PIERSTONE

GDPR Desatero pro školy

1. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

Jmenujte pověřence pro ochranu osobních údajů. Zajistěte, aby mu byl vydělen dostatečný čas a prostředky na plnění jeho úkolu a aby byl podřízen přímo vedení školy. Může to být stávající zaměstnanec nebo nový zaměstnanec, zpravidla na částečný úvazek či externí pracovník. Jeden pracovník může tuto roli vykonávat pro více škol.

Školy, jakožto veřejné subjekty[1], budou mít vždy povinnost jmenovat pověřence pro ochranu osobních údajů. Mezi hlavní úkoly pověřence patří poskytovat poradenství vedení školy a být kontaktním místem jak pro ÚOOÚ[2], tak pro subjekty údajů, tedy zejména žáky, rodiče a učitele.

Dle metodiky MŠMT může být pověřencem jak zaměstnanec školy, tak externí pracovník či společnost. Jedinou výjimkou v rámci vzdělávacího sektoru je Česká školní inspekce, která jakožto služební úřad dle stanoviska Ministerstva vnitra nemá možnost využít externího pověřence a musí pověřencem jmenovat pracovníka ve služebním poměru.

Každý jmenovaný pověřenec musí naplňovat všechny požadavky dle GDPR, kterými jsou v prvé řadě dostatečná odbornost, ale i snadná dosažitelnost, důvěrnost, a neexistence střetu zájmů. GDPR nicméně neklade na pověřence formální nároky konkrétního typu či stupně vzdělání či konkrétní certifikace.

Pokud je pověřencem zaměstnanec školy, může dle GDPR vykonávat i jiné úkoly, ale tyto nesmí zakládat střet zájmů a zároveň musí být zachován dostatečný čas pro plnění povinností pověřence. V rámci hierarchie školních zaměstnanců by měl být pověřenec přímo podřízen vedení školy a na jeho činnost by měly být vyděleny dostačující prostředky. V praxi by se mohlo jednat např. o jednoho z učitelů, který by byl určen jako zástupce ředitele pro oblast ochrany soukromí a zároveň jmenován jako pověřenec pro ochranu osobních údajů.

Ačkoli každá škola musí mít pověřence, je možné, aby vícero škol pověřence sdílelo. Pověřenec však musí mít dostatečný časový prostor na každého správce, proto bude počet škol na jednoho pověřence záviset na velikosti škol, rozsahu zpracovávaných údajů a dalších okolnostech. Zároveň je možné, aby byl pověřenec zajištěn zřizovatelem pro všechny nebo některé jeho školy centrálně. Může být dokonce jmenován celý tým pověřenců, ale vždy je třeba určit jednu konkrétní osobu, která bude odpovědným styčným pracovníkem a také kontaktním bodem jak pro školu, tak pro ÚOOÚ.

Pověřenec je kontaktním místem pro dozorový úřad, tedy ÚOOÚ. Na pověřence se ale mohou obracet i samotné subjekty údajů (zejména žáci, rodiče a učitelé) s dotazy v souvislosti se zpracováním osobních údajů a s uplatňováním svých práv. Pověřenec je také jejich kontaktním místem v případě bezpečnostního incidentu. V neposlední řadě je úlohou pověřence monitorovat činnosti zpracování a jejich soulad s GDPR, včetně podílení se na školení pracovníků školy. Povinností pověřence budou vymezeny buď v náplni pracovní pozice nebo ve smlouvě, kterou s ním škola uzavře.

Samotné jmenování pověřence však školu nezbavuje odpovědnosti za dodržení souladu s požadavky GDPR. Odpovědnou totiž vždy zůstává škola, nikoli jí jmenovaný pověřenec. Případnou škodu, která by škole za nesplnění povinností pověřence vznikla, může škola následně na pověřenci vymáhat. Jeho odpovědnost za škodu však bude zpravidla omezená, ať už zákoníkem práce, pokud se jedná o zaměstnance školy, nebo smluvními ustanoveními, pokud by šlo o externího pověřence.

---

[1] Dle Metodiky MŠMT bude škola či školské zařízení s akreditací dle školského zákona veřejným subjektem, protože může rozhodovat o právech a povinnostech fyzických osob.

[2] Úřad pro ochranu osobních údajů, který je českým dozorovým orgánem v oblasti ochrany osobních údajů.

2. ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Připravte přehledné záznamy o činnostech zpracování a stanovte mechanismus pro jejich pravidelnou aktualizaci.

Účelem záznamů o činnostech zpracování je primárně poskytnout informace ÚOOÚ na základě jeho žádosti či v rámci kontroly. Záznamy zároveň mohou pomoci doložit, že zpracování prováděné školou je v souladu s nároky, které na ně klade GDPR.

Na školy se povinnost vést záznamy zpracování uplatní, protože při výkonu své hlavní činnosti, totiž poskytování vzdělání, škola pravidelně a ve velkém rozsahu zpracovává osobní údaje primárně žáků a zaměstnanců, ale také třetích osob (např. dodavatelů) a dále proto, že škola může zpracovávat i zvláštní kategorie údajů, primárně o zdravotním stavu žáků.

Aby byl zajištěn soulad s GDPR, tyto záznamy musí obsahovat následující rozsah informací:

- Název a kontaktní údaje školy, spolu se jménem a kontaktními údaji pověřence školy.
- Účely zpracování. Většina účelů zpracování, jako je výchova a vzdělání dětí, bude pro školu stanovena v zákoně. Pokud by však škola sledovala další účely, které ze zákona neplynou, jako např. kroužky, e-learning a další vedlejší činnosti, bude třeba tyto další účely také uvést.
- Kategorie subjektů a kategorie osobních údajů. Kategorie osobních údajů mohou být definovány v obecné rovině (např. kontaktní údaje, údaje o klasifikaci, údaje související s výukou, údaje o zákonných zástupcích apod.). Kategoriemi subjektů údajů budou hlavně žáci, zákonní zástupci žáků, zaměstnanci, dodavatelé školy. Podobným způsobem je pak vhodné definovat i kategorie osobních údajů.
- Kategorie příjemců osobních údajů. Pokud škola předává údaje dalším subjektům, je třeba takové příjemce uvést. Tato povinnost se však nevztahuje na orgány veřejné moci, které mohou údaje po škole požadovat např. v souvislosti s trestním stíháním, protože povinnost takového předání plyne pro školu ze zákona. Ostatní příjemce je však škola povinna identifikovat. Budou jimi primárně zpracovatelé, jako jsou IT dodavatelé, externí účetní, auditoři či pojišťovny.

  Další informace by bylo nutné uvést, pokud se údaje předávaly do třetích zemí, tedy mimo Evropský hospodářský prostor. To se bude týkat škol, pokud pro zpracovávání využívají různé IT aplikace, které mohou údaje uchovávat v datových centrech umístěných mimo EU.
- Lhůty pro výmaz jednotlivých údajů, je-li to možné. Většina lhůt pro uchovávání osobních údajů bude pro školu plynout ze zákona či podzákonného předpisu (školský zákon, zákoník práce). Tyto lhůty tak bude třeba uvést s odkazem na daný předpis. Pokud by však údaje byly zpracovávány na jiném základě, například na základě oprávněného zájmu (zejména pro účely ochrany majetku) měla by škola alespoň uvést popis, jak lhůtu stanoví.
- Obecný popis technických a organizačních bezpečnostních opatření na ochranu osobních údajů, je-li to možné. Vzhledem k tomu, že by podrobný seznam konkrétních opatření mohl zabezpečení údajů spíše ohrozit, škola by v záznamech o činnostech zpracování měla pouze uvést obecný popis, jaká opatření provedla a zajistila, např. použití technologie šifrování pro interní i externí komunikaci školy, pseudonymizace uchovávaných údajů, fyzické zabezpečení apod.

Záznamy o činnostech zpracování musí mít písemnou formu, listinnou nebo elektronickou. Elektronická forma může značně zjednodušit jejich aktualizaci. Škola by měla zajistit, že jí vedené záznamy jsou vždy aktuální a že každá změna (např. v IT dodavateli) je do nich řádně zanesena. Jako vhodné řešení se jeví pololetní aktualizace.

3. PRÁVNÍ TITULY

Zajistěte si, že pro zpracování veškerých osobních údajů máte právní titul (zákonná povinnost, smlouva, oprávněný zájem, souhlas, aj.). V případě, že pro zpracování údajů nemáte potřebný titul, smažte je. Souhlas by měl být používán jako právní titul jen zcela výjimečně.

Škola by neměla zpracovávat žádné údaje, které nepotřebuje nebo pro jejichž zpracování nemá náležitý právní titul.

Primárním titulem zpracování bude pro školu plnění zákonné povinnosti, zejména v souvislosti se školským zákonem[3] a jeho prováděcími předpisy, případně pak zákoníkem práce[4] v oblasti zaměstnanecké agendy.

Právním titulem zpracování osobních údajů ve vztazích s dodavateli bude smlouva, kterou s nimi škola uzavřela.

Právním titulem pro zpracování údajů při ochraně majetku a zdraví a bezpečí žáků, např. v rámci kamerových systémů, bude veřejný zájem a oprávněný zájem školy. Veřejný zájem se bude týkat zejména zajištění bezpečnosti žáků a dalších osob v prostorách školy, oprávněný zájem se bude týkat ochrany majetku.

Souhlas se ve školním prostředí uplatní ve velmi malém rozsahu, např. pro využití fotografií žáků a učitelů při propagaci školy či pro zpracování kontaktních údajů bývalých žáků za účelem klubů absolventů. Škola musí mít vždy vhodné řešení pro žáky a učitele, kteří souhlas neudělí a nesmí souhlas nijak vynucovat či požadovat jako podmínku studia či výkonu pracovní pozice. V této souvislosti je zásadní, aby souhlas byl svobodný, určitý, informovaný a jednoznačný. Lze však předpokládat, že souhlas udělený žáky a učiteli nebude ve většině případů zcela svobodný, s ohledem na jejich závislé postavení na škole.

Pro zpracování osobních údajů žáků mladších 18 let bude ve většině případů nutné získat souhlas (nebo schválení souhlasu) zákonného zástupce. Pouze v omezené míře, pro zpracování týkající se např. e-learningových aplikací a dalších služeb informační společnosti, bude možné, aby dítě starší 13 let samo udělilo platný souhlas se zpracováním svých údajů. Tato snížená hranice, která byla stanovena návrhem českého adaptačního zákona, se ve školním prostředí příliš neuplatní.

Nicméně i v případech, kdy bude souhlas udělován zákonným zástupcem, je třeba brát ohled na vůli dítěte. Pokud nastane konflikt mezi vůli dítěte a jeho zákonného zástupce, doporučujeme souhlas považovat za neudělený. Souhlas tak bude účinně udělen, pouze pokud dojde ke shodě.

Dále je třeba stanovit omezenou dobu platnosti souhlasu (k tomu více v bodě 4).

V rámci vnitřní databáze školy je vhodné jednotlivé kategorie osobních údajů spojit s příslušným titulem, na jehož základě jsou zpracovávány. Tak bude pro školu jednodušší přiřadit k těmto kategoriím údajů i správné lhůty pro výmaz, po jejichž uplynutí je škola povinna údaje vymazat.

[3] Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání.
[4] Zákon č. 262/2006 Sb., zákoník práce.

4. DOBY ZPRACOVÁNÍ

Nastavte si správně doby zpracování jednotlivých kategorií osobních údajů, po jejichž uplynutí zajistěte úplný výmaz těchto údajů.

Škola může zpracovávat pouze ty údaje, ke kterým má trvající titul. Jakmile ke zpracovávaným údajům již nebude existovat žádný platný titul, je škola povinna údaje vymazat či anonymizovat a dále již nezpracovávat.

Ve školním prostředí bude primárním titulem plnění zákonné povinnosti, a to zejména na základě školského zákona a zákoníku práce. Školský zákon, podzákonné předpisy[5] a zákon o archivnictví[6] pro jednotlivé povinnosti stanoví mimo jiné také dobu uchování, kterou škola musí respektovat.

