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 škola Bruntál, Okružní 38, příspěvková organizace
Okružní 1890/38
792 01 Bruntál

Vaše značka	Naše značka	Praha
-----	GDPR/2017/019	---

ANALÝZA SOULADU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZÁKLADNÍ ŠKOLY BRUNTÁL, OKRUŽNÍ 38 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“) zadal Městský úřad Bruntál, se sídlem Nádražní 994/20, 79201 Bruntál, advokátní kanceláři Holubová advokáti s.r.o. (dále jen „AK“) vypracování GAP analýzy neboli analýzy souladu stavu zpracování osobních údajů ZŠ Bruntál, Okružní 38 (dále jen „Klient“) s požadavky GDPR. Účelem této analýzy je tedy zjistit současný stav zpracování osobních údajů v Klientovi a navrhnout změny k dosažení souladu zpracování osobních údajů s požadavky GDPR.

Tato zpráva vychází z právního stavu, který nabude účinnosti 25. 5. 2018. Neposuzuje faktický soulad činností Klienta se stávající legislativou o ochraně osobních údajů a z tohoto důvodů ani nezkoumá ani nečiní výčet existujících plnění oznamovacích povinností – tzv. registrací u Úřadu pro ochranu osobních údajů.

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 nahradí současnou 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 budou 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 se 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 únoru 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 analýze nazvané 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 vykonává činnost základní školy, školní jídelny a školní družiny. Zřizovatelem Klienta je město Bruntál. Školu navštěvuje přibližně 400 žáků.

V. Seznam zdrojů GAP analýzy

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

1. GDPR analýza technického stavu
2. kamery foto
3. LVVZ informace + návratka
4. mapování
5. pracovní smlouva vzor
6. přihlášení do informačního systému
7. školní server v PC učebně
8. smlouva DM software
9. smlouva VEMA
10. smlouva VIS
11. smlouva závodní lékař
12. souhlas se zpracováním osobních údajů, záznamů…
13. co doložit k nové pracovní smlouvě
14. žádost o přestup
15. údaje dítěte
16. osobní dotazník zaměstnance
17. leták školy

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

Tato část je rozdělena podle jednotlivých činností Klienta. 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. Základní škola

V oblasti přijímání a poskytování základního vzdělávání je Klient povinen vést tzv. školní matriku. Tuto vede převážně elektronicky v systému DM software. V dodaném formuláři od DM software (karta při zápisu) jsme shledali, že několik údajů by Klient požadovat neměl, resp. by u nich mělo být jednoznačně uvedeno, že se jedná o nepovinné údaje. Platí, že ke zpracování osobních údajů musí existovat právní důvod. V případě vedení školní matriky je tímto důvodem zpravidla zákon č. 561/2004 Sb., školský zákon a některé podzákonné předpisy (zejm. vyhláška č. 364/2005 Sb., o dokumentaci škol a školských zařízeních). Tyto předpisy specifikují, co jsou povinné údaje uvedené ve školní matrice. Pro další je třeba hledat jiný právní důvod zpracování, kterým bude zpravidla dobrovolné sdělení

odpovídajícího souhlasu se zpracováním osobních údajů. Údaji, které bez dalšího nelze od žáků požadovat, resp. existují o tom pochybnosti, jsou:

- zdravotní pojišťovna,
- zaměstnavatel a funkce zákonných zástupců.

Požadavek na uvedení zaměstnavatele rodičů nemá oporu v žádném právním předpise. Klient zpravidla nepracuje s těmito údaji, může je využít pouze v případě, že potřebuje zákonné zástupce rychle kontaktovat. K tomu mu však postačí např. jejich telefonní číslo, resp. telefonní číslo na zaměstnavatele a nepotřebuje znát funkci zákonného zástupce.

