Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva

Bakalářská práce

GDPR a jeho implementace v právnické osobě

Miroslav Pavelka

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Miroslav Pavelka

Veřejná správa a regionální rozvoj – k.s. Jičín

Název práce

GDPR a jeho implementace v právnické osobě

Název anglicky

GDPR and its implementation on a legal person

Cíle práce

Autor bakalářské práce si klade za cíl uceleným způsobem vysvětlit proces implementace Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR) u konkrétního typu právnické osoby – školského zařízení.

Zároveň se bude snažit o zjištění, zda po účinnosti zákona o zpracování osobních údajů (adaptačního zákona č. 110/2019 Sb.) představuje implementace nařízení GDPR u konkrétní právnické osoby významnou změnu v procesech zpracování a principech ochrany osobních údajů, a v neposlední řadě odpovědět na otázku, zdali se s účinností nařízení GDPR zvýšila administrativní a finanční zátěž této konkrétní právnické osoby.

Obecným záměrem je pak vysvětlení principu nařízení GDPR a rozdílů v přístupu k problematice ochrany osobních údajů v České republice před a po účinnosti GDPR.

Metodika

Práce je metodicky rozdělena do několika částí.

První část je literární rešerší založenou na analýze dokumentů a právních předpisů. Bakalářská práce pracuje s různými typy zdrojů, z nichž hlavním je obecné nařízení o ochraně osobních údajů a navazující vnitrostátní legislativa. Cenným pramenem informací jsou stanoviska Evropského sboru pro ochranu osobních údajů a Úřadu pro ochranu osobních údajů. Kromě seznámení se základními právními předpisy se v teoretické rovině zabývá přiblížením problematiky ochrany osobních údajů při aplikaci nařízení GDPR po adaptaci zákonem o zpracování osobních údajů. Mimo jednotlivých pojmů vysvětluje tato část také princip nařízení GDPR a základní rozdíly mezi zákonem č. 101/2000 Sb., o ochraně osobních údajů a samotným předmětným nařízením.

Druhá část popisuje přípravu na implementaci nařízení GDPR spočívající v nezbytné detailní analýze organizace, zdůrazňuje význam odpovídajícího financování a podpory vrcholového managementu/vedení organizace. Zde bude při psaní práce čerpáno také z praktických zkušeností získaných při implementaci nařízení GDPR u několika právnických osob vystupujících v pozici orgánu veřejné moci.

Třetí část je analytická, čerpá z reálných dat získaných při vzorových implementacích GDPR a praktickým způsobem popisuje proces implementace. Detailněji se věnuje analýze nejčastějších problémů při implementaci GDPR, charakterizuje úlohu jednotlivých zaměstnanců z pohledu nezbytné spolupráce na procesu implementace, vysvětluje význam jejich dalšího vzdělávání a řeší jeden z nejvýznamnějších úkolů – zavádění technicko-organizačních opatření nejen s ohledem na samotné nařízení GDPR, ale veškerou legislativu vztahující se na konkrétní právnickou osobu včetně pravidel pro zajištění kybernetické bezpečnosti v prostředí ICT technologií.

Závěrečná část hodnotí dopad implementace nařízení GDPR na právnickou osobu, objasňuje pozitivní i negativní důsledky implementace GDPR a odpovídá na otázku, zda se s účinností nařízení GDPR opravdu zvýšila administrativní a finanční zátěž konkrétní právnické osoby.

Doporučený rozsah práce

30-40 stran

Klíčová slova

GDPR, obecné nařízení o ochraně osobních údajů, implementace GDPR

Doporučené zdroje informací

EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide 3rd Three ed. Edition, Autor: IT Governance Privacy Team ISBN 978-1-78778-192-4

GDPR for Dummies, 2019, Autor: Suzanne Dibble. ISBN 978-11-1954-614-6

GDPR / Obecné nařízení o ochraně osobních údajů (2016/679/EU) – Praktický komentář – 2., aktualizované vydání, Autor: Michal Nulíček, Josef Donát, František Nonnemann, Bohuslav Lichnovský, Jan Tomíšek, Kristýna Kovaříková. ISBN 978-80-7598-068-7

GDPR: Praktický průvodce implementací, Autor: Luděk Nezmar. ISBN 978-80-271-0668-4

Kybernetická kriminalita, 2. rozšířené a aktualizované vydání, 2018, Autor: Vladimír Smejkal. ISBN: 978-80-7380-720-7

Ochrana osobních údajů podle obecného nařízení o ochraně osobních údajů (nejen) se zaměřením na pracovněprávní vztahy, Autor: Jakub Morávek, ISBN 978-80-7598-587-3

Úřední věstník Evropské unie NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Zákon o zpracování osobních údajů (110/2019 Sb.). Praktický komentář, Autor: Michal Nulíček, Josef Donát, Bohuslav Lichnovský, František Nonnemann, Petr Habarta, Kateřina Kašpárková. ISBN 978-80-7598-467-8

Předběžný termín obhajoby

2020/21 LS – PEF

Vedoucí práce

Mgr. Michal Reichert, DiS.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 22. 9. 2020

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 15. 03. 2021

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "GDPR a jeho implementace v právnické osobě" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. 3. 2021 _____

Poděkování

Na tomto místě bych chtěl velmi poděkovat vedoucímu mé bakalářské práce Mgr. Michalu Reichertovi, DiS. za vstřícný přístup, který mi byl při tvorbě práce, zejména pak při její finalizaci, velkou oporou. Děkuji rovněž za cenné rady a v neposlední řadě za podporu a trpělivost při konzultacích.

GDPR a jeho implementace v právnické osobě

Abstrakt

Tato práce se věnuje tématu implementace nařízení GDPR ve školských zařízeních a související revizi již přijatých opatření či nastavených postupů v rámci dříve realizované implementace.

Úvodní rozsáhlá teoretická část velmi detailně popisuje nejdůležitější pojmy v oblasti ochrany a zpracování osobních údajů včetně přehledu povinností správců a práv subjektů osobních údajů. Literární rešerše je doplněna o analýzu související i navazující legislativy. V reakci na obecně špatné povědomí o smyslu a principech fungování obecného nařízení obsahuje komplexní vysvětlení významu nejdůležitějších pojmů a ustanovení. Pro správné propojení zdrojů do podoby relevantního teoretického vymezení pojmů a pravidel vyplývajících z předmětné právní úpravy byly již v této části aplikovány analyticko-syntetické metody. Cennými zdroji byla literatura vztahující se k dané problematice doplněná o formální prameny českého i evropského práva.

Vlastní část práce, analyticko-praktická, zasazuje zásady zpracování osobních údajů a dílčí teoretická vymezení do reálného provozu škol a přibližuje statutárním zástupcům těchto organizací problematiku ochrany osobních údajů konkrétními doporučeními. V návaznosti na informace získané při desítkách konzultací uskutečněných na základních a středních školách, při prováděných školeních a praktických implementacích GDPR je tato část doplněna o zcela konkrétní doporučení a o vybrané vzory dokumentů. Souhrnně je praktická část strukturována do postupu pro svépomocné provedení celé implementace GDPR, resp. její revize.

Obecným záměrem celé práce je představit nařízení GDPR a související adaptační zákon jako smysluplné normativní právní akty, které jsou při správném výkladu snadno uchopitelné a při dobře provedené implementaci nijak nenarušují činnost školských zařízení.

Klíčová slova: GDPR, implementace GDPR, zásady zpracování, ochrana osobních údajů, subjekt údajů, správce, zpracovatel, příjemce, pověřenec

GDPR and its implementation on a legal person

Abstract

This thesis deals with the topic of the GDPR implementation in the educational facilities and connected revision of already taken measures or set procedures under the terms of already realized implementation.