Nicméně pro činnosti zpracování, které ze zákona přímo neplynou, není možné automaticky uplatnit stejnou dobu zpracování. Zpracování údajů, které souvisí s vedlejšími činnostmi, např. družina či dobrovolné kroužky, bude zpravidla prováděno na základě smlouvy, která nastavuje podmínky využívání takových služeb (byť je písemná dokumentace většinou omezena na vyplnění přihlášky).

V některých případech může přicházet v úvahu i zpracování údajů na základě souhlasu žáka, případně jeho zákonného zástupce. Doba zpracování je jednou z nutných náležitostí souhlasu. Obecně lze za přijatelnou dobu trvání souhlasu a tedy doby zpracování související se souhlasem považovat období kolem 3-5 let. Souhlasy udělené na dobu přesahující tuto hranici budou pravděpodobně považovány za přílišný zásah do práv žáků.

V oblastech zpracování založeného na plnění smlouvy bude doba zpracování omezena trváním dané smlouvy. Nicméně je možné, aby po ukončení platnosti smlouvy došlo ke změně titulu na oprávněný zájem, kterým je typicky určení či zajištění právních nároků plynoucích ze smlouvy, zejména v rámci promlčecí doby.

V případě kamerových záznamů, jejichž použití by škola zakládala na veřejném nebo oprávněném zájmu, lze předpokládat, že maximální doba zpracování by neměla přesáhnout pouhých několik dní.

Aby bylo pro školu snadné a přehledné doby zpracování dodržovat a po jejich uplynutí údaje vymazat, je vhodné v rámci vnitřní evidence údajů evidovat jednak tituly, na jejichž základě jsou zpracovávány, a jednak jednotlivé doby zpracování.

V souvislosti s následným výmazem údajů je třeba, aby byly údaje opravdu efektivně vymazány nebo anonymizovány. Jejich přesun do koše v počítači povinnost výmazu nenaplní. Oproti tomu je možné výmaz provést např. skartací listinných dokumentů či anonymizací těch elektronických. Povinnost výmazu nelze však vykládat tak, že má škola povinnost vyloučit veškeré možnosti případného obnovení osobních údajů. Pokud obnova údajů vyžaduje nadměrné úsilí, např. použití vysoce specializovaného programu či jiného nástroje, lze předpokládat, že škola svou povinnost údaje vymazat splnila.

5. POŽADAVKY NA IT DODAVATELE

Vyžádejte si od IT dodavatelů prohlášení o souladu jejich systémů s GDPR a uzavřete s nimi zpracovatelskou smlouvu. Vyžádejte si od nich popis bezpečnostních opatření.

Většina dodavatelů softwarového řešení (jako je např. školní informační systém, a další softwarová řešení, která se neprovozují na hardwaru školy a jsou spravována dodavateli těchto

[5] Např. vyhláška č. 364/2005 Sb., o vedení dokumentace škol a školských zařízení a školní matriky a o předávání údajů z dokumentace škol a školských zařízení ze školní matriky, vyhláška č. 223/2005 Sb., o některých dokladech o vzdělání, vyhláška č. 15/2005 Sb., kterou se stanoví náležitosti dlouhodobého záměru a výročních zpráv.
[6] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů.

řešení, dále, online aplikací, „nebalíkového“ software aj.) bude vůči škole v postavení zpracovatele osobních údajů. Těm GDPR ukládá různé povinnosti, mezi které patří povinnost zpracovávat osobní údaje jen v souladu se zpracovatelskou smlouvou a pokyny školy, zavést a dodržovat technická a organizační opatření, poskytovat škole součinnost při plnění jejích povinností dle GDPR a po ukončení obchodního vztahu vymazat či vrátit veškeré zpracovávané údaje škole. Zpracovatel může do zpracovatelského řetězce zapojit další osobu (dalšího zpracovatele) pouze s výslovným souhlasem školy. Zpracovatel není oprávněn nakládat s osobními údaji svévolně a bez vědomí školy.

Zpracovatelská smlouva, kterou je škola povinna s každým zpracovatelem uzavřít, má přesně stanovené náležitosti, a měla by tedy přesně stanovit předmět a účel zpracování (např. poskytování IT řešení), kategorie osobních údajů (jako jsou jméno, příjmení, kontaktní údaje, atd.), kategorie subjektů (žáci, učitelé, atd.), jakož i dobu zpracování a rozdělení povinností správce (školy) a zpracovatele (dodavatele řešení). Jelikož uzavření zpracovatelské smlouvy je povinností školy, je nutné na uzavření zpracovatelské smlouvy trvat. Ve stávajících smluvních vztazích je možné tuto situaci řešit buď uzavřením dodatku, nebo samostatné smlouvy. Pokud by dodavatel IT produktů odmítal zpracovatelskou smlouvu uzavřít, bude tak ve výsledku nutné smluvní vztah ukončit a vybrat jiného dodavatele. Od IT dodavatelů doporučujeme dále vyžádat prohlášení o souladu jejich systémů s GDPR, resp. o jejich dostatečném zabezpečení. Tím bude pro školu jednodušší doložit, že škola samotná, jakožto správce, naplňuje při předání údajů třetím osobám všechny náležitosti týkající se jejich zabezpečení (více k zabezpečení v bodu 7).

Někteří dodavatelé však nemusí být nutně v postavení zpracovatelů. Zpracovatelskou smlouvu není nutné uzavřít s dodavateli tzv. „krabicových produktů“, v rámci kterých je zákazníkovi poskytnuta pouze licence pro užívání aplikace na vlastním hardwaru, nikoli externí úložiště. Důvodem je, že výrobci těchto softwarů nemají žádný přístup k údajům, které software zpracovává, a tak se nemohou dostat do postavení zpracovatelů. Takovými produkty jsou např. Microsoft Windows, Microsoft Office (pokud se však nejedná o služby Office 365 – u těchto služeb jsou otázky ochrany osobních údajů a souladu s GDPR řešeny v rámci licenční smlouvy Microsoft).

V souvislosti se zpracovatelskou smlouvou stanovilo MŠMT ve svém stanovisku z března 2018[7] některé požadavky, které má školou uzavřená zpracovatelská smlouva naplňovat. Níže shrnujeme hlavní doporučení a zároveň na příkladu produktů Microsoft uvádíme, jak tato doporučení mohou být u globálních cloudových služeb naplněna:

(i) MŠMT doporučuje uzavírat smlouvy výslovným souhlasem se všemi dokumenty, které tvoří zpracovatelskou smlouvu. Podmínky pro online služby (Online Service Terms, OST) společnosti Microsoft, které tvoří součást smlouvy o poskytování služeb, naplňují všechny náležitosti zpracovatelské smlouvy dle čl. 28 GDPR. Souhlas s těmito Podmínkami pro online služby vyjadřuje každý zákazník výslovně kliknutím na tlačítko „Souhlasím“ pod textem OST [aktivním zaškrtnutím políčka „Souhlasím“, přičemž je poskytnut celý text OST].

(ii) MŠMT doporučuje sjednat pokud možno příslušnost českých soudů a české právo jako rozhodné právo. V každém případě je však dle MŠMT třeba se vyhnout zejména příslušnosti mimoevropských soudů, což podle názoru MŠMT podstatným způsobem ztěžuje vymahatelnost práv školy. Pro produkty společnosti Microsoft je sjednána příslušnost irských soudů a irské právo, a toto smluvní nastavení tudíž nespadá do kategorie považované MŠMT za podstatně snižující možnost domáhání se práv školy, jakožto správce osobních údajů.

[7] MŠMT: Stručný návod na zabezpečení procesů souvisejících s GDPR ve školách (nástin pracovního postupu).

Nad rámec toho, pokud to bude škola pro dané řešení považovat za nutné, může na související služby a podporu Microsoft produktů uzavřít smlouvu s lokálním partnerem společnosti Microsoft, který jí umožní sjednat příslušnost českých soudů i české právo jako právo rozhodné.

(iii) MŠMT doporučuje uchování osobních údajů v Evropské Unii. V rámci produktů Microsoft jsou údaje všech evropských zákazníků uchovávány v datových centrech na území Evropské Unie, pokud si zákazník sám nezvolí datové centrum v jiném regionu.

6. DOHLED NAD POUŽÍVANÝMI APLIKACEMI

Zajistěte, aby zaměstnanci pro práci s osobními údaji nevyužívali volně dostupné aplikace, které lze stáhnout z internetu a které nebyly pořízeny školou.

Učitelé a jiní pracovníci by zásadně měli využívat jen ty aplikace, které byly pořízeny centrálně pro celou školu a pro které byla školou schválena a uzavřena zpracovatelská smlouva. Učitelé by si neměli stahovat a vkládat do nich osobní údaje žáků do volně dostupných aplikací jako, např. různé z internetu volně dostupné emailové schránky či aplikace na ukládání a úpravu fotografií a správu kalendářů nebo e-learning apod. Vzhledem k tomu, že při stažení těchto aplikací zpravidla není uzavírána žádná zpracovatelská smlouva, není možné zajistit soulad s GDPR a dohled nad zpracovávanými osobními údaji v rámci těchto aplikací. Není zajištěno, že údaje nejsou z těchto aplikací předávány mimo území EHP bez dostatečných záruk nebo že údaje budou po stanovené době vymazány.

Často se také stává, že učitelé používají pro komunikaci s žáky i jejich rodiči své soukromé emailové adresy, které si zřídili přes volně dostupné emailové služby. Takový přístup však není v souladu s GDPR a škola by měla zajistit, že komunikace, ve které se objevují osobní údaje žáků, bude probíhat pouze přes emailové adresy oficiálně zřízené školou.

Při poskytování aplikací pro celou školu na centrální úrovni je možné zajistit odpovědnost výrobce aplikace za odpovídající úroveň zabezpečení i plnění dalších povinnosti dle GDPR. Zároveň takový postup umožní škole kontrolu nad způsobem zpracování osobních údajů v rámci IT systémů a umožní škole také vyřizovat žádosti subjektů údajů.

7. ZABEZPEČENÍ ÚDAJŮ

Zkontrolujte zabezpečení systémů a koncových zařízení zajistěte, že přístupová práva k osobním údajům mají jen oprávněné osoby.

GDPR v článku 32 ukládá povinnost škole zajistit odpovídající úroveň zabezpečení údajů, aby se předešlo ohrožení důvěrnosti, dostupnosti či integrity osobních údajů.

Při zajišťování zabezpečení osobních údajů a systémů, ve kterých jsou zpracovávány, je třeba zohlednit charakter a povahu údajů, protože některé kategorie osobních údajů lze zpracovávat jen se zvýšenou úrovní ochrany. Ve školním prostřední budou těmito zvláštními druhy údajů primárně údaje o zdravotním stavu dětí a zaměstnanců školy. Z důvodu rozsáhlého zpracovávání těchto kategorií údajů, zejména v rámci informačních systémů školy, se na většinu škol uplatní i povinnost provést posouzení vlivu na ochranu osobních údajů (tzv. DPIA).

Pro zajištění adekvátní úrovně zabezpečení ve školním prostředí jsou zásadní následující body:

- vhodná volba používaných aplikací a jejich zajištění na centrální úrovni pro celou školu (k tomu viz bod 6),
- zavedení vhodného firewallu a tedy ochrana vnitřní sítě,
- zabezpečení koncových zařízení, ze kterých lze k osobním údajům přistupovat, a
- kontrola a správa přístupových práv.