V oblasti průběhu základního vzdělávání je nutné podotknout, že uchování údaje o zdravotní pojišťovně, tzn. i kód zdravotní pojišťovny, mateřském jazyku a sourozenci v mateřské škole dle metodiky MŠMT podléhá souhlasu zákonného zástupce dítěte. Dle našeho názoru tomu tak sice není, jelikož je oprávněným zájmem Klienta znát a mít v případě potřeby přístupné tyto údaje, nicméně z opatrnosti vycházíme z přísnější úpravy, a tedy doporučujeme mít tento souhlas se zpracováním osobních údajů. Vzorový souhlas, který tvoří přílohu této analýzy, reflektuje názor MŠMT, jelikož je přísnější než názor naší advokátní kanceláře.

Doporučení: Doporučujeme nepožadovat od zákonných zástupců údaj o zaměstnání a funkci. Doporučujeme zajistit souhlas s uchováním údaje o zdravotní pojišťovně nebo jasně označit, že se jedná o nepovinný údaj.

2. Propagace školy

Klient zveřejňuje fotografie dětí a učitelů na svých internetových stránkách. Klient v současné době nemá vlastní facebook, twitter či jinou sociální síť, kde by zveřejňoval osobní údaje žáků a zaměstnanců. Klient v současné době uvádí maximálně křestní jméno a třídu spolu s fotografií žáka. Dle současného názoru Úřadu pro ochranu osobních údajů zveřejňování skupinových fotografií z výuky, resp. z akcí Klienta bez jmenného popisku, 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 jedná o fotografie dětí, doporučili bychom i tak si souhlas od zákonných zástupců vyžádat. Vzor souhlasu, který je použitelný nejen na fotografie, ale i na uložení údajů o zdravotní pojišťovně, tvoří přílohu této analýzy.

Klient dále zveřejňuje fotografie dětí v prostorách budovy školy. Žáci se tak mohou dozvědět, jaké výtvory zhotovili jejich spolužáci a mají tak možnost poznat se i mimo vlastní třídu, čímž jsou naplňovány zásady vzdělávání. Dle našeho názoru není třeba ke zveřejnění fotografií, obrázků (autorských děl) a podobných děl v prostorách budovy školy souhlas zákonných zástupců, jelikož se jedná o způsob výuky, tedy je zveřejněním ve veřejném zájmu (přispívá vzájemnému porozumění mezi dětmi).

Klient sice v současné době disponuje souhlasem se zpracováním osobních údajů, nicméně tento souhlas do budoucna již nebude odpovídat požadavkům GDPR, a to z toho důvodu, že žák, resp. jeho zákonný zástupce, nemůže souhlasit pouze s určitým typem zpracování osobních údajů (tzv. granulovaný souhlas), např. pouze s pořizováním záznamů pedagogického procesu ve třídě, jelikož je souhlas založen na zásadě všechno nebo nic. Vedle toho souhlas vychází ze současné právní úpravy a obsahuje tak odkaz na zákon o ochraně osobních údajů, který bude zrušen.

Doporučení: Doporučujeme nadále nepoužívat Souhlas se zpracování osobních údajů nebo ho upravit dle požadavků GDPR, tedy zejm. zajistit tzv. granulovaný souhlas a poučit žáka o právu souhlas odvolat. Alternativně lze použít vzorový souhlas, který tvoří přílohu této

analýzy.

3. Školní jídelna
Na základě místního šetření a dodaných podkladů se domníváme, že provoz školní jídelny odpovídá požadavkům GDPR. Nicméně doporučujeme v systému školní jídelny zajistit pravidelný výmaz údajů ze systému (VIS Plzeň), které nepodléhají vedení školní matriky.

4. Školní družina
Na základě místního šetření a dodaných podkladů se domníváme, že provoz školní družiny odpovídá požadavkům GDPR.