The extensive theoretical introductory part describes the most important key concepts in the field of personal data protection and processing including the summary of the data processor duty and personal data subjects rights in detail. The literary research is completed with the analysis of related and followed legislation and with the complex clarification of the most important concepts meaning and provisions in the reaction to generally poor awareness of the meanings and principles of the general regulation working. The analytical-synthetical methods were applied in this part for the right interconnection of the sources to the form of the relevant theoretical definition of meanings and rules arising from the concerned legislation. Highly valued source was the literature related to this topic completed with the formal sources of the Czech and European law.

The main part of the thesis – the analytical-practical part – implements the personal data processing principles and partial theoretical determination into the real school operation and describes the personal data protection issue by the particular recommendation to the statutory representatives of this establishment. As a result of information gained during tens of consultations in the primary and secondary schools, during the provided training courses and practical GDPR implementation, this practical part is completed with absolutely real recommendations and representative samples of documents. In general, the practical part is structured into the method for the self-help execution of all GDPR implementation, or its revision.

General aim of this thesis is to introduce the GDPR and the following adaptation law as useful normative legal acts that are easily realizable by means of the right explanation and that do not disrupt educational facilities activity with a perfectly accomplished implementation.

Keywords: GDPR, GDPR implementation, principles relating to processing, the protection of personal data, data subject, controller, processor, recipient, DPO

Obsah

Seznam obrázků

Seznam příloh

Seznam použitých zkratek

adaptační zákon	zákon č. 110/2019 Sb., o zpracování osobních údajů
AR	analýza rizik
DS	datová schránka
dozorový úřad	Úřad pro ochranu osobních údajů
DPIA	data protection impact assessment – posouzení vlivu na ochranu osobních údajů
DPO	data protection officer – pověřenec pro ochranu osobních údajů
EDPB	The European Data Protection Board / Evropský sbor pro ochranu osobních údajů
EHP	Evropský hospodářský prostor
EU	Evropská unie
GDPR	General Data Protection Regulation – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
HW	hardware
ICT	informační a komunikační technologie
informační zákon	zákon č. 106/1999 Sb., o svobodném přístupu k informacím
IS	informační systém
ISDS	Informační systém datových schránek
kontrolní řád	zákon č. 255/2012 Sb., zákon o kontrole
Listina základních práv a svobod	Usnesení č. 2/1993 Sb.; Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky
LZPS	viz Listina základních práv a svobod
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
nařízení GDPR	viz GDPR
NDA	Non-disclosure agreement (dohoda o mlčenlivosti)
NSS	Nejvyšší správní soud
Občanský zákoník	zákon č. 89/2012 Sb., občanský zákoník
obecné nařízení	viz GDPR
obecné nařízení o ochraně osobních údajů	viz GDPR

OČTŘ	orgány činné v trestním řízení
OVM	orgán veřejné moci
OÚ	osobní údaje
pověřenec	viz DPO
příjemce	příjemce osobních údajů
SLA	Service Level Agreement (dohoda o úrovni poskytovaných služeb)
správce	správce osobních údajů
správní řád	zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
subjekt	subjekt osobních údajů (subjekt údajů)
SÚ	viz subjekt
SW	software
ÚOOÚ	viz dozorový úřad
školský zákon	zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání
Směrnice 95/46/ES	Směrnice Evropského parlamentu a rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů
zákon o svobodném přístupu k informacím	viz informační zákon
vyhláška o základním vzdělávání	vyhláška č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky
zákoník práce	zákon č. 262/2006 Sb., zákon zákoník práce
zákon o ochraně osobních údajů	zákon č. 101/2000 Sb., o ochraně osobních údajů
zákon o registru smluv	zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů
zákon o svobodném přístupu k informacím	zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
zákon o zpracování osobních údajů	zákon č. 110/2019 Sb., o zpracování osobních údajů
ZOOÚ	viz zákon o ochraně osobních údajů
zpracovatel	zpracovatel osobních údajů
zpracování	zpracování osobních údajů
ZZOÚ	viz zákon o zpracování osobních údajů

1 Úvod

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), známé pod obecně užívanou zkratkou GDPR (dále také jako „obecné nařízení" nebo „nařízení GDPR"), je veřejností stále vnímáno vesměs negativně. Jde však spíše o neporozumění smyslu a principu tohoto nařízení. Nepochopení problematiky ochrany osobních údajů jednotlivými správci osobních údajů spolu s mediálním tlakem sílícím zejména od poloviny roku 2017 přerůstalo na jaře 2018 až v paniku. Spolu se špatným uchopením implementace to vedlo, a v celé řadě organizací stále vede, k zavádění zbytečně restriktivních opatření narušujících samotné efektivní fungování organizace. S tím pochopitelně souvisejí neadekvátní jednorázové výdaje na implementaci či periodické výdaje například na pověřence.

Z této situace v posledních měsících před účinností GDPR profitovaly různé poradenské firmy, ovšem vedle zavedených právních kanceláří a poradenských společností vznikalo na trhu velké množství menších firem s minimálními zkušenostmi s danou problematikou. Nabízely například služby v podobě vstupních analýz GDPR, často však bez schopnosti provést následně tzv. GAP analýzu[1] nebo samotnou implementaci GDPR.

Kromě pozdějšího prozření dochází v dnešní době při revizích souladu s obecným nařízením o ochraně osobních údajů a po zhodnocení vysokých vynaložených nákladů nekorelujících s kvalitou služeb poskytnutých zmíněnými firmami leckdy ke zjištěním, že pravidla a opatření zavedená na základě nekvalitních analýz jsou nejen často v přímém rozporu s GDPR, ale dostávají se do konfliktu i s další vnitrostátní legislativou. Příkladem budiž četné množství souhlasů se zpracováním osobních údajů aplikovaných s příchodem obecného nařízení, především ve školství. Vyznačovaly se nejen absencí povinných náležitostí, ale i absencí dodržení elementárního principu, kterým je svobodná vůle subjektu poskytujícího souhlas. Dokonce byly, a i v dnešní době stále jsou, tyto souhlasy hojně aplikovány na zpracování osobních údajů, které je ve skutečnosti prováděno na základě jiného důvodu zpracování, případně se dokonce o zpracování osobních údajů ve smyslu nařízení GDPR vůbec nejedná. Velmi podobně, byť s méně negativním dopadem, byla řešena problematika spolupráce s externími dodavateli služeb. Ti byli tlačeni svými zákazníky, tj.

[1] GAP analýza neboli analýza mezer – metoda komparace skutečného stavu s požadovaným stavem

správci osobních údajů, do podepisování zpracovatelských smluv, přestože se fakticky v roli zpracovatelů nenacházeli.

Obětmi neprofesionálního přístupu ze strany nezkušených poradenských firem se stávali nejen drobní podnikatelé, obecní úřady, školská zařízení, ale leckdy i větší organizace v podobě nemocnic či větších městských úřadů. Je zřejmé, že prostor pro takovou situaci vznikl nevhodným přístupem vlády, zejména pak vybraných ministerstev, které neřešily problematiku GDPR buď dostatečně včas nebo na potřebné úrovni. Politici využívali toto téma ke zviditelnění, čímž mj. přiživovali strach z blížící se účinnosti obecného nařízení.