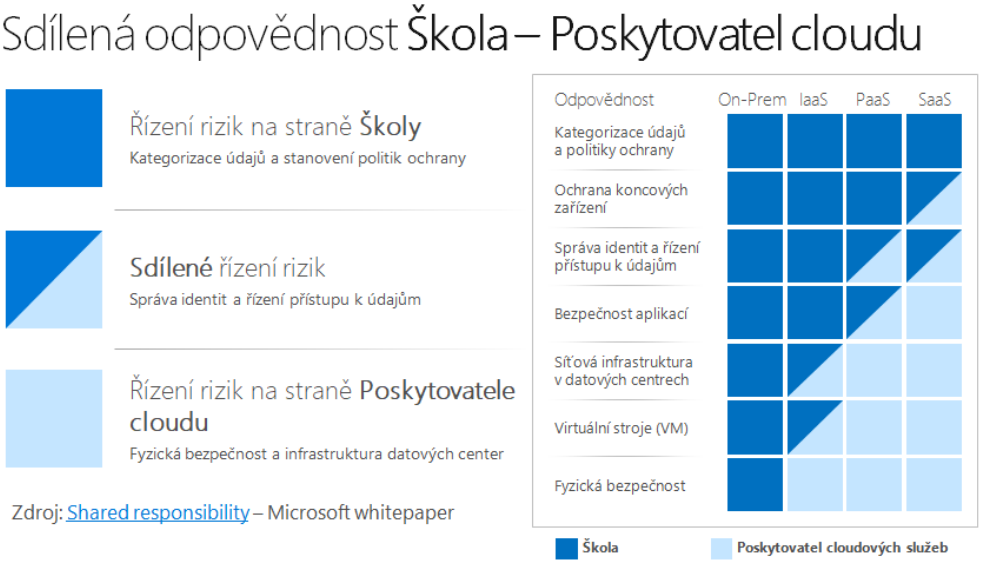
Škola by měla vždy ověřit, které osoby a za jakých okolností mají přístup k osobním údajům. Jiné požadavky budou kladené na zabezpečení osobních údajů v listinné podobě (kde bude potřeba zajistit především fyzické zabezpečení formou např. uzamykatelné kartotéky) a jiné na údaje v elektronické podobě. U elektronicky uchovávaných údajů je nezbytné se zaměřit na nastavení systému evidence přístupů (logů) a přístupových hesel, které zajistí, že osobní údaje uchovávané v databázích nejsou zpřístupněny ani do nich není zasahováno neoprávněnou osobou.

Konkrétní zvolená opatření by měla sledovat aktuální vývoj moderních technologií tak, aby vždy poskytovala maximální úroveň zabezpečení za daných okolností. Mezi doporučovaná opatření patří rovněž šifrování, případně pak tzv. pseudonymizace údajů.

Část odpovědnosti za zabezpečení může škola přenést na zpracovatele volbou vhodného IT řešení (např. přenesením údajů do cloudu neboli vzdáleného úložiště spravovaného a zabezpečovaného IT dodavatelem), prostřednictvím kterého škola splní požadavky na zabezpečení systémů. Pro školu bude následně jednodušší dokládat soulad s požadavky GDPR (prostřednictvím zpracovatelské smlouvy a vhodných záruk ze strany zpracovatele) a zároveň tím sníží celkové riziko z porušení zabezpečení. Tím, že je škole a jejím zaměstnancům zajištěn dálkový přístup je zároveň zajištěna neustálá dostupnost těchto údajů.

Jestliže učitelům či žákům škola umožňuje při výuce využívat vlastní zařízení, je třeba zajistit, že přístup do sítě, školní emailové schránky a dalších databází bude umožněn jen na základě vhodných přístupových oprávnění a osobní údaje tak nebudou zbytečně vystavené zbytečnému riziku. Škola by rovněž měla dbát na celkové zabezpečení těchto zařízení (včetně zavedení vhodných softwarových nástrojů). Aby škola zajistila, že v případě ztráty soukromého telefonu či jiného zařízení zaměstnance používaného pro pracovní účely nedojde k porušení bezpečnosti dat a neuplatní se povinnost hlášení takového incidentu (k tomu více v bodě 8), je třeba, aby v pracovní smlouvě nebo vnitřním předpise byla stanovena přesná pravidla pro užívání tohoto zařízení pro pracovní účely. Tato pravidla musí obsahovat zejména technická opatření, která efektivně pomohou předejít rizikům ohrožení či porušení práv a svobod fyzických osob. Je tak třeba zaměstnance zavázat, aby své zařízení opatřil přístupovými kódy a hesly, tak aby ho nemohl odemknout kdokoli (vhodným řešením může být odemknutí otiskem prstu). Dále je také nutné přístup do pracovní emailové schránky podmínit přístupovými údaji a zároveň nařídit oddělení pracovní komunikace (včetně komunikace s rodiči a žáky) od komunikace soukromé. Zároveň je třeba zajistit, aby údaje v soukromém zařízení zaměstnance nebyly jedinou kopií – škola musí mít vždy odpovídající zálohu. Zejména pro tyto účely je vhodným postupem využívání vzdálených úložišť, neboť je tak zajištěna aktualizace i dostupnost údajů.

Ukládání údajů v cloudu se dnes již považuje za standard a cloud se tak nabízí jako jedno z možných řešení, jak rovněž částečně snižovat rizika spojená se zabezpečením infrastruktury. V případě využití cloudu se nabízejí různé varianty řešení, přičemž každá z nich znamená různou míru přenesení odpovědnosti na poskytovatele cloudu – a tedy tím snížení rizik pro školu.



V závislosti na zvoleném řešení a konkrétních poskytovaných službách může poskytovatel celého IT řešení – tedy i poskytovatel cloudu – škole dále pomoci vhodným nastavením jednotlivých systémů a jejich funkcionalit s výkonem práv subjektů údajů (zejména žáků a učitelů), jakou jsou práva na přístup, omezení, přenositelnost či výmaz. Při zajišťování zabezpečení může poskytovatel cloudu převzít odpovědnost za správu záložních kopií, testování a audity účinnosti zavedených opatření. Prostřednictvím IT řešení je dále možné zajistit pseudonymizaci a šifrování údajů a jednodušší šetření a hlášení bezpečnostních incidentů. Nicméně je třeba mít na paměti, že zpracovatel může vždy odpovídat jen za splnění požadavků, které GDPR klade na zpracovatele. Ačkoliv tak využití vhodného IT řešení (včetně cloudového) může škole značně usnadnit plnění jejích povinností, není všespasitelné, jak se často snaží někteří IT dodavatelé tvrdit, a hlavní odpovědnost za splnění všech požadavků při ochraně osobních údajů vždy zůstane na škole, jakožto správci těchto údajů.

8. ÚNIK DAT

Nastavte vhodný vnitřní proces monitorování zabezpečení osobních údajů a stanovte postup hlášení úniku dat.

Únik dat, přesněji porušení zabezpečení osobních údajů, nastane, jestliže dojde k náhodnému nebo protiprávnímu zničení, ztrátě, pozměnění nebo neoprávněnému přístupu předávaných, uložených nebo jinak zpracovávaných osobních údajů. Porušení zabezpečení spočívá buď v porušení důvěrnosti dat, v porušení jejich dostupnosti nebo v porušení jejich integrity. Porušení bezpečnosti osobních údajů tak může spočívat také v (dočasném) porušení jejich dostupnosti.

V první řadě je třeba zajistit naplnění všech technických a organizačních opatření dle čl. 32 GDPR, kterými by měla být zajištěna adekvátní úroveň zabezpečení. Jestliže i přes všechna tato opatření nastane situace bezpečnostního incidentu, GDPR ukládá správci, tedy škole, povinnost do 72 h nahlásit porušení zabezpečení ÚOOÚ a osobám, jejichž údaje byly ohroženy. V rámci tohoto hlášení musí škola informovat ÚOOÚ, jakých kategorií údajů a osob se porušení týká, jaké jsou pravděpodobné důsledky, jakým způsobem bude škola situaci řešit a v neposlední řadě poskytne kontaktní údaje na pověřence pro ochranu osobních údajů či jiné místo, kde lze získat více informací. Proto, aby se tato povinnost uplatnila, není nutné, aby škola disponovala veškerými informacemi o incidentu, a mohla tak s určitostí říci, že k incidentu skutečně došlo. Pokud bude mít informace, např. na základě vlastního monitorovacího systému, o tom, že k incidentu došlo, a zároveň nebude zjevné, že tyto informace jsou nepravdivé, bude mít povinnost porušení zabezpečení nahlásit.

Škola však tuto povinnost mít nebude, pokud může doložit, že porušení zabezpečení nevede k riziku ohrožení nebo porušení práv a svobod fyzických osob. Jeden ze způsobů, jak tomu lze předejít, je použití technologií účinného šifrování. Jestliže šifrovací klíč zůstane po úniku dat v moci školy, který má zároveň k dispozici odpovídající zálohu dat, která byla kompromitována, pak lze předpokládat, že riziko ohrožení nebo porušení práv fyzických osob je minimální, a škola nebude mít povinnost incident hlásit ÚOOÚ.

V případech, kdy porušení zabezpečení znamená dokonce vysoké riziko pro práva a svobody subjektů údajů, bude mít škola povinnost informovat i je, a to např. formou vnitřního oznámení. V tomto oznámení musí škola kromě popisu povahy porušení, pravděpodobných důsledků a následných opatření uvést také kontaktní údaje na pověřence pro ochranu osobních údajů nebo jiného kontaktního místa pro bližší informace, pokud pověřenec není jmenován.

Kromě ohlášení má škola také povinnost každé porušení zabezpečení řádně dokumentovat, včetně případů, kdy dle názoru školy není pravděpodobné, že by takové porušení mělo za následek ohrožení či porušení práv nebo svobod osob, jako je např. dočasná nedostupnost systémů. V rámci této dokumentace by škola měla uvádět popis porušení, jeho dopad a přijatá nápravná opatření.

Pro předcházení porušením zabezpečení je dále vhodné pravidelně testovat vnitřní systémy a školit zaměstnance školy. Je třeba vhodným způsobem, nejlépe formou vnitřního předpisu, nastavit vnitřní postup pro případ, že by k porušení zabezpečení došlo, aby byl co nejdříve informován ředitel školy. Následně je před samotným hlášením ÚOOÚ možné provést rychlé šetření pro ujištění, zda k porušení opravdu došlo a pokud ano, zda bude mít za následek riziko ohrožení nebo porušení práv osob.

9. VÝKON PRÁV SUBJEKTŮ

Zajistěte, aby subjekty (např. žáci a jejich zákonní zástupci nebo učitelé) údajů mohly uplatnit právo na přístup a další práva. Nastavte efektivní vnitřní postup vyřizování jejich žádostí.

Subjektu údajů, tedy zejména žákům, jejich zákonným zástupcům a učitelům, musí být umožněno, aby bez obtíží mohli podat žádosti u uplatnění svých práv dle GDPR. Mezi tato práva patří právo na informace, právo na přístup k osobním údajům, právo na opravu a výmaz a omezení zpracování, právo na přenositelnost a právo podat námitky.

Ve školním prostředí se primárně uplatní právo na přístup a informace a právo na opravu. Způsob podávání žádostí nesmí představovat administrativní ani jinou zátěž pro žadatele, a pokud je to možné, měl by jim být umožněn výběr z několika možných způsobů podání žádosti.

Škola je nicméně oprávněna provést ověření totožnosti osoby, která žádost podává, jelikož v případě poskytnutí přístupu neoprávněné osobě může dojít k ohrožení či porušení práv např. žáka. Za tímto účelem si může škola vyžádat další, dodatečné údaje. Může však požadovat jen nezbytně nutný rozsah údajů, které mu umožní ověřit totožnost fyzické osoby, V určitých případech bude škola moci požadovat např. doklad totožnosti či ověřený podpis žádosti.

Škola by měla vést přehlednou vnitřní evidenci žádostí a způsobu jejich vyřízení.

Dle GDPR by škola měla žádost vyřídit do 1 měsíce a informovat jej o výsledku. Tato lhůta však může být v složitých případech prodloužena až o 2 další měsíce, o čemž musí být žadatel rovněž informován. Škola není povinna žádosti vyhovět, jestliže není objektivně možné žadatele identifikovat. To se může například stát, pokud žadatel odmítne poskytnout další údaje nutné k ověření jeho totožnosti.