5. Zaměstnanci
Zaměstnanci musí při nástupu do zaměstnání vyplnit osobní dotazník zaměstnance. Tento dotazník dle našeho názoru neobsahuje žádné nadbytečné osobní údaje o zaměstnanci, tedy jedná se pouze o údaje vyžadované právními předpisy. K pracovní smlouvě dále zaměstnanec přikládá: vstupní lékařskou prohlídku, výpis z rejstříku trestů, doklad o posledním ukončeném vzdělání a vysvědčení, zápočtový list, kartičku pojišťovny, kartičku od bankovního účtu a emailovou adresu k zasílání výplatních lístků.

Na tomto místě si dovolujeme upozornit, že zasílání výplatních pásek emailem je možné, nicméně podléhá větší ochraně a je tak třeba minimálně soubor obsahující výplatní lístek zaheslovat.

V pracovní smlouvě jsou uvedeny údaje zaměstnanců v rozsahu: jméno, příjmení, titul, datum narození, rodné číslo a adresa. Z hlediska minimalizace osobních údajů doporučujeme, aby rodné číslo bylo uvedeno pouze v osobním dotazníku a nikoliv též v pracovní smlouvě.

6. Kamery
Klient provozuje 5 kamer, které zabírají chodby školy (vestibul, šatny) a hlavní vchod. Kamery nejsou namířené do tříd, převlékáren či sborovny. Záznam je uchován po dobu 30 dnů. Ve veřejném registru Úřadu pro ochranu osobních údajů není záznam o tom, že by Klient byl na ÚOOÚ registrován. Ačkoliv by to znamenalo případný rozpor se současným zákonem o ochraně osobních údajů, GDPR tuto registrační povinnost ruší. Doba uchování je 30 dnů. Upozorňujeme, že 30 dnů je doba hraniční, za dobu obvyklou se zpravidla považují 3 dny.

7. Docházkový systém
Klient na základě smlouvy s VIS Plzeň má koupenou licenci na provozování tzv. vrátnice. Tento program pomocí čipu umožňuje žákům a učitelům projít do budovy školy. Údaj o tom, kdo v kolik hodin přišel, je zaznamenán. Doporučujeme vymazat tato data vždy na konci školního roku.

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.

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, strávníci) 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.

Klient nám předložil následující smlouvy, které z hlediska GDPR mohou být považovány za smlouvy mezi správcem a zpracovatelem osobních údajů:

- Smlouva o poskytování aplikačních služeb (ASP) mezi Klientem a Vema, a.s.;
- Smlouva s dm Software;
- Smlouva o poskytování licencí k užití SW a souvisejících služeb mezi Klientem a Veřejnou informační službou, spol. s.r.o. (VIS Plzeň);
- Smlouva se společností alarmy Vávra (správce kamerového systému).

Co se týče smlouvy se společností Vema, a.s., ta plně reflektuje povinnosti vyplývající ze současné legislativy, nicméně závazek k některým povinnostem absentuje (např. povinnost součinnosti). Doporučili bychom též, aby se Vema, a.s. zavázala, příp. potvrdila, že její servery se nachází na území Evropské unie, nikoliv ve třetích zemích.

Smlouva se společností dm Software, která obdobně jako Vema, a.s. zajišťuje ukládání údajů na vlastních serverech, obsahuje Přílohu č. 1, která se věnuje ochraně osobních údajů. Obdobě jako u smlouvy s Vema, a.s. i zde vychází tato příloha ze současné právní úpravy, tedy ze zákona o ochraně osobních údajů. Některé nové povinnosti tak absentují (např. povinnost

nezapojit do zpracování dalšího zpracovatele bez souhlasu Klienta). Dále doporučujeme, aby se dm Software zavázal, příp. potvrdil, že jeho servery se nacházejí na území Evropské unie, nikoliv ve třetích zemích.

Z naší činnosti víme, že VIS Plzeň již nabízí dodatek smlouvy tak, aby reflektoval povinnosti společnosti VIS jakožto zpracovatele osobních údajů.