V organizacích, které existovaly již před účinností nařízení GDPR, tedy před 25. květnem 2018, rozhodně nemělo docházet k zásadním změnám pravidel při ochraně a zpracování osobních údajů, natožpak k významnému nárůstu administrativní a finanční zátěže. Pochopitelně hrálo významnou roli dodržování platné legislativy, zejména zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále také jako „ZOOÚ“ nebo „zákonu o ochraně osobních údajů“) a zákona č. 89/2012 Sb., občanský zákoník (dále pouze jako „občanský zákoník“).

Příchod obecného nařízení přináší mnoha správcům dokonce zjednodušení. Je to i díky přístupu založenému na odpovědnosti správce a riziku zpracování, na němž je téměř celé nařízení GDPR vystavěno. Ukazuje tak legislativní stránku problematiky ochrany a zpracování osobních údajů v poněkud lepším světle, než tomu bylo v době aplikace původní vnitrostátní legislativy. Příkladem může být zrušení oznamovací povinnosti do veřejného registru v den účinnosti GDPR, podle které museli v minulosti správci osobních údajů povinně oznamovat zahájení či změnu určitých zpracování osobních údajů na ÚOOÚ. Zásadně se také zjednodušila přeshraniční výměna údajů mezi správci údajů, zejména těch ze zemí Evropského hospodářského prostoru (dále jen „EHP“)[2].

Dnešní pohled na oblast zpracování a ochrany osobních údajů organizacemi v postavení orgánu veřejné moci se s účinností zákona č. 110/2019 Sb., o zpracování osobních údajů (dále také jako „adaptační zákon“, „zákona o zpracování osobních údajů“ nebo „ZZOÚ“) mění ještě výrazněji. Ve srovnání s obdobím, ve kterém se zpracování osobních údajů řídilo pravidly a povinnostmi vyplývajícími z původního, téměř dvě dekády platného, zákona o ochraně osobních údajů, přináší aktuálně platná legislativa organizacím a společnostem větší prostor pro nastavení odpovídajících pravidel. Pro orgány veřejné moci

[2] Prostor zaručující svobodu pohybu, zboží, služeb, osob, kapitálu a znalostí sdružující země Evropské Unie a Islandu, Norska a Lichtenštejnska

(dále také „OVM“) navíc se zásadně menším rizikem sankcionování. Velmi k tomu přispívá absence klíčového represivního mechanismu v podobě pravomoci Úřadu pro ochranu osobních údajů (dále také „dozorový úřad“ nebo „ÚOOÚ“) ukládat kromě nápravných opatření také finanční postihy za porušení ochrany osobních údajů.

Praxe nicméně dlouhodobě ukazuje, že se v minulosti problematice ochrany osobních údajů a dodržování dříve platného ZOOÚ obecně nevěnovala patřičná pozornost. Příchod nové evropské právní úpravy tak výrazně pomáhá dostat pravidla pro ochranu a zpracování osobních údajů nejen v organizacích veřejné a státní správy, ale i v soukromých společnostech, do stavu, ve kterém měla být mnoho let před příchodem GDPR.

I když není možné z důvodu krátkého časového období účinnosti nařízení GDPR a nedostatku přímo související judikatury predikovat přesněji budoucí rozhodovací praxi soudů, snaží se tato práce čerpáním z výsledků šetření ÚOOÚ a z analýzy výkladových stanovisek a komentářů k legislativě co nejlépe přiblížit laikům proces implementace GDPR, respektive revize jeho již dříve uskutečněné implementace. Tito laici obvykle nedisponují hlubšími znalostmi v oblasti ochrany a zpracování osobních údajů. Snahou této práce je osobám přímo odpovědným za dodržování nařízení poskytnout ucelené informace ke zvládnutí revize aplikace GDPR a k přijetí přiměřeně nákladných nápravných opatření, a to bez narušení chodu organizace.

Vzhledem k orientaci práce na školství je řešeno i velmi specifické pojetí aplikace GDPR, ke kterému přispělo Ministerstvo školství, mládeže a tělovýchovy (MŠMT) svým metodickým doporučením pro školy a školská zařízení. Chyby vzniknuvší tvorbou doporučení a postupů pro nakládání s osobními údaji, a to zejména v rámci zpracování informací při organizaci vzdělávání, se dostávají do legislativního souladu jen pozvolna.

Přetrvávající mediální nezájem o toto evropské nařízení spolu s nutností řešit důležitější celospolečenská témata v období pandemie COVID-19 nedává velký prostor pro efektivnější napravování chybně zavedených postupů.

Pochopení fungování nařízení GDPR, spolu s celým souborem právních předpisů upravujících oblast ochrany a zpracování osobních údajů, není tak složité, jak by se mnoho na první pohled zdát. Nevytrhávají-li se jednotlivá ustanovení z kontextu, ale naopak vykládají-li se komplexně při zohlednění vazeb na ustanovení z dalších částí nařízení a rovněž v kontextu souvisejících právních norem, je poměrně jednoduché aplikovat pravidla na jednotlivé operace zpracování prováděné správci osobních údajů, případně prováděné najatými zpracovateli.

2 Cíl práce a metodika

2.1 Cíle práce

Obecným záměrem práce je vysvětlit základní principy, na kterých je nařízení GDPR postaveno, a propojit abstraktní svět legislativní vrstvy ochrany osobních údajů s mnohdy velmi vzdáleným praktickým prostředím škol.

Hlavním cílem této práce je na základě analýzy právní úpravy v oblasti ochrany a zpracování osobních údajů vytvořit komplexní soubor praktických pravidel pro nakládání s osobními údaji doplněný v závěru o chronologicky sestavený návod na revizi aplikace GDPR ve veřejné škole. V rámci tohoto cíle se práce zaměřuje na zcela konkrétní zasazení zásad zpracování osobních údajů a jednotlivých teoreticky vymezených povinností správce a práv subjektů osobních údajů do činností prováděných školským zařízením.

Dílčím cílem práce je najít vysvětlení pro masivní chybné aplikování obecného nařízení tisíci škol v České republice v letech 2017 a 2018. Pro realizaci tohoto sekundárního cíle bude ověřována hypotéza, že mohla významnou roli ve složitém a nesprávném zavádění GDPR ve školství hrát kromě veřejně se šířících a mediálně přiživovaných fám také Metodická pomůcka k aplikaci GDPR vydaná MŠMT na podzim roku 2017.

2.2 Metodika

Práce je metodicky rozdělena do dvou vzájemně provázaných částí, teoretickou a analyticko-praktickou.

V teoretické části je v rámci sekundárního výzkumu informací využito zejména rozsáhlých a detailních rešerší odborné literatury a předpisů týkajících se problematiky ochrany a zpracování osobních údajů zahrnujících zejména formální prameny českého a evropského práva. Výchozí metodu výkladu evropských předpisů tvoří výklad gramatický (jazykový), na který navazuje výklad teleologický (účelový) a komparativní.

Pro literární rešerše doplněné deskripcí jednotlivých pojmů, povinností, zásad atd. a o v praxi uchopitelná vysvětlení či zdůvodnění je čerpáno především z elektronických informačních zdrojů.

Vlastní část práce přechází od teoretického konstruktu k praktickému pohledu na oblast ochrany a zpracování osobních údajů v prostředí základních a základních uměleckých škol,

propojuje výklady pojmů a teoretická vymezení z první části s konkrétními postupy pro nakládání s osobními údaji žáků, jejich zákonných zástupců, ale i vedení a zaměstnanců školy.

Pro primární, tj. vlastní výzkum je z kvalitativních metod využito pozorování a zejména metoda nestrukturovaných dialogů na téma GDPR s desítkami statutárních zástupců škol a rovněž asymetrické výměny informací s pracovníky dozorového úřadu.