10. ZÁSADY ZPRACOVÁNÍ

Připravte transparentní zásady ochrany osobních údajů pro zaměstnance (např. formou vnitřního předpisu) a zajistěte, že budou se zásadami seznámeni.

Role zaměstnanců v institucionálním rámci ochrany osobních údajů je dvojí: v prvé řadě jsou zaměstnanci sami subjekty údajů a škola či školské zařízení je správcem jejich osobních údajů, neméně důležité je však zapojení zaměstnanců ve zpracovatelských činnostech školy ve vztahu k dalším subjektům (zejména žákům a jejich zákonným zástupcům). Je tedy třeba splnit vůči zaměstnancům všechny povinnosti, které má škola vůči nim jako subjektům údajů, a zároveň zajistit, aby se zaměstnanci, kteří se podílejí na zpracování osobních údajů školou, řídili pravidly stanovenými školou.

Zaměstnanec jako subjekt údajů

V rámci zásady transparentnosti má škola povinnost informovat osobu nejpozději v okamžiku získání jejích údajů o náležitostech zpracování dle článku 13 GDPR. Tyto informace mají být poskytnuty stručným, snadno přístupným a srozumitelným způsobem, jednoduchým a jasným jazykem a bezplatně. Tato povinnost není vázána na žádost a škola je povinna ji plnit i bez žádosti.

Ve školním prostředí bude nejvhodnější způsobem plnění informační povinnosti vůči zaměstnancům vydání vnitřního předpisu, který bude obsahovat zásady ochrany osobních údajů a se kterým se zaměstnanci budou moci seznámit již při uzavření pracovní smlouvy, ale zároveň pro ně bude kdykoli snadno dostupný po celou dobu trvání pracovního poměru se školou. Zásady nemusí mít jen listinnou podobu, ale mohou být také přístupné v elektronické podobě. Je nutné, aby byl vnitřní předpis vždy v souladu s pravidly pro vydávání vnitřních předpisů zaměstnavatele dle § 305 zákoníku práce.

Pro splnění informační povinnosti musí škola v interním předpisu nebo jiném dokumentu uvést alespoň následující rozsah informací:

- Název a kontaktní údaje jak správce (školy), tak pověřence pro ochranu osobních údajů.
- Příjemce či kategorie příjemců osobních údajů (v této souvislosti by škola měla mít přehled i o tom, pokud tito příjemci mohou údaje dále předávat dalším příjemcům, a to na základě jakého účelu a titulu). Pokud by snad údaje byly předávány do třetích zemí (tedy mimo Evropský hospodářský prostor), je třeba uvést další informace o těchto příjemcích, zejména na jakém základě jsou údaje do třetích zemí předávány (např. rozhodnutí Komise o odpovídající ochraně osobních údajů).
- Účel zpracování neboli důvod, pro který škola údaje potřebuje, jaký cíl tím sleduje. Ve školním prostředí bude většina účelů souviset s poskytováním vzdělání, ale pokud jsou údaje zpracovávány i za jinými účely, které s poskytování vzdělání přímo nesouvisí, je třeba je uvést a popsat odděleně a dostatečně určitě. Pokud by se v průběhu zpracování účel změnil, je škola povinna osoby informovat, a to ještě před počátkem zpracování na základě nového účelu a pouze za podmínky, že se jedná o slučitelné účely. Kdyby nový účel nebyl slučitelný s tím původním, jednalo by se o zcela nové zpracování, které by vyžadovalo samostatný titul.
- Titul zpracování nebo legitimní odůvodnění, proč je zpracování údajů potřebné. Primárním titulem pro školy bude plnění zákonné povinnosti – ve vztahu k zaměstnancům tyto povinnosti stanoví zejména zákoník práce – a plnění smlouvy, tedy pracovní smlouvy. Za určitých okolností se ve vztahu k zaměstnancům může uplatnit i oprávněný zájem školy, zejména v oblasti monitorování sítě, případně užití kamerového systému. V této souvislosti je třeba dbát na to, aby zvolený prostředek monitorování představoval co nejmenší zásah do soukromí a práv zaměstnanců. Vzhledem k monitorování počítačové sítě lze doporučit založit zvolené techniky spíše na blokaci a zabránění přístupu k vybranému obsahu, než na detekci a soustavném monitorování chování zaměstnance na síti. Zároveň je třeba zdůraznit, že žádný účel spojený s monitorováním není možné založit na souhlasu zaměstnanců, a to zejména z toho důvodu, že dle výkladové praxe souhlas

v pracovněprávních vztazích nemusí být zcela svobodný, a proto by jakékoli zpracování dat zaměstnanců mělo být založeno na jiném titulu.

- Dalším údajem, který by měl být v zásadách zpracování uveden, je doba zpracování. Jak je rozvedeno v bodě 4, škola by měla nejprve správně nastavit doby zpracování pro jednotlivé kategorie osobních údajů. Pro některé kategorie doba zpracování vyplyne přímo z titulu, na jehož základě jsou zpracovávány – právní předpis, smlouva. Pro údaje podléhající jiným titulům však bude škola muset dobu zpracování stanovit samostatně, dle vlastního uvážení tak, aby bylo dosaženo vytyčeného účelu a zároveň se zabránilo nadměrnému zásahu do práv a svobod osob.
- V neposlední řadě musí škola své zaměstnance řádně informovat o veškerých jejich právech souvisejících s ochranou jejich osobních údajů. Mezi tato práva patří jak právo na přístup, na informace, na opravu apod., tak možnost podat stížnost u ÚOOÚ.

Takto sestavené zásady zpracování je třeba průběžně aktualizovat a o každé změně zaměstnance předem informovat, aby měli čas se se změnou seznámit a případně uplatnit některá ze svých práv. Pro účely informování o změně nebude stačit, pokud budou nové zásady pouze vyvěšeny na nástěnce školy či na jejích internetových stránkách. Škola je povinna zaměstnance na tyto změny přímo upozornit a nikoli očekávat, že budou zásady pravidelně kontrolovat. I kdyby v delším časovém úseku k žádné změně zásad nedošlo, pro naplnění informační povinnosti lze doporučit zaměstnancům existenci a obsah zásad pravidelně při vhodné příležitosti připomenout.

Zaměstnanec jako osoba, která se podílí na zpracování osobních údajů

Lze doporučit, aby interní předpis v separátní části stanovil alespoň základní rozsah povinností zaměstnanců, kteří při plnění pracovních úkolů přijdou do styku s osobními údaji. Tyto povinnosti se budou zpravidla týkat zejména mlčenlivosti, zabezpečení osobních údajů, postupu v případě porušení zabezpečení osobních údajů. Následně by škola měla zajistit pravidelná školení svých zaměstnanců, která jednak zajistí, že jsou zaměstnanci informováni o zpracování svých osobních údajů a jednak zajistí, že při zpracování údajů žáků a dalších osob budou dodržovány nastavené zásady zpracování.

Informační povinnost vůči dalším subjektům

Pro úplnost je třeba uvést, že stejnou informační povinnost, jako jsme popsali výše ve vztahu k zaměstnancům, musí škola splnit i vůči ostatním subjektům, zejména žákům a jejich zákonným zástupcům. Jako nejvhodnější řešení se jeví zhotovení samostatných zásad zpracování, jejichž předmětem bude informování žáků a rodičů. Tyto zásady by mohly být zveřejněné na webových stránkách školy a jejich aktualizace by dotčeným osobám mohla být oznamována prostřednictvím emailu či např. při konání třídních schůzek.

PIERSTONE

Otázky & Odpovědi

ROZSAH ZPRACOVÁNÍ

1. **Jak poznáme, že naše škola zpracovává osobní údaje? Je škola vždy v postavení správce osobních údajů?**

   Ve vztahu ke školní agendě bude škola primárně v postavení správce osobních údajů. Důvodem je, že škola určuje účely a prostředky zpracování, což je definičním znakem správce. Nemění na tom nic fakt, že škola může být v tomto stanovení určitým způsobem omezena, zejména např. zákonem, který může účely a prostředky buď omezit, nebo přímo stanovit. Typicky se bude jednat o povinnosti školy plynoucí ze školského zákona, které spočívají v nakládání s osobními údaji nebo jej zahrnují, např. vedení evidence žáků, třídní knihy, knihy úrazů či katalogových listů.

2. **Jak škola pozná, která data považovat za osobní údaje?**

   Některé údaje jsou zjevně údaji osobními, např. jméno, příjmení, rodné číslo, adresa, telefonní číslo či emailová adresa žáka nebo jeho rodiče. Osobními údaji jsou ale také např. lokalizační údaje, IP adresa nebo údaje o zaměstnání rodičů. U dalších údajů je pak nutné zkoumat, zda naplňují v konkrétních případech definici osobních údajů, tj. zjednodušeně, zda mohou vést k identifikaci fyzické osoby. Pro školu tak budou osobními údaji i čísla skříněk či výsledky testů a soutěží.

   Jednoduchým doporučovaným testem pro určení, zda se jedná o osobní údaj, je zadání informace do internetového vyhledávače. Pokud je internetový vyhledávač schopen informaci přiřadit ke konkrétní fyzické osobě, bude se jednat o osobní údaj. Jak je však uvedeno výše, ne u všech údajů bude určení tak jednoduché. Je proto vždy třeba brát ohled na konkrétní okolnosti.

3. **Pokud škola obdrží email ze strany subjektu údajů s hlavičkou/patičkou obsahující další osobní údaje (např. telefonní číslo), může škola takto poskytnutý email a další údaje dále volně využívat?**

   V první řadě je vždy třeba dodržet princip minimalizace, a nezpracovávat tak údaje, které škola přímo nepotřebuje k dosažení vytyčeného účelu. Dále je možné provádět jen taková zpracování, která budou založena na řádném právním titulu. Pokud jsou osobní údaje škole poskytnuty pro splnění zákonné povinnosti a jsou pro toto splnění nezbytně nutné, bude možné je uchovávat. Tak tomu bude například, pokud škola v emailu obdrží kromě emailové adresy ještě telefonní číslo zákonného zástupce žáka a bude ho uchovávat za účelem kontaktování zákonného zástupce v zákonem vymezených případech – např. pokud jeho dítě utrpí úraz.

   Pokud však bude škola chtít takové údaje zpracovat způsobem, který s účelem ani právním titulem nesouvisí, nebude takové zpracování bez dalšího možné. Konkrétně bude tedy v první řadě záležet na slučitelnosti účelu, za kterým byly osobní údaje poskytnuty, a účelu, za jakým si škola přeje údaje zpracovávat. Dále bude zpracování záviset na tom, jestli i pro tento nový účel existuje trvající právní titul. Z toho plyne, že pokud škola bude chtít údaje zpracovávat z jiného důvodu, než ke splnění zákonné povinnosti či v případě dodavatelů ke splnění smlouvy, bude ve většině případů nutné získat souhlas. Situace, na které se okrajově uplatní i jiné tituly dle GDPR jsme rozvedli ve 3. bodě Desatera.

   Takto získané osobní údaje zejména zákonných zástupců či přímo žáků tak v praxi nebude možné využívat pro reprezentaci školy, informace o akcích či další marketingové účely, neboť naplnění těchto účelů není stanoveno žádným zákonným předpisem a není možné uplatnit žádný jiný titul.

Tam, kde pro zpracování nadbytečných údajů neexistuje jasný právní základ, bude vhodné takové osobní údaje odmítnout a dále nezpracovávat.

4. **Může škola vytvářet a udržovat vnitřní databázi kontaktů (rodičů žáků, svých dodavatelů)?**

   Škola může uchovávat ty údaje, které nezbytně potřebuje pro splnění vytyčeného účelu a jejichž zpracování může odůvodnit trvajícím právním titulem. Ve školním prostředí bude primárním titulem plnění zákonné povinnosti, která spočívá nebo souvisí se zpracováním osobních údajů. Škola má povinnost vést evidenci kontaktních údajů zákonných zástupců žáků dle školského zákona.