Smlouvu se společností alarmy Vávra nemáme k dispozici, nicméně ve striktním pojetí jsou i oni zpracovateli osobních údajů, jelikož mohou mít přístup k záznamům bez dohledu správce – Klienta.

Doporučujeme uzavřít dodatek ke všem těmto smlouvám tak, aby obsahoval ustanovení podle čl. 28 GDPR. Vzor dodatku tvoří přílohu této analýzy.

VIII. Předávání osobních údajů cizím subjektům, do třetích zemí

Klient nepředává osobní údaje do třetích zemí, tzn. 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 zákazníkovi či zaměstnanci, 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 může plnit informační povinnost podle čl. 13 až 14 GDPR vůči svým zaměstnancům prostřednictvím Interní směrnice o ochraně osobních údajů, resp. jejích příloh, které všechny potřebné informace obsahují.

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 rozdělit interaktivní odkaz na část týkající se zákona o veřejném přístupu k informacím a ochraně osobních údajů na tomto místě: http://zsbrok.cz/povinne-informace/. Nový odkaz nazvaný „ochrana osobních údajů“ by obsahoval předmětné informace, jež tvoří přílohu této analýzy.

Klient je dále povinen zveřejnit informace týkající se pověřence pro ochranu osobních údajů na svých webových stránkách, kdy na adrese http://zsbrok.cz/category/kontakty/ doporučujeme zřídit nový odkaz nazvaný pověřenec pro ochranu osobních údajů, kde bude zveřejněno jméno pověřence, sídlo/adresa, e-mail, telefon, údaj o dostupnosti, příp. ID datové schránky.

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 je orgánem veřejné moci a jehož některá zpracování (např. v oblasti poskytování podpůrných opatření) představují riziko pro práva a svobody subjektů údajů a taktéž 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 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, 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).

Klient důkladně zmapoval a zdokumentoval použití osobních dat v rámci organizace a jejich technické zabezpečení:

- jaká osobní data se elektronicky zpracovávají;
- kde jsou data uložena (datové uložiště, informační systémy);
- kam a jak se data předávají;

- jaká je ochrana sítě, klientských zařízení (PC, mobil) a serverových komponent.

Za nedostatečné považujeme umístění školního serveru v počítačové učebně bez jakéhokoliv fyzického zabezpečení. K serveru tak mají přístup všichni žáci a učitelé. Doporučujeme přesunout server na místo, kam budou mít přístup pouze oprávněné osoby. Ve zbytku hodnotíme úroveň technického zabezpečení jako odpovídající úrovni osobních údajů, které Klient zpracovává.

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 ELKA na vlastním serveru a dm Software na serveru poskytovatele. Klient má nastavená odlišná přístupová oprávnění podle pracovního zařazení zaměstnanců. Dále je omezen přístup k tzv. citlivým osobním údajů žáků, které má k dispozici zpravidla pouze výchovný poradce a třídní učitel (příp. ředitel školy). Údaje o zaměstnancích jsou taktéž adekvátně dobře zabezpečené s tím, že k nim má přístup pouze ředitel školy a mzdová účetní.

Níže uvedené odstavce popisují návrhy na rozšíření technického zabezpečení. Některé z doporučení mohou být již implementovány, neboť nám nebyly zřejmé z dodaných podkladů.

Předávání dat a elektronická komunikace

- V případě nutnosti předání citlivých dat na externí email, například rodičům, doporučujeme zaslat emailem link na webový portál, kde se klient autentizuje a stáhne si data přes zabezpečené https spojení. Alternativním řešením je zaslat citlivá data jako zašifrovaný soubor přiložený v emailu (př. zip soubor).
- V rámci interního školení a pravidel pro používání citlivých dokumentů, doporučujeme poučit zaměstnance o bezpečných kanálech komunikace. V případě otázek by měl mít zaměstnanec možnost konzultovat bezpečnost kanálu s pověřencem pro ochranu osobních údajů či s IT oddělením.