Analytické metody byly pro splnění dílčího cíle doplněny metodou komparace za účelem porovnání dvou verzí metodik MŠMT, na což navázalo explanační vyhodnocení vlivu zjištěné diskrepance. Jako technický nástroj pro relevantní identifikaci rozdílů mezi metodikami byl použit program ABBYY FineReader PDF 15 Corporate obsahující modul pro komparaci PDF souborů.

Závěry, doporučení a návrhy v práci se sice opírají o právní předpisy a dostupnou literaturu, ale díky rozhovorům, znalosti praktického prostředí škol a vlastních zkušeností a poznatků z prováděných implementací GDPR jsou sestaveny do podoby podpůrného materiálu pro revizi aplikování GDPR.

Vzhledem ke komplikované situaci způsobené déle než rok trvající pandemií COVID-19 nebylo možné realizovat plánovaný empirický výzkum přímo v prostředí škol. Původním záměrem bylo ve dvou vybraných veřejných školách (základní škola a základní umělecká škola) prakticky ověřit realizovatelnost navrženého postupu implementace. Praktická část závěrečné práce měla být doplněna o hodnocení a komparaci úrovně souladu s obecným nařízením mezi oběma školami, které přislíbily aktivní spolupráci.

S ohledem na vládní nařízení a obecně složitou situaci ve školství byly plánované schůzky opakovaně odkládány. Po opětovném vyhlášení nouzového stavu na začátku roku 2021 bylo po konzultaci s vedoucím práce od původního záměru upuštěno. Teoretická část práce byla rozšířena za účelem komplexního vysvětlení celé problematiky. Analogicky došlo k přepracování vlastní části práce a doporučené postupy byly zobecněny pro co nejširší aplikovatelnost napříč školskými zařízeními. Využity byly dříve získané zkušeností z prováděných implementací GDPR.

3 Teoretická východiska

Vznik Evropského nařízení GDPR nebyl nijak nečekaný a náhlý, jak se mnohdy široká veřejnost mylně domnívá. Již v roce 1981 byla ve Štrasburku přijata Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, známá také jako úmluva Rady Evropy č. 108 a která vstoupila v platnost v roce 1985. Česká republika ji ovšem ratifikovala až v roce 2001[3].

Mezinárodní vnímání ochrany práv a soukromí osob lze dovodit i z výkladu čl. 17 Mezinárodního paktu o občanských a politických právech z roku 1988[4]. Snaha Evropské Unie (EU) nastavit jednotné podmínky pro zpracování osobních údajů a ochranu jejich nositelů vyústila v klíčový instrument evropského práva, kterým se stala na téměř 23 let, tedy až do účinnosti obecného nařízení o ochraně osobních údajů, Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[5]. Na rozdíl od nařízení, která jsou přímo účinná i bez implementace do národní legislativy, však směrnice představuje pouze určitý soubor pravidel a doporučení. Právě tuto roli hrála směrnice 95/46/ES od 24. října 1995 až do 25. května 2018, tedy do účinnosti nařízení GDPR, které je již přímo aplikovatelné, a to bez jakýchkoliv zásahů do národní legislativy jednotlivých členských zemí.

3.1 Legislativa před účinností GDPR

Oblast ochrany soukromí je upravena v mnoha právních odvětvích. Prolíná se občanským právem hmotným a procesním, trestním právem, pracovním právem, ale i právem správním. Vyskytuje se v právu informačním, týká se svobody sdružování, veřejnoprávní kontroly, veřejnoprávní databáze, svobodného přístupu k informacím, oblasti daní, účetnictví a poplatků, finančního trhu a dohledu, zdravotní, sociální oblasti a bezpečnostní oblasti.

Ve vztahu k obecnému nařízení byly po analýze legislativních norem zahrnuty do teoretické části pouze předpisy bezprostředně související s GDPR, dále předpisy, které

[3] Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. In: *Sbírka mezinárodních smluv*. 2001, částka 52, 115/2001 Sb. m. s.
[4] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.3.6. Právní monografie (Wolters Kluwer ČR).
[5] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995. In: *EUR-Lex*. Lucemburk, 1995, Úř. věst. L 281, Svazek 015, 95/46/ES.

mu předcházely a které s ním aktuálně souvisí nebo na něj adaptují český právní řád. Dokumenty přímo neupravující ochranu osobních údajů způsobem hodným výzkumu za účelem naplnění cílů této práce však byly zohledněny při celkovém posuzování dopadů GDPR, a to především v praktické části.

Následující deskriptivní přehled právních norem zastřešený adaptačním zákonem se soustředí převáženě na tři poslední dekády a nepředstavuje taxativní výčet legislativních norem přímo či nepřímo dopadajících na ochranu a zpracování osobních údajů.

3.1.1 Listina základních práv a svobod

V souvislosti s aplikací právních předpisů na zpracování a ochranu osobních údajů je vhodné zmínit 2. a 3. odstavec čl. 10 Usnesení předsednictva České národní rady č. 2/1993 Sb. o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky (dále také jako „LZPS“ nebo „listina základnách práv a svobod“), které pojednávají o ochraně před neoprávněným zasahováním do soukromého života, resp. o informačním sebeurčení. Odstavec 3 čl. 10 výslovně říká, že „každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“.[6]

V komentáři k LZPS se hovoří o právu na informační sebeurčení jako o součásti osobní a soukromé sféry. Při omezování či zasahování do této sféry jsou požadována přísná kritéria na hodnocení opodstatněnosti narušení práva na informační sebeurčení.[7]

Evropský soud pro lidská práva dovozuje z práva na soukromý život reprezentovaného právem na informační sebeurčení také roli státu, který musí za vybraných okolností zpřístupnit subjektům informace z jejich osobní sféry, tedy osobních údajů, jejichž shromažďování příslušný stát provádí.[8]

3.1.2 Občanský zákoník

Občanský zákoník se explicitně ochraně osobních údajů nevěnuje, nicméně jako úplný kodex soukromého práva obsahuje celou řadu ustanovení zasahujících do této problematiky. Již první části v hlavě I hovoří o právu na ochranu soukromí, přičemž toto právo staví na

[6] Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů*. Praha, 1992, částka 1, číslo 2, čl. 10, odst. 3.
[7] Pospíšil, ., Langášek, ., Šimíček, ., Wagnerová a kol., . *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR).
[8] The European Court of Human Rights. *JUDGMENT - CASE OF ROTARU v. ROMANIA* [online]. STRASBOURG [cit. 01.03.2021].

roveň práv na ochranu života, zdraví, svobody, cti a důstojnosti.[9] Zcela zásadní je pak oddíl 6 hlavy II, věnující se osobnosti člověka. Pro správnou implementaci GDPR ve školském zařízení bude relevantní výklad paragrafů 84 až 90 podstatný. Upravují totiž aspekty možného pořizování a používání zvukového či obrazového záznamu, oprávněnosti zásahu do soukromí a pravidla pro šíření podobizny či písemnosti osobní povahy.[10]

Obzvláště fotografování, (detailně viz kapitola 4.6), bylo s příchodem GDPR často skloňováno. Stalo se zdrojem, v mnoha případech jím stále je, pro velmi nešťastná rozhodnutí správců vedoucí např. k neodůvodněnému ukončení zpracovávání fotografií nebo k opatřování nevalidních souhlasů se zpracováním osobních údajů.