   Zpracování údajů dodavatelů formou vnitřních databází školy je možné založit na právním titulu, kterým je plnění smlouvy s dodavatelem. Je třeba však brát v potaz, že se toto pravidlo netýká všech dodavatelů školy obecně, ale pouze (i) těch, kteří jsou fyzickými osobami, nebo (ii) fyzických osob, které dodavatele, jenž je právnickou osobou, zastupují.

   Pokud škola takovou databázi vytvoří, je povinna ji odpovídajícím způsobem zabezpečit, aby byla zajištěna maximální ochrana osobních údajů v ní obsažených. Listinnou formu je možné zabezpečit např. uzamykatelnými skříňkami a umístěním v místnostech, ke kterým bude mít přístup jen velmi omezený a předem daný okruh osob. Zabezpečení elektronické databáze bude záviset na tom, zda jsou data uchovávána na školních serverech v prostorách školy, či zda jsou využívána vzdálená úložiště vybraného cloudového řešení, jejichž poskytovatelé mohou často nabídnout efektivnější zajištění ochrany a zabezpečení s nižšími náklady.

5. **Jak má škola ošetřit situaci, kdy jsou údaje žáků předávané třetím stranám – společnostem, kde se studenti účastní odborné praxe?**

   Pokud je absolvování praxe součástí studijního programu, tedy zákonným požadavkem, nebude nutné pro předání osobních údajů společnostem, u kterých je praxe vykonávána, získat souhlasy žáků, případně jejich zákonných zástupců. V opačném případě, tedy pokud je odborná praxe zcela dobrovolnou záležitostí, možností, ke které se studenti přihlásí, bude nutné zajistit jejich souhlasy.

   Samotné předání osobních údajů mezi jedním správcem (školou) a druhým správcem (subjektem, u kterého je praxe konána), bude upraveno v rámci jejich smluvních vztahů. Každý správce přitom bude určovat vlastní účely i prostředky zpracování a bude mít samostatnou odpovědnost za soulad s GDPR. Také žáci budou svá práva uplatňovat ke každému ze správců samostatně. Subjekty poskytující praxi pak budou muset zvážit a vyhodnotit, zda ke zpracování osobních údajů mají trvající právní tituly a případně zajistit souhlasy pro ta zpracování, která pod trvající titul již nelze podřadit.

   Pro úplnost dodáváme, že další povinnosti se mohou uplatnit, pokud budou praxe vykonávány ve třetích státech, tedy mimo Evropský hospodářský prostor, kdy bude zejména třeba doložit dostatečné záruky pro takové předání osobních údajů.

ORGANIZAČNÍ OTÁZKY

6. **Uplatní se nějaké povinnosti v souvislosti se stanovením názvů uživatelských účtů emailů a dalších přístupových údajů?**

   Specifická pravidla pro stanovení názvů uživatelských účtů stanovena nejsou. Je však třeba brát v potaz, že ať už zní název účtu jakkoli, pro školu se vždy bude jednat o osobní údaj, neboť bude schopna jej přiřadit ke konkrétní fyzické osobě. Primárně bude třeba zajistit naplnění technických a organizačních opatření zabezpečení, zejména zvážit, zda stanovené názvy účtu

a přístupové údaje odpovídají bezpečnostním standardům. Určitou roli může hrát zejména fakt, že ačkoli pro školu bude název uživatelského účtu osobním údajem vždy, pro třetí osoby nemusí být vždy možné pomocí tohoto údaje konkrétní fyzickou osobu identifikovat. Z toho důvodu lze doporučit nestanovit uživatelské názvy ve znění celého jména studenta.

7. Jak často je třeba kontrolovat soulad s GDPR?

Zajištění souladu s GDPR je kontinuálním procesem, který by však neměl být starostí učitelů a dalších pracovníků školy, jejichž primární náplní práce není kontrola procesů zpracování, pouze se činností zpracování účastní v rámci výkonu povolání. K tomuto účelu slouží zejména pozice pověřence pro ochranu osobních údajů, jehož jmenování bude pro školu povinné. Vzhledem k tomu, jak jsou formulovány úkoly pověřence v článku 39 GDPR, zejména v souvislosti s monitorováním souladu, lze usoudit, že kontinuální zajištění souladu a návrhy případných změn v procesech zpracování jsou hlavní úlohou pověřence. Více ke jmenování pověřence a jeho postavení ve školním prostředí lze nalézt v 1. bodě Desatera.

8. Kdo je odpovědnou osobou za soulad s GDPR v rámci školy?

Odpovědnou osobou za soulad s GDPR bude vždy navenek ve vztahu k dozorovým úřadům škola. Ředitel školy, který je dle školského zákona osobou odpovědnou za vnitřní chod školy, bude primárně tím, kdo bude interně zajišťovat, že jsou povinnosti dle GDPR dodržovány, primárně prostřednictvím jmenování pověřence pro ochranu osobních údajů a uložením odpovídajících úkolů. Lze dovodit, že zřizovatel školy nemá v této souvislosti žádné přímé povinnosti, neboť správcem osobních údajů zůstává škola. Vyplývá to i z ustanovení GDPR a Metodiky MŠMT, dle kterých má povinnost zřídit pozici pověřence pro ochranu osobních údajů každá škola a školské zařízení, nikoli jejich zřizovatel.

V případě vzniku škody z důvodu pochybení jmenovaného pověřence není možné dovozovat jeho přímou odpovědnost za uloženou pokutu či další důsledky. Škola může vzniklou škodu po pověřenci zpětně vymáhat, jeho odpovědnost však bude vždy omezená v závislosti na druhu vztahu (pracovněprávními předpisy, pokud je zaměstnancem, případně ustanoveními smlouvy o poskytování služeb, pokud je externím spolupracovníkem).

ŠKOLENÍ ZAMĚSTNANCŮ

9. O čem je potřeba školit učitele a další zaměstnance? Jaké dokumenty mají podepsat, aby bylo prokázané jejich dostatečné proškolení?

Všechny stávající i nové zaměstnance, kteří pracují s osobními údaji, je zejména třeba proškolit o konkrétních postupech a pravidlech pro práci s osobními údaji žáků, případně dalších osob tak, aby byla zajištěna jejich dostatečná ochrana. Jak je více rozvedeno v 10. bodě Desatera, konkrétně je třeba je seznámit např. s nastavenými dobami zpracování, o náležitostech pro předání dalším osobám, o tom, jak mají pověření zaměstnanci postupovat při vyřizování žádostí apod. Dále doporučujeme v tomto vnitřním předpisu zakázat zasílání osobních údajů prostřednictvím SMS zpráv a minimalizovat jejich zasílání emailem, případně pouze jako zabezpečenou komunikaci, ke které je umožněn přístup jen konkrétnímu příjemci či příjemcům.

Pro zajištění maximální úrovně ochrany je vhodné omezit práci s listinnými dokumenty a ve vnitřním předpisu přesně stanovit povinnost zaměstnanců ve vztahu k dokumentům elektronickým, zejména povinnost ukládat data pouze na jedno konkrétní a předem pojmenované úložiště dat, které bude dostatečně zabezpečeno. Toto úložiště může být fyzicky umístěno v prostorech školy, která pak musí zajistit implementaci a pravidelnou aktualizaci bezpečnostních opatření, nebo může být poskytováno dálkově poskytovatelem cloudových služeb, který pak odpovídá za jeho zabezpečení.

S vnitřním předpisem stanovujícím výše uvedené povinnosti je nutné seznámit všechny stávající i nové zaměstnance, ale zároveň zajistit jeho neustálou dostupnost pro budoucí nahlížení, ideálně např. formou dálkového přístupu na školním intranetu. Zároveň je třeba zaměstnance informovat o každé nové aktualizaci tohoto dokumentu, případně je průběžně seznamovat s významnějšími novinkami formou „udržovacích“ školení. Je také třeba uvědomit zaměstnance o možnosti konzultace se školním IT specialistou či s pověřencem pro ochranu osobních údajů, kterého škola jmenovala.

Potvrzení, že zaměstnanec byl skutečně s obsahem vnitřního předpisu a dalších souvisejících dokumentů seznámen a bere je na vědomí, je vhodné doložit např. prohlášením zaměstnance či obdobným dokumentem, který budou zaměstnanci podepisovat při nástupu do zaměstnání. Stávající zaměstnanci mohou takový dokument podepsat dodatečně.

ZVEŘEJŇOVÁNÍ FOTOGRAFIÍ A JINÝCH ÚDAJŮ

10. Jsou nějaká pravidla, jaké údaje má škola zveřejňovat na úřední desce?

Škola bude muset zveřejnit osobní údaje v tom rozsahu, v jakém to předepisuje zákon. Na tomto místě nelze obsáhnout všechny situace, kdy zákon ukládá škole zveřejnit informace, jejichž součástí jsou i osobní údaje. Pokud se však taková povinnost na školu uplatní, přesto je třeba zachovat náležitosti dle GDPR, zejména princip minimalizace rozsahu údajů. Je tedy nutné zhodnotit, jaké údaje jsou opravdu nezbytné pro naplnění daného účelu. Pokud např. bude účelem identifikovat ředitele školy, bude jistě v pořádku zveřejnit celé jméno ředitele, případně s pracovními kontaktními údaji. Datum narození ale již k naplnění účelu nutné nebude. Obdobně je třeba uvažovat i při zveřejnění údajů týkajících se učitelů – např. pracovní kontaktní údaje třídních učitelů lze považovat za neodporující ustanovením GDPR.

Specifická je situace doručování veřejnou vyhláškou. Správní řád výslovně neumožňuje zveřejňované údaje anonymizovat (začernit, zalepit), z toho důvodu se jako nejvhodnější řešení jeví zveřejnění oznámení o možnosti převzít doručovanou písemnost u ředitele školy (či na jiném určeném místě).

Pokud by škola chtěla na úřední desce či na jiném místě zveřejňovat další údaje, jejichž zveřejnění jí přímo neukládá žádný právní předpis, je nad rámec výše uvedeného třeba zajistit, že pro takové zveřejnění, které je rovněž zpracováním, existuje trvající právní titul. Případně by bylo nutné zajistit souhlas dotčených osob, jestliže by žádný jiný titul nebylo možné uplatnit.

11. Jak má škola postupovat, pokud chce zveřejňovat osobní údaje za účelem poskytnutí informací o akcích organizovaných školou atp.?

Primárně může škola tyto informace uveřejnit na svých webových stránkách nebo poskytnout např. rodičům přímo na třídních schůzkách. Pokud by však škola chtěla informovat žáky, jejich rodiče, případně další osoby prostřednictvím emailu, je nutné, aby pro takové sdělení měla souhlas dotčených osob. Pakliže má škola ve své vnitřní evidenci emailové adresy žáků a dalších osob, je tomu tak většinou za účelem plnění zákonné povinnosti. Tento účel je v zákonných předpisech přesně vymezen a není možné jej dále rozšířit. Z toho důvodu je třeba nový účel, kterým je zasílání informačních emailů, novinek a další marketingové praktiky, založit na jiném právním titulu zpracování. Souhlas může škola získat např. právě na třídních schůzkách.

Souhlas musí splňovat náležitosti dle GDPR, zejména musí být svobodný, určitý, informovaný a jednoznačný (k tomu více ve 3. bodě Desatera) a musí být udělen pouze na omezenou, předem určenou dobu. Nicméně i když bude souhlas udělen, povinnosti školy tím nekončí. V každém emailu, který je informačním nebo marketingovým sdělením, je třeba příjemci sdělení umožnit tento souhlas do budoucna odvolat. Pro tyto účely je vhodným řešením uvést tuto informaci a např. odkaz na příslušnou webovou stránku v patičce takového emailu. Je však třeba mít na paměti, že odvolání souhlasu musí být zásadně stejně jednoduché/složité, jako bylo jeho udělení. Proto není vhodné s odvoláním souhlasu spojovat další formuláře či dotazníky.