Úložiště

- Doporučujeme dokumenty s osobními údaji (existují-li) ukládat na sdíleném file server a vyhnout se ukládání souborů na lokální zařízení (PC, notebook, flash disk). Tento server je přístupný v rámci LAN a přes VPN mimo organizaci. V případě, že toto není možné, doporučujeme zapnout šifrování úložišť lokálních zařízení, např. službou Bit Locker dostupnou od Win7 a důsledně vyžadovat autentizaci.
- Všechna úložiště musí být pravidelně a bezpečně zálohovány včetně dat, která jsou uložena lokálně na PC v rámci organizace.

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 úřadem 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.

Jelikož je Klient orgánem veřejné moci, s ohledem na výše uvedené musí jmenovat pověřence pro ochranu osobních údajů. Pověřenec poté plní své povinnosti vůči všem aktivitám Klienta (tedy nejen základní škole, ale i školní jídelně, školnímu klubu, školní družině a stanici zájmových činností).

Pověřenec pro ochranu osobních údajů může být zaměstnanec nebo může úkoly plnit na základě smlouvy o poskytování služeb. Pověřenec jako zaměstnanec musí být přímo podřízen vrcholovým řídícím pracovníkům. Z toho vyplývá, že pověřencem nemůže být statutární orgán, tedy ředitel. Pověřence je též možné sdílet s jinými správci či zpracovateli.

Podstatnou náležitostí postavení pověřence je jeho nezávislost. Tím je míněno, že pověřenec nesmí dostávat žádné pokyny ohledně výkonu svých úkolů. Nezávislost pověřence je též zaručena zákazem sankcí za plnění úkolů pověřence. Pokud je pověřenec zaměstnancem správce, nesmí být propuštěn v souvislosti s plněním svých úkolů. Zároveň nesmí být pověřenec ve střetu zájmů, který by mohl vzniknout v souvislosti s jinou činností pro správce, resp. zpracovatele.

Co se týče odborných znalostí, pověřenec by měl mít znalosti práva a praxe v oblasti ochrany osobních údajů. Důležité mohou být také jiné znalosti (např. znalost v oblastech IT a bezpečnosti dat). Úroveň znalostí by měla odpovídat rozsahu, citlivosti a způsobu zpracování. Jiné znalosti tedy bude mít pověřenec pro školu, jiné pro hlavní město Praha a jiné pro Facebook.

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

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.

pověřenec bude často potřebovat podklady od konkrétních zaměstnanců, je nutné, aby zaměstnanci byli informováni o existenci pověřence a o povinnosti poskytnout mu potřebnou součinnost.

Doporučujeme Klientovi, aby sdělil zaměstnancům, např. na pedagogické poradě, kdo je pověřencem Klienta.

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. Správce 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. Správce se jeho doporučeními nemusí řídit.

XV. Shrnutí základních doporučení

1. Klient požadoval v zadání této analýzy identifikaci a popis dopadů nařízení GDPR do procesů ZŠ Bruntál zahrnující nejméně následující okruhy:

a. udělování souhlasu se zpracováním osobních údajů;
   Popis procesu udělování souhlasu se zpracováním osobních údajů je popsán v bodě VI.2, dále ve vzorové směrnici o ochraně osobních údajů a ve vzoru souhlasu pro účely Klienta, které tvoří přílohu této analýzy.
b. zpracování a uchování osobních údajů;
   Zpracování a uchování osobních údajů je popsáno v bodu XII. a dále ve vzorových záznamech o činnostech zpracování osobních údajů.
c. organizační opatření proti ztrátě, zničení, poškození a odcizení osobních údajů;
   Organizační opatření spočívající v povinnostech zaměstnanců chránit osobní údaje, jsou detailně popsána v návrhu interní směrnice o ochraně osobních údajů.
d. eskalační procedury a postupy pro hlášení incidentů;
   Eskalační procedury a postupy pro hlášení incidentů pro prostředí mateřských škol jsou popsány v návrhu interní směrnice pro prostředí základních škol.
e. organizační struktura a odpovědnosti za ochranu osobních údajů;
   Organizační struktura a odpovědnosti za ochranu osobních údajů jsou popsány v návrhu interní směrnice pro prostředí základních škol.
f. předávání osobních údajů;
   Předávání osobních údajů do třetích zemí je popsáno v bodu VIII.
g. právo být zapomenut – po stránce právní a technické;
   Právo být zapomenut a jeho realizace je popsána (i) v návrhu interní směrnice o ochraně osobních údajů a (ii) v bodě IX. resp. v dokumentu nazvaném informační povinnost správce.
h. další související interní a externí procesy.