3.1.3 Trestní zákoník

S blížící se účinností GDPR sílily reakce na výši sankcí uvedených v GDPR (blíže se této otázce věnuje kapitola 3.8). Málokdo si uvědomoval, že deliktní odpovědnost za neoprávněné nakládání s osobními údaji nestojí pouze na případných pokutách, ale na potenciálním odnětí svobody, přičemž toto riziko zde bylo dávno před účinností GDPR a vztahuje se přeneseně i na právnické osoby. Že může být jako trestný čin kvalifikováno i nedbalostní neoprávněné zveřejnění, sdělení či zpřístupnění osobních údajů, je patrné z § 180 zákona č. 40/2009 Sb., trestní zákoník (dále jen „trestní zákoník“).[11]

Zahrnutí i nedbalostní varianty této skutkové podstaty do trestního zákoníku je jistě pozitivním signálem a posunem ve snaze řešit nezodpovědný, v ČR velmi rozšířený, přístup k ochraně osobních údajů ze strany správců ze soukromého i veřejného sektoru.[12]

Cílem této práce není dovozovat, že by školy mohly při zpracovávání osobních údajů způsobovat závažná pochybení, na která by bylo možné aplikovat paragrafy trestního zákoníku z části „Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství“, je však vhodné mít o případných důsledcích nezákonného nakládání s osobními údaji povědomí. Po schválení výjimky z možného ukládání finančních postihů OVM ze strany ÚOOÚ při porušení obecného nařízení by mohli někteří správci osobních údajů dospět k názoru, že není nutné se souladem s obecným nařízením příliš zabývat.

[9] Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2012, částka 33, číslo 89, § 3, odst. 2.
[10] Ibid., § 84-90.
[11] Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2009, částka 11, číslo 40, § 180.
[12] Smejkal, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, s. 254.

3.1.4 Směrnice 95/46/ES

Stavebním kamenem GDPR byla Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice 95/46/ES“). Zrušena byla nařízením GDPR k 25. květnu 2018. Její transpozice vyústila na konci minulého tisíciletí ve všech členských státech EU k vytvoření národní legislativy regulující nakládání s osobními údaji. Unijní státy však k implementaci do svého právního řádu přistupovaly odlišně. Mnoho jich šlo při stanovování pravidel na ochranu osobních údajů nad rámec povinností stanovených touto směrnicí.[13] To však stěžovalo orientaci v předmětné problematice při přeshraniční spolupráci a při výměně dat nejen jednotlivým správcům osobních údajů, ale i samotným subjektům při posuzování oprávněnosti a zákonnosti nakládání s jejich osobními údaji v jiných evropských státech.

V České republice, která se v době vydání směrnice 95/46/ES na vstup do EU teprve připravovala, byla oblast ochrany a zpracování osobních údajů upravena kromě ustanovení v LZPS a v občanském zákoníku zejména zákonem č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.[14] Ten však nevyhovoval narůstajícímu objemu a rozsahu zpracovávání osobních údajů akcelerovaného překotným rozvojem ICT. Komplikovaná byla také jeho vymahatelnost, neobsahoval totiž sankční ustanovení, ani nestanovoval dozorový úřad, jako to později napravil zákon o ochraně osobních údajů. Neposkytoval rovněž soulad se zmíněnou směrnicí 95/46/ES, jejíž transpozice v předvstupní fázi, tedy v období harmonizace českého právní řádu s řádem EU před vstupem ČR do EU, byla završena v roce 2000 přijetím výše zmíněného zákona o ochraně osobních údajů.

3.1.5 Zákon o ochraně osobních údajů

ZOOÚ transponoval evropskou směrnici 95/46/ES a upravoval v české legislativní historii pravidla pro zpracování a ochranu osobních údajů bezmála devatenáct let. Díky mnoha novelám udržoval krok s rozvojem ICT a narůstajícím objemem zpracovávaných osobních údajů až do jeho zrušení v dubnu 2019. Obsahoval, a to v dostatečném rozsahu, sankční ustanovení za porušení zákona a zajistil nezbytný vznik dozorového úřadu. Jak se však s příchodem GDPR ukázalo, řada správců dlouhodobě nevěnovala problematice

[13] Governance, I. *EU General Data Protection Regulation (GDPR), third edition: An Implementation and Compliance Guide*. 978-1-78778-193-1: IT GOVERNANCE Publishing, 2019, s. 12.
[14] *Důvodová zpráva k vládnímu návrhu zákona o ochraně osobních údajů a o změně některých zákonů*. In: . Praha, 1999, číslo 374.

ochrany osobních údajů prakticky žádnou pozornost[15]. Obdobný přístup měly ovšem i subjekty, s jejichž údaji bylo nakládáno. Aktivněji začaly vnímat svá práva až s blížící se účinností mediálně sledovaného GDPR.

Při porovnání s GDPR sloužil ZOOÚ dozorovému úřadu v určitých aspektech jako represivnější nástroj na regulaci zacházení s osobními údaji, subjektům zajišťoval odpovídající práva, správcům osobních údajů ukládal adekvátní povinnosti a ÚOOÚ zajistil prostor pro sankcionování. Přestože tedy příchod GDPR neznamenal pro ČR fakticky zásadní změny v přístupu k otázce ochrany osobních údajů, hovořilo se o GDPR doslova jako o revoluci v ochraně osobních údajů.[16] ZZOÚ však nastavoval pravidla velmi podobně, jako to dnes dělá GDPR.

3.2 Legislativa po účinnosti nařízení GDPR

Účinnost GDPR měl původně doprovázet i český adaptační zákon, který měl nahradit ZOOÚ. Jeho přípravu však doprovázely komplikace kvůli politickým neshodám a proces schvalování byl ovlivněn velkým počtem pozměňovacích návrhů. Mezi platnou legislativu v období po účinnosti GDPR tak patřil i ZOOÚ (blíže viz „ETAPA II.“ v kapitole 3.3.4).

Ještě před účinností GDPR bylo oznámeno související evropské nařízení ePrivacy (název vychází z anglického Regulation on Privacy and Electronic Communications), celým názvem NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích). Jeho schvalování však stále provázejí komplikace a v době finalizace této práce nebyl znám ani očekávaný termín schválení.[17] V budoucnu bude doplňovat nařízení GDPR a regulovat ochranu soukromí účinněji v online prostředí.

3.2.1 Zákon o zpracování osobních údajů

ZZOÚ je v české legislativě zastřešujícím právním dokumentem, který formálně nahradil ZOOÚ a odstranil tak jeho přechodný souběh s nařízením GDPR („ETAPA II“ v kapitole 3.3.4). Jeho účinnost se překrývá i s jeho platností, tedy dnem vyhlášení ve sbírce,

[15] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017, s. 13. Právo pro praxi.
[16] *Hospodářská komora České republiky: GDPR – REVOLUCE V OCHRANĚ OSOBNÍCH ÚDAJŮ* [online]. [cit. 2.2.2021].
[17] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) COM/2017/010 final - 2017/03 (COD) [NÁVRH - NAŘÍZENÍ NENÍ ZATÍM SCHVÁLENO]. In: *EUR-Lex*. Brussels, 2017.

ke kterému došlo 24. dubna 2019. Kromě adaptace českého práva na GDPR implementuje, pochopitelně za přispění velmi rozsáhlého změnového zákona, dvě evropské směrnice, konkrétně (EU) 2016/680[18] a (EU) 2016/681[19], které již ze své povahy přímý dopad neměly. Povinně měly být implementovány jednotlivými státy EHP do 25. května 2018, tj. do nabytí účinnosti nařízení GDPR.

Po vzoru ZOOÚ platného od počátku milénia je prakticky totožná myšlenka vyjádřena i v ZZOÚ, a to v § 1. *„Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie a k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů“*.