12. Může škola zveřejňovat kontaktní osobní údaje učitelů? A členů školské rady?

Škola bude v první řadě zveřejňovat osobní údaje osob, pokud jí to ukládá zákon. I v těch případech je však třeba dbát na dodržování principu minimalizace a nezveřejňovat tak údaje, které nejsou nezbytně nutné pro splnění zákonné povinnosti.

Pokud povinnost zveřejnit osobní údaje učitelů neplyne z právního předpisu, za určitých podmínek lze přesto zveřejnit jejich kontaktní údaje. Zveřejnění, které je také zpracováním, lze založit na veřejném zájmu, neboť je jistě v zájmu veřejnosti mít přístup k určitým zaměstnancům

školy. Takto lze tedy odůvodnit zejména zveřejnění kontaktních údajů širšího vedení školy, případně sekretariátu. Pod veřejný zájem lze nejspíše podřadit i zveřejnění kontaktních údajů třídních učitelů či vedoucích kateder/kabinetů. Není však možné na základě veřejného zájmu zveřejnit kontaktní údaje všech učitelů či případně dalších nepedagogických pracovníků.

Co se týká rozsahu zveřejněných údajů, jak je uvedeno výše, z důvodu minimalizace je třeba zveřejnit pouze minimální rozsah údajů. V souladu s GDPR tak bude zveřejnění celého jména a pracovních kontaktních údajů. Případné zveřejnění dalších údajů, jako je např. datum narození či fotografie, je však nutné důkladně zvážit a případně založit na jiném právním titulu, ve většině případů souhlasu dotčených osob.

V této souvislosti upozorňujeme, že škola by vždy svým zaměstnancům měla zřídit školní – pracovní emailové adresy, neboť soukromé emailové adresy zaměstnanců není možné zveřejnit jinak než s jejich souhlasem. Zároveň používání soukromých emailových adres zřízených na základě z internetu volně dostupných emailových služeb ohrožuje zabezpečení osobních údajů. Z toho důvodu, jak jsme blíže uvedli v bodě 6 Desatera, by pracovní emailové adresy měly být zajištěny prostřednictvím emailové služby centrálně pořízené pro celou školu.

13. Může škola zveřejňovat fotografie zaměstnanců na svých webových stránkách?

Povinnost zveřejnit fotografie zpravidla neplyne z žádného právního předpisu. Zároveň není možné takové zpracování odůvodnit veřejným zájmem na identifikaci pověřených zaměstnanců. Pro tyto účely v rámci principu minimalizace postačí uvedení jména a příjmení a pracovních kontaktních údajů. Zveřejnění podobizny je tak nadbytečné, a pokud by škola na zveřejnění na svých webových stránkách trvala, bylo by nutné zajistit souhlasy zaměstnanců, kterých by se to týkalo. Tyto souhlasy musí být svobodné, určité, informované a jednoznačné a musí být uděleny na omezenou, předem určenou dobu (k otázce souhlasu jako právního titulu více ve 3. bodě Desatera).

14. Za jakých podmínek může škola zveřejňovat fotografie žáků?

Pořizování a zveřejňování fotografií žáků zpravidla nebude možné založit na žádném jiném právním titulu kromě souhlasu. Výjimkou je oprávněný zájem školy v případě vydávání studentských kartiček či průkazek, které slouží pro identifikaci studenta; v tomto případě lze pořídit fotografii bez dalšího, její zveřejnění však bez souhlasu nepřichází v úvahu. Nicméně v ostatních případech, kdy se uplatní souhlas, je třeba zajistit splnění náležitostí dle GDPR, zejména aby byl souhlas svobodný, určitý, informovaný a jednoznačný a aby byl udělen na omezenou, předem určenou dobu (více k náležitostem souhlasu ve 3. bodě Desatera).

Souhlas je ideální zajistit již při pořizování fotografie, kdy by také měla být splněna informační povinnost školy vůči žákovi.

Obecnou výjimkou jsou fotografie, na kterých nelze rozeznat konkrétní osoby, neboť tyto nepodléhají ochraně dle GDPR.

15. Může škola zveřejňovat údaje o úspěších svých žáků?

Zpracování takových údajů zpravidla nebude možné založit na žádném jiném právním titulu kromě souhlasu.

Aby byl souhlas udělovaný žáky v souladu s GDPR, je třeba, aby byl svobodný, určitý, informovaný a jednoznačný a aby byl udělen na omezenou, předem určenou dobu (k náležitostem souhlasu více ve 3. bodě Desatera).

Pro úplnost dodáváme, že předávání údajů při samotné organizaci účasti studentů v soutěžích či školních olympiádách apod. bude rovněž třeba založit na souhlasu žáků, případně jejich

zákonných zástupců (pokud se tedy žáci nebudou přihlašovat sami přímo). Důvodem je, že se jedná o dobrovolnou aktivitu, jejíž organizace není povinností ukládanou právními předpisy.

16. Je škola povinna smazat veškeré fotografie poté, co žák ze školy odejde?

Škola je oprávněná zpracovávat osobní údaje žáka pouze po dobu trvání právního titulu, na základě kterého jsou údaje zpracovávány. Pořizování a zveřejňování fotografií zpravidla podléhá souhlasu žáka nebo jeho zákonného zástupce, neboť není možné jej založit na žádném jiném právním titulu. Právní předpis takovou povinnost nestanoví a oprávněný zájem se ve školním prostředí v této souvislosti prakticky neuplatní. Výjimku tvoří pořízení fotografií studentů za účelem vytvoření studentských kartiček či průkazek, které slouží k identifikaci studenta a které podléhá oprávněnému zájmu školy.

Nicméně, vzhledem k omezené době platnosti souhlasu, je po uplynutí této doby nutné veškeré fotografie, kterých se týká, smazat a dál nezpracovávat. To se týká veškerých galerií, archivních databází i záloh, které má škola k dispozici. Pokud má škola zájem na dalším uchovávání fotografií, je třeba udělené souhlasy obnovit, včetně bývalých studentů, u kterých může být obnovení souhlasu složitější. Při pořízení fotografie je však možné koncipovat udělení souhlasu tak, aby pokrylo dobu studia studenta a předem určenou dobu následující po ukončení studia. Není však možné udělit souhlas na dobu neurčitou.

Jako vhodné technické řešení se jeví vytvořit databázi osobních údajů žáků a systém štítkování, ze kterého bude jasné, zda se jedná o údaje současného žáka školy, či o absolventa, zejména např. fotografie ze školních akcí či údaje týkající se jeho školních úspěchů. Některé technické nástroje pak mohou umožňovat nastavení systému upozornění v závislosti na nastavení doby platnosti souhlasu. Implementací takového postupu bude pro školu jednodušší údaje bývalých žáků vyhledat a vymazat, či případně nastavit novou dobu uchování při udělení nového souhlasu.

Obecnými výjimkami jsou fotografie, na kterých nelze rozeznat konkrétní osoby, neboť tyto nepodléhají ochraně dle GDPR.

DRUŽINA

17. Je nutné pro účely zájmových, mimoškolních aktivit organizovaných přímo školou, kterými jsou např. různé kroužky či družina získávat souhlasy žáků, případně jejich zákonných zástupců?

Pokud škola organizuje mimoškolní aktivity nad rámec jejích povinností dle dle školského zákona, poskytuje tak žákům služby na základě smlouvy (nehraje roli, zda se za tuto službu platí, či nikoli). Škola tak bude moci zpracovávat údaje žáků, případně jejich zákonných zástupců, pokud je to nezbytně nutné pro poskytnutí služby. Konkrétní rozsah nutných údajů bude záležet na konkrétní aktivitě, kterou škola organizuje. Dá se předpokládat, že mezi tyto údaje budou obvykle patřit jméno, příjmení a kontaktní údaje. Pro fyzické aktivity, jako je např. plavání, však bude nutným údajem i údaj o zdravotním stavu žáka (tam, kde například bude sdělena konkrétní informace o zdravotních omezeních, samotná informace o tom, že je žák schopen se sportovní aktivity účastnit, není nutně údajem o zdravotním stavu). Bez těchto údajů nebude možné službu poskytnout.

Ostatní údaje, které pro poskytování služby družiny či dobrovolného kroužku nebudou nezbytně nutné, bude možné zpracovávat pouze na základě souhlasu žáka či jeho zákonného zástupce. Takovými údaji mohou být např. fotografie či v některých případech data narození. Pokud žák tyto údaje odmítne poskytnout, neznamená to, že nebude možné službu poskytnout. Škola ji pouze poskytne v omezeném rozsahu, ve kterém dodatečné údaje nejsou potřebné. Ve všech případech se však uplatní informační povinnost, dle které musí škola žáka, případně i

zákonného zástupce, informovat o důsledcích jejich případného rozhodnutí údaje neposkytnout.

KAMERY A KONTROLA SÍTĚ

18. Za jakých podmínek může škola provozovat kamerový systém v prostorách školy?

Provozování kamerového záznamu je možné založit na oprávněném zájmu, kterým je ochrana majetku, a veřejném zájmu, kterým je ochrana bezpečnosti žáků a dalších osob. Nicméně, dle výkladové praxe ÚOOÚ není možné zvolit kamerový systém se záznamem jakožto obecné a plošné opatření, aniž by škola již historicky zažila problém s ochranou majetku nebo bezpečnosti osob.

Pokud se však škola rozhodne kamerový systém využívat, je třeba při volbě konkrétního řešení dbát na zásadu přiměřenosti, a to zejména ze tří následujících hledisek. V první řadě je třeba zvážit umístění kamer. Žákům a zaměstnancům školy musí být vymezeny soukromé prostory, ve kterých nebudou podrobení sledování kamer. V prostorách školy to budou zejména toalety, šatny a kabinety učitelů. Oproti tomu umístění kamer monitorující vchod do budovy či u šatních skříněk lze obecně považovat za přijatelné řešení. Další oblastí, kde se uplatní zásada přiměřenosti, je nastavení doby uchování kamerového záznamu. Záznam není možné uchovávat několik měsíců či dokonce let. Jako obecně přiměřená doba uchování se považují řády jednotek dní. V neposlední řadě je třeba vzít v úvahu kvalitu záznamu. Zvukový záznam bude dle ÚOOÚ ve většině případů považován za hrubý zásah do soukromí osob, a tedy za nepřiměřené opatření.

Škola však bude mít vždy informační povinnost. K tomuto účelu obvykle využívané piktogramy je třeba doplnit o identifikaci správce (školy) a odkaz na podrobnější informace o tomto zpracování osobních údajů (např. konkrétní osoba, místo či web).

Pro úplnost dodáváme, že provoz kamerového systému bez záznamu není dle stanoviska ÚOOÚ považováno za zpracování osobních údajů, a nevztahuje se tedy na něj ochrana relevantních předpisů.

19. Za jakých podmínek může škola monitorovat užívání počítačové sítě? Je rozdíl mezi monitorováním žáků a zaměstnanců?

Přípustným účelem monitorování počítačové sítě může být primárně např. zajištění kybernetické bezpečnosti, nikoli však sledování a kontrola zaměstnanců při plnění jejich pracovních povinností. Právním základem pak bude oprávněný zájem školy, a to jak pro monitorování užívání počítačové sítě žáky, tak i zaměstnanci. V obecné rovině není z pohledu GDPR zásadní rozdíl mezi monitorováním užívání počítačové sítě žáky nebo zaměstnanci; ten může být dán spíše faktickými okolnostmi, kdy například zaměstnanci budou oprávněni používat zařízení školy pro soukromé účely, zatímco žáci nikoli atp.

Při volbě konkrétního řešení sloužícího k monitorování počítačové sítě je třeba dbát na dodržení zásady přiměřenosti tak, aby byla zvolena metodika, která nezasahuje do práv a svobod osob více, než je nezbytně nutné pro dosažení vytyčeného účelu. Dle výkladové praxe je zejména třeba volit opatření k prevenci hrozeb, nikoli k jejich detekci na základě chování uživatele na síti (např. pohyby kursorem myši apod.). Za vhodné opatření lze považovat zablokování určitých stránek či podezřelých příchozích a odchozích dat, aniž by docházelo k analýze jejich obsahu.