Dále Klient požadoval v zadání této analýzy:

2. identifikaci a pojmenování procesů, které osobní údaje zpracovávají
Procesy zpracování osobních údajů jsou identifikované a pojmenované v bodu VI. a také v podkladu pro záznamy o činnostech zpracování osobních údajů.

3. identifikace aktuálně provozovaných a nově řešených (připravovaných) technických opatření
Tato agenda je zevrubně popsána v bodu XII. této analýzy.

4. identifikace souvisejících (existujících i neexistujících, interních i externích) organizačních opatření a technických řešení prostředí ICT, které bude nutné aktualizovat a navrhnout způsob a znění jejich aktualizace a znění nových předpisů.
Organizační opatření jsou identifikována průběžně v celé analýze, nicméně jako nejvýznamnější se nám jeví:

- *přijmout interní směrnici o ochraně osobních údajů a proškolit o ní zaměstnance, kteří přicházejí (i pasivně) do styku s osobními údaji*
- *realizace informační povinnosti Klienta*
- *vést a aktualizovat záznamy o činnostech zpracování osobních údajů*
- *uzavřít dodatky ke smlouvám se zpracovateli*

5. Na základě identifikovaných rozdílů, změn a znalosti prostředí vytvořit a prioritizovat kroky, které zajistí potřebné úpravy.
Viz bod 4.

XVI. Shrnutí

Základním mapováním zpracování osobních údajů bylo zjištěno, že nedochází k zásadnímu porušování GDPR. 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 zejm. v následujících krocích:

- uzavření smluv, resp. dodatků smluv se společností VEMA a dm Software, příp. VIS Plzeň a alarmy VÁVRA dle vzoru obsaženého v příloze této analýzy;
- přemístit školní server na bezpečnější místo;
- přijetí a dodržování Interní směrnice o ochraně osobních údajů;
- zajištění souhlasu, resp. jeho úprava pro zpracování osobních údajů dětí a jejich zákonných zástupců vždy od zákonného zástupce žáka: vzorový souhlas tvoří přílohu této analýzy;
- vést a aktualizovat záznamy o činnostech zpracování osobních údajů: Podklad pro vyplnění záznamů tvoří přílohu této analýzy;
- jmenovat/vybrat pověřence pro ochranu osobních údajů a uzavřít s ním smlouvu;
- zveřejnit údaje o pověřenci na webových stránkách Klienta a nahlásit ho na Úřad pro ochranu osobních údajů;
- plnění informační povinnosti vůči veřejnosti na webových stránkách Klienta;
- proškolit zaměstnance (zejm. pedagogické) o jejich povinnostech vyplývajících z GDPR.

Všechny doporučené změny dokumentů tvoří přílohu této analýzy.

Přílohy:
1. Interní směrnice o ochraně osobních údajů
2. Záznamy o činnostech zpracování osobních údajů ZŠ Bruntál
3. Informační povinnost správce osobních údajů
4. Doložka o mlčenlivosti pro zaměstnance nepodléhající povinnosti mlčenlivosti, tzn. nepedagogičtí zaměstnanci
5. Vzorové ustanovení/dodatek do smluv mezi správcem a zpracovatelem osobních údajů