Toto ustanovení koreluje s očekáváním autorů GDPR a dokládá konstantnost přístupu k ochraně osobních údajů v posledních dekádách. Hovořit o obecném nařízení pejorativně (viz kapitola 3.3.4), není na místě.

Zákon o zpracování osobních údajů má tři významné atributy:

a) Doprovodný zákon č. 111/2019 Sb. - za účelem adaptace českého právního řádu na obecné nařízení a za účelem implementace dvou souvisejících směrnic změnil celkem třicet devět zákonů[20].
b) Zrušení ZOOÚ – odstranění duplicitní právní úpravy a vyjasnění role i pravomocí ÚOOÚ, kterému ve druhé etapě (kapitola 3.3.4), tedy po účinnosti GDPR, ale před účinností adaptačního zákona, komplikovaly provádění kontrol určité nejasnosti ohledně obecné oprávněnosti sankcionování.
c) Zbavení všech orgánů veřejné moci sankční odpovědnosti za porušení nařízení GDPR, a to ustanovením: „*Úřad upustí od uložení správního trestu také tehdy, jde-li o subjekty uvedené v čl. 83 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016/679“.*[21]

[18] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. In: *EUR-Lex*. Brusel, 2016, L 119/89, 2016/680.
[19] Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. In: *EUR-Lex*. Brusel, 2016, L 119/132, 2016/681.
[20] Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 111.
[21] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 61, odst. 3.

Kromě již zmíněného, v českém právním prostředí netradičního, vyřazení OVM z okruhu pokutovatelných správců ze strany ÚOOÚ však nepřinesl tento zákon žádné převratné změny. Upravil práva a povinnosti správců osobních údajů v oblastech, kde nařízení GDPR neposkytuje komplexní právní úpravu, nebo kde zůstalo dispozitivní. Upravil rovněž některé specifické výjimky a dokončil proces první vlny adaptace českého právního řádu na GDPR. Splnil taktéž jednu významnou úlohu, a to vytvořením právního rámce pro Úřad pro ochranu osobních údajů s cílem zvýšení efektivity vykonávané dozorové a kontrolní činnosti v oblasti ochrany osobních údajů, která byla do té doby omezena z důvodu absence právní úpravy provádějící GDPR.[22]

V reakci na Směrnici 2016/680, resp. 2016/681, je velmi významná část ZZOÚ zaměřena na zpracování osobních údajů „*za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkon trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti a ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky*“.[23]

Jak je patrné z výčtu právních předpisů v předchozích podkapitolách, ZZOÚ není aktuálně jediným právním předpisem, který se zpracování osobních údajů přímo dotýká. Vytváří obecný právní rámec pro ochranu soukromí a je k ostatním zákonům ve vztahu podpůrnosti, tedy tzv. subsidiarity. Tento princip lze vysvětlit na vztahu dvou právních norem, má-li jedna ve vztahu k druhé povahu předpisu podpůrného, lze subsidiární předpis použít jen tehdy, neupravuje-li příslušnou otázku předpis druhý, který má ve vztahu povahu předpisu speciálního.

3.2.2 Pokyny Evropského sboru pro ochranu osobních údajů

Pokyny nezávislého poradního orgánu EU, Evropského sboru pro ochranu osobních údajů (The European Data Protection Board – EDPB), představují velmi důležitý zdroj práva v oblasti ochrany osobních údajů a ochrany soukromí.[24]

Tento orgán kromě metodického vedení vydává zejména stanoviska a doporučení v oblasti ochrany osobních údajů a ochrany soukromí, která zásadním způsobem pomáhají s výkladem a aplikací nařízení GDPR. Činnost EDPB rovněž přispívá k jednotnému

[22] Ježek, M. *Nový český zákon o zpracování osobních údajů z roku 2019* [online]. [cit. 2021-01-09].
[23] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 2, písm. b).
[24] *The European Data Protection Board (EDPB)* [online]. [cit. 2021-02-20].

uplatňování pravidel ochrany údajů v celé EU a zkvalitňuje spolupráci mezi místními dozorovými úřady v jednotlivých zemích EHP.[25]

Sbor vnikl s účinností GDPR transformací z pracovní skupiny 29 (Article 29 Working Party – WP29) zřízené podle článku 29 směrnice 95/46/ES. Odtud plynul i její název. Některá dříve vydává stanoviska a doporučení, která ještě před účinností GDPR toto nové nařízení reflektovala, byla postupně po příchodu GDPR ze strany EDPB revidována a opětovně publikována.[26] Úřad pro ochranu osobních údajů na svých stránkách pokyny, stanoviska a další materiály vydávané EDPB pravidelně zveřejňuje. Dokonce zajišťuje u vybraných dokumentů přednostně jejich překlad do českého jazyka, absentuje-li česká jazyková mutace. Zejména stanoviska jsou v době turbulentních změn cenným zdrojem informací, protože velmi pružně reagují na světové dění. Například v souvislosti s propuknutím nákazy covid-19 připravil EDPB expresně soubor doporučení pro nakládání s osobními údaji v boji proti globální pandemii.[27]

3.3 Základní seznámení s nařízením GDPR

Protože se téměř celá tato práce věnuje detailně přímo nařízení GDPR, dává ho do kontextu s další legislativou v teoretické i praktické části práce a popisuje jeho reálnou aplikaci, slouží tato kapitola pouze k obecnému seznámení s GDPR a s historií jeho vzniku, k vysvětlení jeho účelu a k deskripci několika základních atributů.

3.3.1 Historie vzniku GDPR

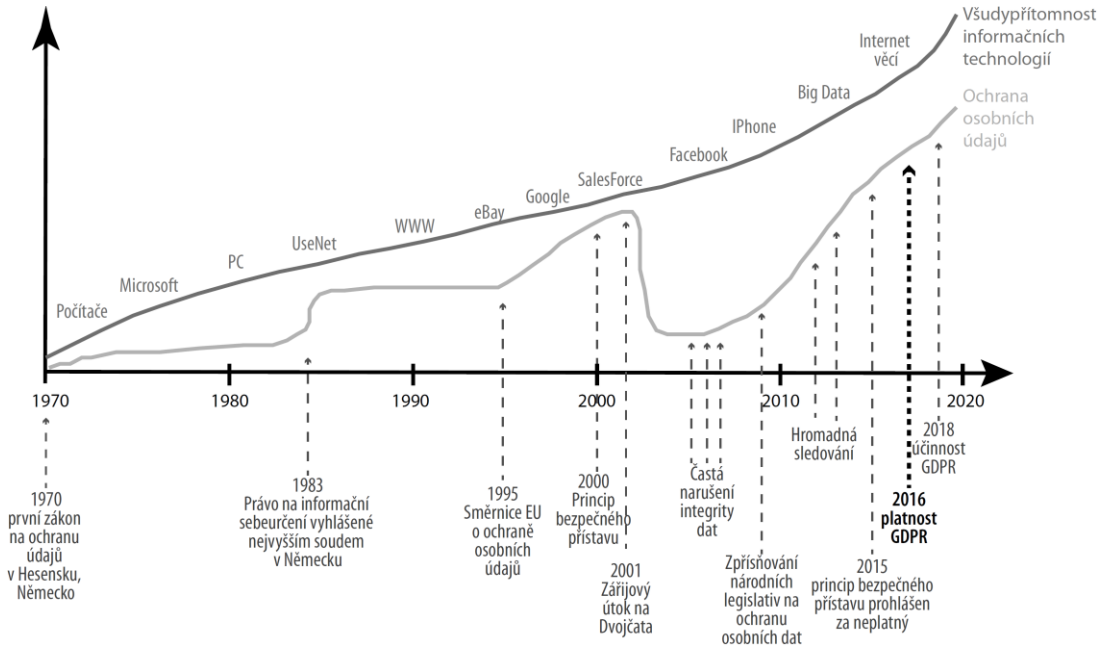
První veřejné oficiální oznámení plánu Evropské komise na zavedení nařízení nahradivšího tehdy platnou směrnici 95/46/ES pochází ze 17. listopadu 2011 ze zasedání 35. konference Datenschutzfachtagung, konference o ochraně osobních údajů, německé asociace pro ochranu a bezpečnost údajů (Gesellschaft für Datenschutz und Datensicherheit).[28]