Zaměstnancům a dalším uživatelům by však měl být vymezen soukromý virtuální prostor, který monitorování nebude podléhat. Relevantní je to zejména ve vztahu k pracovním kalendářům, které jsou často užívány i pro soukromé schůzky. K tomuto účelu je vhodné implementovat vnitřní systém značení či štítkování, který striktně odliší pracovní/školní obsah od toho

soukromého. Pokud by nebylo možné takové oddělení provést či monitorování sítě a přístrojů jinak omezit, je vhodné zvážit úplný zákaz užívání školních přístrojů k soukromým účelům. Obdobné oddělení pracovního a soukromého obsahu je třeba zajistit i v případě, pokud je zaměstnancům školy umožněno využívat vlastní zařízení pro pracovní účely (soukromé telefony, soukromé počítače apod.). Lze doporučit, aby zaměstnanci v těchto případech měli povinnost implementovat určitá bezpečnostní opatření na vlastních zařízeních, aby byla zajištěna stejná úroveň ochrany osobních údajů.

V neposlední řadě má škola povinnost uživatele o monitorování informovat, včetně pokynů k užívání monitorovaných zařízení. Informační povinnost může být plněna zejména vnitřním předpisem, který bude zaměstnancům a dalším osobám neustále dostupný a ve kterém je třeba uvést také podmínky užívání vlastního zařízení pro pracovní účely.

20. Je nutné požadovat souhlas zákonného zástupce pro připojení vlastního zařízení žáka do sítě (Wi-Fi poskytovaná školou), pokud je síť monitorována?

Monitorování počítačové sítě (a přístup do ní) není vhodné zakládat na souhlasu žáka nebo jeho zákonného zástupce. Důvodem je, že ve školním prostředí lze pochybovat o svobodnosti uděleného souhlasu, vzhledem k nerovnému postavení školy a subjektů, zejména žáků. Naproti tomu vhodným právním titulem zpracování je oprávněný zájem školy, účelem pak zajištění kybernetické bezpečnosti.

Při monitorování počítačové sítě je třeba zajistit přiměřenost zvoleného opatření, aby nedocházelo k nadměrnému zásahu do práv a svobod osob. Nejvhodnější je pouze pasivně chránit školní síť a provoz, který se v rámci ní odehrává. Vzhledem k tomu, že je prostřednictvím školní sítě možné získat přístup k osobním údajům, je třeba zvolit takové IT systémy a software, které umožní kontrolu uživatele a zabrání přístupu neoprávněným osobám k těmto údajům, ať už prostřednictvím zařízení školy či soukromého zařízení uživatele připojeného do školní sítě. Základním opatřením např. bude zajistit, že Wi-Fi síť určená pro běžné užívání studenty a např. návštěvníky školy bude oddělená od „interní“ Wi-Fi sítě používané pracovníky školy pro plnění pracovních úkolů. Pokud by správa a kontrola oprávnění přístupu zajištěna nebyla a každé zařízení připojené do sítě by tak mohlo mít přístup k osobním údajům, případná ztráta i soukromého zařízení by mohla mít za následek porušení zabezpečení údajů a uplatnění povinnosti hlášení incidentů ÚOOÚ.

Škola by vždy měla upozornit na podmínky monitorování a ochrany osobních údajů v rámci informační povinnosti, např. formou vnitřního předpisu, ve kterém je zároveň třeba popsat, za jakých okolností je možné připojit vlastní zařízení do sítě a jakými zárukami je chráněno soukromí osob.

UKLÁDÁNÍ ÚDAJŮ MIMO INFRASTRUKTURU ŠKOLY A CLOUD

21. Je možné ukládat všechny údaje na jednom místě?

Ano, neexistuje žádný požadavek dle GDPR, který by škole ukládal povinnost uchovávat osobní údaje na několika oddělených místech. Zásadní je, aby vybrané místo, na kterém jsou údaje ukládány, bylo dostatečně zabezpečeno, aby byly naplněny náležitosti týkající se technických a organizačních opatření, zejména dle článku 32 GDPR.

Škola má v zásadě dvě možnosti, kde může jí zpracovávané údaje uložit. V první řadě může pro ukládání údajů využívat server umístěný ve vlastních prostorách, v takovém případě však jednak musí být vyhrazen odpovídající prostor splňující technické a bezpečnostní a jednak musí škola vyčlenit podstatné náklady na údržbu a pravidelnou aktualizaci systémů zabezpečení tak, aby vždy byla zajištěna nejvyšší možná úroveň zabezpečení osobních údajů. Druhou možností je využít služeb poskytovatelů cloudových služeb, kteří pro uložení údajů poskytují vlastní datová centra – tzv. vzdálená úložiště. Škole je pak zajištěn neustálý vzdálený přístup k těmto

údajům, díky čemuž může škola, resp. její zaměstnanci uložené údaje upravovat, opravovat, mazat a dále s nimi pracovat.

Ať už zvolí škola jakoukoli z výše uvedených možností pro uložení osobních údajů (nebo jejich kombinaci), dle GDPR je jakožto správce povinna zajistit také neustálou dostupnost údajů. Z toho důvodu by škola měla zajistit, aby v případě bezpečnostního incidentu nedošlo ke ztrátě celého obsahu úložiště, a tedy ke ztrátě osobních údajů. Za tímto účelem by škola vždy měla uchovávat odpovídající zálohy dat, které by měla pravidelně aktualizovat, aby odpovídaly skutečnému a současnému stavu. Pokud by škola zvolila první možnost a ukládala údaje ve svých prostorech, odpovídala by i za správu záloh dat. Oproti tomu při volbě druhé možnosti je možné tuto odpovědnost přenést na poskytovatele cloudových služeb, který je vůči škole v postavení zpracovatele a který tak musí zajistit jednak nejvyšší úroveň zabezpečení a jednak aktuální zálohy všech údajů.

S ohledem na to, že obnova dat při případné ztrátě prakticky nebude možná, pokud budou data i jejich zálohy fyzicky na stejném místě, a bezpečnostní incident tak pravděpodobně postihne jak originál dat, tak jejich zálohy, doporučujeme zálohy dat oddělit a neuchovávat tak na stejném místě, např. ve stejné místnosti, na stejném serveru apod.

22. Může škola outsourcovat určité činnosti, např. zajištění bezpečnosti?

Ano, může. GDPR nezakazuje outsourcing některých služeb pro zajištění povinností správce za předpokladu, že jsou naplněny všechny požadavky. Zejména je třeba uzavřít smlouvu s poskytovateli outsourcovaných služeb, kteří jsou z pohledu GDPR považováni za zpracovatele. Ve zpracovatelské smlouvě je nutné upravit rozsah odpovědnosti zpracovatele, přičemž však primárně odpovědným za soulad vnitřních procesů s GDPR zůstává vždy správce, tedy škola. Zpracovatel může správci pouze pomoci některé povinnosti naplnit či jejich naplnění doložit.

Typicky jsou outsourcovány služby, jejichž účelem je uložení a zabezpečení osobních údajů, které jsou poskytovány zejména poskytovateli cloudových služeb. Existuje celá škála cloudových řešení, která se liší rozsahem odpovědnosti, která je přenesena na poskytovatele cloudových služeb, jakožto zpracovatele. Při využití maximálního zapojení poskytovatele cloudových služeb (tzv. SaaS – software jako služba) jsou všechny údaje uloženy ve vzdálených úložištích zpracovatele, který je smluvně zavázán zajišťovat maximální úroveň jejich zabezpečení a odpovídající aktualizované zálohy, aby v případě bezpečnostního incidentu nedošlo ke ztrátě dat. Škole jakožto správci je pak zajištěn neustálý dálkový přístup k údajům, aby s nimi mohla nakládat a uživatelům zajišťovat jejich dostupnost, integritu a důvěrnost. S ohledem na přístup k údajům a zajištění kvalitního fungování služby je vhodné do zpracovatelské smlouvy zapracovat (nebo k ní připojit) také dohodu o úrovni služeb (Service Level Agreement, SLA), která blíže specifikuje rozsah uživatelské podpory, míru dostupnosti poskytované služby a nápravná opatření/sankce v případě nedodržení stanovených podmínek ze strany poskytovatele služby.

Při volbě konkrétního řešení pro zajištění bezpečnosti a dalších outsourcovaných služeb je třeba vzít v úvahu další relevantní faktory, kterými jsou např. náklady, včetně nákladů na údržbu a aktualizaci, kvalita poskytovaných služeb, tedy zejména úroveň garantovaného zabezpečení, reference a reputace poskytovatele cloudových služeb dokládající zkušenosti v oblasti školství atd.

23. Jaká cloudová řešení může škola bez problémů používat pro vzdělávací účely?

Škola může v zásadě využívat jakákoli cloudová řešení, která uzná za vhodná, za předpokladu, že budou splňovat všechny požadavky GDPR. V první řadě je třeba zajistit uzavření zpracovatelské smlouvy s vybraným poskytovatelem cloudové služby, ve které bude přesně

stanoven rozsah jeho odpovědnosti. Zároveň je třeba, aby cloudová služba poskytovala odpovídající kvalitu, která zajistí nebo pomůže zajistit maximální možnou úroveň zabezpečení osobních údajů.

V závislosti na konkrétní cloudové službě a smluvních ujednáních s jejím poskytovatelem je třeba zajistit, aby uložená data nebyla zneužívána pro neslučitelné účely zpracovatele (tzv. data mining), aby byly poskytnuty odpovídající záruky pro zajištění garantované úrovně ochrany, aby existovala aktuální záloha uložených údajů apod. Při výběru konkrétní cloudové služby a jejího poskytovatele je vhodné volit renomované poskytovatele se zkušenostmi ze sektoru školství, kteří jsou schopní garantovat nejvyšší úroveň zabezpečení a pomoci škole při plnění jejích povinností jakožto správce osobních údajů.

ÚNIK OSOBNÍCH ÚDAJŮ

24. Bude ztráta služebního telefonu zaměstnance školy považována za únik dat? Uplatní se na školu povinnosti v souvislosti s hlášením úniku dat?

Porušení zabezpečení osobních údajů nastane, pokud dojde k bezpečnostnímu incidentu, kvůli kterému hrozí (i) porušení důvěrnosti dat (tzn., že data mohla být zpřístupněna neoprávněné osobě), (ii) porušení dostupnosti dat (tzn., že data jsou na určitou, i přechodnou, dobu nedostupná škole a žákům či dalším subjektům údajů), nebo (iii) porušení integrity dat (tzn., že mohlo dojít k neautorizované změně zpracovávaných údajů). Pokud takové riziko nastane, je škola povinna bezpečnostní incident nahlásit ÚOOÚ. Výjimkou je, pokud je škola schopna prokázat, že není pravděpodobné, že incident bude mít za následek riziko ohrožení či porušení práv fyzických osob. Pro účely předcházení takovým následkům je obecně nejčastěji doporučovaným opatřením šifrování dat, neboť i v případě odcizení či ztráty dat jsou tato data pro třetí osoby nečitelná a tím pádem dostatečně zabezpečená. Je však nutné splnit dvě podmínky: šifrovací klíč k zašifrovaným datům musí zůstat v moci školy a škola musí disponovat odpovídající zálohou ztracených dat.

Vzhledem k tomu, že služební telefony učitelů mohou obsahovat osobní údaje, je možné, že jejich ztráta způsobí porušení zabezpečení, pokud nebudou implementována technická opatření, která tomu mohou zabránit. Kromě zmíněného šifrování je vhodné zajistit další úrovně zabezpečení, např. přístupové údaje do databází a emailové schránky či odemknutí zařízení otiskem prstu.

