŠ Karla Malicha
3. Informační povinnost správce osobních údajů

[1] Pracovní skupina 29 byla ustanovena článkem 29. směrnice 95/46/EC jako nezávislý evropský poradní orgán na ochranu dat a soukromí. Je složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie.

4. Doložka o mlčenlivosti pro zaměstnance nepodléhající povinnosti mlčenlivosti
5. Vzorové ustanovení/dodatek do smluv mezi správcem a zpracovatelem osobních údajů
6. Souhlas se zpracováním osobních údajů