V roce 2012 započaly intenzivní přípravy nařízení GDPR, a přestože bylo v roce 2014 téměř připraveno, byla kompromisní varianta po mnoha úpravách schválena až v roce

[25] Obecné pokyny Evropského sboru pro ochranu osobních údajů. *The European Data Protection Board (EDPB)* [online]. [cit. 07.01.2021].
[26] Article 29 working party. *Directorate-General for Justice and Consumers European Commission* [online]. [cit. 29.12.2020].
[27] Pokyny evropského Sboru (EDPB). *Úřad pro ochranu osobních údajů* [online].
[28] Gesellschaft für Datenschutz und Datensicherheit. *35. DAFTA am 17. und 18. November 2011 in Köln* [online]. [cit. 2020-11-18].

2015.[29] V Úředním věstníku EU byla definitivní podoba nařízení GDPR podepsána 27. dubna 2016 a zveřejněna dne 4. května 2016.[30] Odložená účinnost byla nastavena na 25. května 2018 tak, aby měly členské změně dva roky na adaptaci svého právního prostředí a na implementaci související směrnice 2016/680 a 2016/681.

Obrázek 1 interpretuje korelaci vývoje ICT a mezinárodních právních předpisů regulujících nakládání s osobními údaji od 70. let dvacátého století do současnosti. Obrázek rovněž ilustruje, že v závažných situacích a celospolečenských krizích může docházet k výrazným zásahům do soukromí a práva osob jsou omezována. Na ose „x" je znázorněn teroristický útok na budovy Světového obchodního centra v roce 2001, který přesně naplňuje definici kritické situace a podobný trend je možné pozorovat od roku 2020 v rámci protipandemických opatření. Dříve nemyslitelné zpracování údajů o použití platebních karet nebo využití geolokačních údajů z mobilního telefonu využívá mnoho zemí při trasování kontaktů s nakaženými. Z doporučení Komise (EU) vyplývá, že i tato otázka byla konfrontována s přísnými požadavky na ochranu soukromí osob.[31]



Obrázek 1: Vývoj technologií v porovnání s vývojem legislativy[32]

[29] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017, s. 16-19. Právo pro praxi.
[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). In: *Official Journal of the European Union*, 2016, L 119/1.
[31] Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. In: *EUR-Lex*. Brussels: Official Journal of the European Union, L 114/7, číslo 518.
[32] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017, s. 15. Právo pro praxi.

3.3.2 Účel, působnost a struktura nařízení GDPR

ÚČEL

Jedním z hlavních důvodů vzniku GDPR bylo sjednocení evropského právního prostředí ve vztahu k nakládání s osobními údaji fyzických osob. Snahou bylo zkvalitnit vymahatelnost práva a zajistit subjektům vyšší kontrolu nad jejich soukromím.

Pro naplnění tohoto účelu byly Evropskou komisí stanoveny **dva primární cíle**:

a) Ochrana práv, soukromí a svobod fyzických osob v EU

b) Snižování překážek v podnikání zjednodušením volného pohybu údajů v celé EU[33]

Pokud by se jednotlivé zákony implementující předchůdce GDPR, směrnici 95/46/ES, dodržovaly opravdu důsledně, jistě by bylo adekvátní hovořit o simplifikaci pohybu osobních údajů v EHP s příchodem GDPR.

Hledisko zjednodušení je v celé řadě činností zpracování s nabytím účinnosti obecného nařízení relevantní. Je to z velké míry principem, na kterém toto nařízení stojí, především přístupem založeném na odpovědnosti správce a riziku zpracování. Uvedené vymezení vyplývá ze zásad obecného nařízení (blíže viz kapitola 3.5).

Správce i zpracovatel musí vzít při své činnosti v potaz veškeré aspekty nakládání s osobními údaji, v jejich vzájemné vazbě je vyhodnotit, posoudit pravděpodobná rizika zásahu do práv a svobod nositelů osobních údajů a přizpůsobit podle toho další prováděné operace zpracování. Mezi zmíněné aspekty patří především rozsah zpracovávaných dat a jejich povaha v kontextu s účelem zpracování.

S ohledem na další ustanovení obecného nařízení je pravděpodobně jediným východiskem pro správce a zpracovatele zavedení alespoň základního řízení rizik.[34]

PŮSOBNOST

Místní působnost této evropské právní harmonizace sahá i za hranice EU, díky inkorporaci na základě dohod pokrývá celý EHP – kromě unijních států tedy i Island, Lichtenštejnsko a Norsko. Je účinné rovněž ve Švýcarsku z důvodu jeho členství v Evropském sdružení volného obchodu (ESVO)[35].

[33] Governance, I. *EU General Data Protection Regulation (GDPR), third edition: An Implementation and Compliance Guide*. 978-1-78778-193-1: IT GOVERNANCE Publishing, 2019, s. 14.
[34] Gellert, R. Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing. *Jusletter IT* [online]. Weblaw AG, 2017, February [cit. 2021-02-07].
[35] Mezinárodní hospodářská organizace se sídlem v Ženevě založená 1. července 1960 ve Stockholmu za účelem odstranění cel a kvantitativního omezení dovozu a vývozu zboží

Věcná působnost ovšem sahá daleko za hranice místní působnosti. Obecné nařízení se vztahuje nejen na všechny společnosti se sídlem v EU, resp. EHP, ale na veškeré správce osobních údajů, jejichž zákazníky či klienty jsou občané zemí EHP. Tento *extrateritoriální účinek* tak logicky ovlivňuje přístup k ochraně a zpracování osobních údajů celosvětově. Například Velká Británie musí i po svém odchodu z EU při přeshraniční výměně osobních údajů nebo při poskytování služeb vymezených místní působností GDPR nadále ctít zásady zpracování osobních údajů vymezené obecným nařízení.[36]

Vzhledem k úrovni elektronizace a globalizace služeb je třeba toto vzít v potaz při využívání online služeb, jmenovitě pak v případě sociálních sítí či cloudu, a zvolit si takové poskytovatele nabízející odpovídající záruky. O to více v situacích, kdy se v rámci činností rozhodne správce osobních údajů působící např. v ČR využít služeb zahraničních společností a zapojí je tak fakticky do zpracování – stanou se zpracovateli osobních údajů ve smyslu obecného nařízení.

Při deskripci věcné působnosti je vhodné upřesnit okruh potenciálních správců a subjektů, na které může nařízení působit. **GDPR se vztahuje pouze na zpracování osobních údajů žijících osob. Primárním cílem ochrany nejsou samotné osobní údaje, ale jejich nositelé, tedy fyzické osoby v situacích, kdy jsou jejich osobní údaje zpracovávány.** Na zpracování, která nejsou obecným nařízením pokryta (např. ochrana údajů osob zesnulých), se aplikuje jiná legislativa (např. občanský zákoník).