Je třeba brát v potaz, že pokud bezpečnostní riziko znamená *vysoké* riziko pro práva fyzických osob, je kromě hlášení ÚOOÚ škola také povinna oznámit porušení zabezpečení i osobám, jichž se týká.

25. Může za únik dat být považována i ztráta soukromého telefonu zaměstnance?

Škole nevznikne povinnost hlásit porušení zabezpečení osobních údajů v důsledku ztráty soukromého telefonu učitele v případě, že interně nastavila nakládání s osobními údaji tak, že důsledkům spočívajícím v ohrožení či porušení práv fyzických osob předejde. Toho lze dosáhnout dvěma způsoby, přičemž nejbezpečnější je implementovat kombinaci obou. V první řadě je vhodné v pracovní smlouvě učitele či interním předpisu zcela zakázat přístup k osobním údajům, resp. všem dokumentům, které mohou osobní údaje obsahovat prostřednictvím telefonu a dalších soukromých zařízení, a to včetně zákazu přístupu do pracovní emailové schránky. Dále je třeba nastavit pravidla pro užívání soukromých telefonů pro pracovní účely, např. ve vnitřním předpisu. Těmito pravidly budou zejména technická opatření sloužící k účinnému zabezpečení dat i po případné ztrátě zařízení. Učitelé by měli mít povinnost tato opatření ve svých zařízeních implementovat, pokud je chtějí užívat k pracovním účelům. Opatření by měla být stejná jako ta, která by škola případně aplikovala na služební

zařízení a jednalo by se např. o technologie šifrování, přístupové údaje do databází a emailových schránek či odemknutí zařízení otiskem prstu.

UPLATŇOVÁNÍ PRÁV

26. Pokud nás někdo požádá o práva na přístup či výmaz, musíme ověřovat jeho totožnost?

Právo na přístup či výmaz, stejně jako další práva (např. právo na opravu, doplnění nebo omezení zpracování) může primárně uplatnit zaměstnanec či žák, případně zákonný zástupce žáka. Vzhledem k povinnosti školy zajišťovat důvěrnost a integritu osobních údajů, a tedy neumožnit přístup neoprávněné osobě, je ověření totožnosti žádoucí; požadavky na způsoby identifikace osob při uplatňování jejich práv však nejsou přímo GDPR stanoveny. Škola je v souladu s GDPR oprávněna požadovat dodatečné informace k potvrzení totožnosti žadatele údajů a v případě, že jeho totožnost nelze zjistit, může žádost odmítnout. Je vždy nutné dbát na to, aby ověření totožnosti bylo přiměřené a neztěžovalo výkon práv.

V případě osobní žádosti je požadavek předložení průkazu totožnosti (občanský průkaz) v pořádku, avšak nelze za tímto účelem uchovávat kopie dokladu. Ve většině případů bude v rámci principu minimalizace postačovat ověření jména a příjmení fyzické osoby, nicméně lze do rozsahu nezbytných údajů také zahrnout např. datum narození, zejména pokud se jedná o velmi běžné – a tudíž zaměnitelné – jméno.

Jestliže se jedná o uplatnění žádosti prostřednictvím školního internetového systému či online aplikace, lze předpokládat, že pro podání žádosti bude nutné přihlásit se pomocí unikátních přístupových údajů, které škola žáku či jeho zákonnému zástupci přidělila. Tato úroveň ověření identity by měla postačovat, a škola by tak neměla požadovat žádné další údaje pro ověření identity. Postup pro získání, obnovu či případné důsledky ztráty těchto jedinečných přihlašovacích údajů by škola měla stanovit vnitřním předpisem, s nímž budou seznámeni jak zaměstnanci, tak žáci a jejich rodiče, aby bylo zajištěno, že si budou vědomi rizik spojených s neopatrným zacházením s těmito přístupovými údaji. Tyto informace mohou být součástí zásad ochrany osobních údajů, které škola může zveřejnit na svých webových stránkách a umožnit tak nahlížení subjektů údajů v případě jejich potřeby.

Obdobná pravidla se uplatní i pro podávání žádostí prostřednictvím emailu či telefonu. Škola tak bude moci požadovat poskytnutí dalšího údaje, pokud hrozí riziko záměny, a to z důvodu ochrany soukromí osob. Dle GDPR má škola právo odmítnout přístup či další práva žadateli, který dodatečný údaj odmítne poskytnout, ačkoli existují vážné důvody pro pochyby, zda se skutečně jedná o daného oprávněného žadatele.

27. Jaké údaje musíme poskytnout v případě práva na přístup? Vztahuje se tato povinnost i na testy žáků?

V rámci práva na přístup má žadatel právo na všechny osobní údaje, o které požádá. Pokud tedy např. požádá o všechny údaje, které o něm škola zpracovává, měla by mu být poskytnuta kopie všech údajů, tedy i včetně testů, které škola uchovává. Jedna kopie údajů musí být žadateli poskytnuta bezplatně a v elektronické formě (tam, kde byla žádost učiněna taktéž v elektronické formě), pokud žadatel nepožádá o jiný formát. Kromě samotných údajů má žadatel právo na další informace, např. účel a dobu zpracování či kategorie příjemců, kterým jsou údaje předávány.

Pokud škola zpracovává velké množství osobních údajů, může žadatele vyzvat, aby uvedl, kterých informací nebo činností zpracování se jeho žádost týká, ale žadatel údajů není povinen na takové zúžení žádosti přistoupit. S ohledem na potenciální povinnost zpřístupnit poměrně široký rozsah údajů a s ohledem na zásadu minimalizace zpracovávaných údajů lze doporučit, aby škola uchovávala jen nezbytné údaje, které potřebuje ke své činnosti, které jí ukládá zákon a/nebo které je běžné uchovávat s ohledem na zavedenou praxi. Typicky v případě uchovávání

písemných prací žáků tak bude vhodné uchovávat pouze významnější práce, nikoli každý výstup vytvořený žákem během výuky a ověřování jeho znalostí. V tomto ohledu je ovšem vždy třeba dbát zákonných požadavků – požadavek minimalizace osobních údajů samozřejmě nepřeváží nad zákonnou povinností určitý typ dokumentů uchovávat.

Škola může tuto žádost odmítnout, pouze pokud může dokázat, že se jedná o nedůvodnou či nepřiměřenou žádost, např. pokud jde již o opakovanou žádost ve stejném rozsahu. Škola však nemůže žádost odmítnout pouze z důvodu, že je její vyřízení příliš náročné. K tomu účelu může sloužit prodloužení standardní jednoměsíční lhůty o další dva měsíce.

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

28. Jaké kvalifikace má škola požadovat po pověřenci pro ochranu osobních údajů?

Ustanovení GDPR pouze stanoví, že pověřenec pro ochranu osobních údajů má být jmenován na základě svých odborných znalostí a profesních kvalit, zejména v oblasti práva a praxe ochrany osobních údajů. Požadovaná úroveň této odbornosti není předem stanovena. Bude záviset na mnoha faktorech, zejména pro kolik správců je činnost pověřence vykonávána (případy sdílených pověřenců), jaký rozsah osobních údajů je zpracováván jakými zpracovatelskými operacemi a při využití jakých nástrojů.

Jmenovaný pověřenec by v první řadě měl mít odpovídající úroveň znalostí práva, a to nejen vnitrostátního, ale i evropské praxe týkající se ochrany osobních údajů. Zejména by měl být důkladně seznámen s GDPR. Tyto znalosti jsou často dokládány různými certifikáty vydávanými organizacemi zabývajícími se ochranou osobních údajů.

Kromě teoretických znalostí by však pověřenec měl také mít povědomí o vnitřní struktuře školy, o procesech při kterých jsou údaje zpracovávány a o informačních a bezpečnostních systémech a opatřeních, které škola využívá nebo je schopna využívat. Měl by tedy rozumět školnímu prostředí a také zákonným povinnostem, které se na školu uplatní, aby jeho zapojení bylo zcela efektivní.

Skloubení právních a technických znalostí, zejména v oblasti počítačových technologií, nebývá vždy jednoduché ani běžné na pracovním trhu. Z toho důvodu je vhodné zvážit i možnost vytvoření týmu pověřenců, kteří budou společně ovládat celé spektrum nezbytných znalostí. Takový tým by pak mohl efektivně zvládat úkoly pověřence i pro více správců. Nicméně, i v případě, že bude ustaven tým, který jako celek naplňuje kvalifikační kritéria pro pověřence, je nutné jmenovat jednu konkrétní odpovědnou osobu pověřence, a to zejména z důvodu kontaktu s ÚOOÚ.

29. Co všechno může škola po pověřenci požadovat? Jaké úkoly mu můžeme zadávat?

Hlavní úkoly pověřence pro ochranu osobních údajů jsou vyjmenovány v článku 39 GDPR. Pověřenec má zejména za úkol poskytovat škole a jejím zaměstnancům poradenství při zpracování osobních údajů tak, aby byl zajištěn soulad se všemi relevantními předpisy, včetně vnitřních předpisů školy, při jejichž tvorbě by měl být konzultován. Soulad s předpisy ochrany osobních údajů je kontinuálním procesem, pověřenec by tedy v rámci monitorování procesů ve vnitřní struktuře školy měl být schopen případné rozpory a nesoulady zachytit a školu včas upozornit. Odpovědnost za soulad však vždy zůstává na správci, tedy škole, není možné ji na pověřence smluvně přenést.

Pověřenec dále vypracovává posudek při vyhotovení posouzení vlivu na ochranu osobních údajů, spolupracuje a je kontaktním místem pro ÚOOÚ. V neposlední řadě se podílí na školení pracovníků školy. Za tímto účelem by měly být přesně stanoveny jeho úkoly v tom smyslu, aby bylo jasné, zda půjde např. o interní školení či vypracování a zasílání aktualit z oblasti ochrany osobních údajů.

Škola může pověřence pověřit dalšími úkoly, je však nutné, aby nedocházelo ke střetu zájmů a aby na hlavní úkoly byl vydělen dostatečný čas a prostředky. Typicky je dalším vhodným úkolem zpracovávání a správa záznamů o činnostech zpracování, které mohou sloužit jako účinný důkaz souladu s GDPR, nebo zajištění plnění informační povinnosti v rámci zasílání aktualizovaných znění vnitřních předpisů dotčeným osobám. Pokud to umožní smlouva s pověřencem, není vyloučeno ani zapojení pověřence do jiných úkolů, které primárně s osobními údaji nesouvisí, vždy však za dodržení požadavku, že nedojde ke střetu zájmů.

SANKCE

30. Jaké následky dle GDPR hrozí škole, pokud její činnosti nebudou v souladu s GDPR?

Maximální sankce, která je stanovena pro porušení povinností dle GDPR je pokuta 20 milionů EUR, nebo 4 % světového obratu skupiny v závislosti, která z těchto částek je vyšší. Tuto maximální sankci je však možné uložit jen za některá, nejzávažnější porušení povinností, např. za porušení základních zásad, nedodržení náležitostí souhlasu či porušení povinností ve vztahu k výkonu práv subjektů údajů.

GDPR však umožňuje tuto maximální hranici snížit pro orgány veřejné moci, tedy i školy. Návrh českého adaptačního zákona, který v některých oblastech stanoví úpravu odlišnou od GDPR, této možnosti využívá a v § 60 odst. 5 stanoví, že maximální pokuta, která může být orgánům veřejné moci (tedy včetně škol) uložena, je 10 milionů Kč. Konkrétní výše pokuty bude záviset na okolnostech porušení povinnosti a uvážení ÚOOÚ.

Kromě administrativních sankcí ve formě pokut může hrozit také trestní postih, zejména pro trestný čin neoprávněného nakládání s osobními údaji. V neposlední řadě mohou oprávněné osoby požadovat náhradu škody za vzniklou újmu, což by bylo předmětem občanského řízení.

S ohledem na hrozící sankce doporučujeme nastavit závazná pravidla pro práci s osobními údaji pro zaměstnance tak, aby byla rizika porušení povinnosti omezena na minimum (více v odpovědi na otázky 8 a 9).