Rovněž ochranu údajů při zpracování pro osobní potřebu obecné nařízení nepokrývá. Příkladem budiž i rozsáhlé zpracování osobních údajů v online světě, zejména pak na sociálních sítích. Ve virtuálním online prostředí, typicky na sociálních sítích, si mnohdy subjekty mylně vykládají principy nařízení GDPR. V situacích, kdy do procesu nakládání s osobními údaji není zapojen podnikatelský subjekt, právnická osoba či orgán veřejné moci, a zpracování probíhá čistě v rovině soukromé, aplikují se pravidla soukromého práva daná například občanským zákoníkem.

STRUKTURA GDPR

Struktura legislativních dokumentů není obvykle natolik odlišná, aby si zasloužila větší pozornost. Nařízení GDPR je však významem a rozsahem preambule výjimečné. Tato

[36] Governance, I. *EU General Data Protection Regulation (GDPR), third edition: An Implementation and Compliance Guide*. 978-1-78778-193-1: IT GOVERNANCE Publishing, 2019, s. 24-26.

úvodní část sloužící jako soubor doporučení a zdůvodnění obsahuje 173 tzv. recitálů. Následuje vlastní text nařízení složený z 99 článků.

3.3.3 Forma právní normy, nařízení vs. směrnice

Formou normativního aktu, který Evropský parlament a Rada EU pro GDPR zvolili, se stalo **nařízení**. Ustanovení v evropských nařízeních jsou vždy přímo uplatnitelná a aplikovatelná členskými zeměmi i bez přijetí prováděcích právních předpisů, jejichž elementárním účelem je přizpůsobit vlastní právní řád do souladu s kogentními ustanoveními v nařízeních, případně transponovat ustanovení dispozitivní. Příkladem může být jeden z dispozitivních článků GDPR obsahující ustanovení *„Podmínky použitelné na souhlas dítěte v souvislosti se službami informační společnosti“*[37], který stanovil věkovou hranici 16 let pro způsobilost k udělení souhlasu. Připouští však snížení hranice až na 13 let prostřednictvím národní úpravy členského státu (blíže k problematice způsobilosti k poskytnutí souhlasu viz kapitola 4.1.1, zde je příklad uveden pro pochopení vztahu adaptačního zákona a dispozitivních ustanovení evropských nařízení). Ustanovení, která mohou být navazujícími národními zákony upravena, je v GDPR více.

Celkem osm unijních států, ČR nevyjímaje, nestihlo své prováděcí zákony připravit před účinností nařízení. V rozhovoru pro český rozhlas to potvrdila eurokomisařka Věra Jourová v den účinnosti GDPR.[38] V ČR měl nakonec adaptační zákon, blíže popsaný v kapitole 3.2.1, zpoždění téměř rok. V médiích zaznívalo v první polovině roku 2018 z úst politiků i odborníků, že to nepředstavuje problém, protože je nařízení přímo účinné. S tímto však nelze zcela souhlasit.

Je pravdou, že pro samotnou aplikaci GDPR není třeba přijmout adaptační zákon. Subsidiární princip legislativní hierarchie staví nařízení GDPR do role právního předpisu vyšší právní síly, jeho ustanovení jsou tak uplatnitelná i v případě, že pravidla upravuje paralelně, byť odchylně, normativní akt nižší právní síly, tedy např. v ČR v té době platný zákon o ochraně osobních údajů. Kolidující evropská nařízení s národními zákony, k čemuž dochází před schválením změnových zákonů doprovázejících adaptační zákony běžně, mají vždy přednost.

---

[37] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 8.

[38] Redakce iROZHLAS.cz. *Začalo platit GDPR. "Česko stále nemá potřebnou legislativu", varuje Jourová.* [online]. [cit. 2020-12-30].

Přijetí národní právní úpravy ještě před účinností GDPR však bylo pro unijní země nejen důležité, ale i závazné, poněvadž nařízení GDPR bylo doprovázeno dvěma dalšími právními dokumenty:

a) Směrnicí Evropského parlamentu a Rady (EU) 2016/680 (tzv. trestněprávní směrnice) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, ve znění pozdějších úprav, doplňků nebo změn a
b) Směrnicí Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. 4. 2016 o používání jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

K implementaci těchto směrnic došlo v ČR až v roce 2019 přijetím ZZOÚ[39] a přijetím doprovodného zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů[40].

Vybrané zdroje podpořené i judikáty definují v rámci vertikální účinnosti směrnice její přímou aplikovatelnost. Z konzultací s odborníky vyplývá názorový rozkol na tuto problematiku. Je nad možný objem práce toto detailněji zkoumat a není to ani předmětem vytyčených cílů, proto je dále vycházeno v souladu s dokumentem „The direct effect of European law“ z premisy, že směrnice nejsou přímo účinné, pouze v situacích, kdy jsou ohrožena práva osob nečinností členských států, které neprovedou nezbytnou implementaci, rozhodují evropské soudy v duchu směrnice, ve prospěch osob, byť je národní právo příslušného unijního státu v kolizi.[41]

3.3.4 Aplikace GDPR v ČR před a po účinnosti adaptačního zákona

Milníky 25. května 2018, tedy den účinnosti GDPR a 24. dubna 2019, den účinnosti ZZOÚ, rozdělují období posledních pěti let od přijetí GDPR (27. dubna 2016) na **tři etapy**. V každém fungoval přístup k ochraně a zpracování osobních údajů trochu rozdílně.

[39] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110.
[40] Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 111.
[41] The direct effect of European law. In: *EUR-Lex*. Publications Office, 2015.

Je dobré si však uvědomit, že obecné nařízení o ochraně osobních údajů je retroaktivní normou, tzn. že je aplikovatelné zpětně. Vztahuje se tedy i na zpracování osobních údajů činěná dávno před jeho účinností. V prostředí OVM lze zmínit například dopad na velmi zastaralé spisy uložené ve spisovnách mnoho let po lhůtě skartace nebo na elektronické databáze s dodnes nezmapovanými údaji, které nemají desítky let zákonný důvod pro zpracování, přesto jsou strukturovaně uloženy a v některých případech i využívány.

ETAPA I.

V první etapě, tedy v legisvakanční lhůtě ještě před účinností nařízení GDPR, se bez výjimky aplikoval v ČR ZOOÚ, nicméně v rámci příprav na příchod GDPR docházelo ke změně přístupu správců, zpracovatelů i samotných subjektů. Tito si na základě zvýšeného zájmu o GDPR začali více uvědomovat rizika spojená se zpracováním osobních údajů. Subjekty údajů ve větší míře registrovaly svá práva. Přestože obecné nařízení ještě nebylo účinné, již zkvalitňovalo obecný vztah k nakládání s osobními údaji.

Bohužel se v tomto období, resp. v druhé polovině legisvakanční lhůty, stalo v ČR mnoho chyb vedoucích k velmi vysokým investicím do zajišťování souladu s GDPR. To ostatně potvrzuje i vrchní rada pro vládní agendy z Úřadu pro ochranu osobních údajů, PhDr. Miroslava Matoušová.[42] Značná část veřejnosti se začala vůči obecnému nařízení vymezovat. Dělo se tak kvůli šířícím se fámám a v kontextu s neadekvátními veřejně prezentovanými postoji některých politiků. Ti téma GDPR využívali ke svému zviditelnění a kritizovali ho bez jeho hlubších znalostí a bez porovnání se stávající legislativou. Příkladem může být postoj Václava Klause ml., který se v rozhovoru pro Český rozhlas ještě den před účinností GDPR vyjadřoval velmi pejorativně a zastával názor, že GDPR nikdo nepotřebuje. Na účet obecného nařízení mimo jiné uvedl: „*GDPR je to naprostá blbost, která strašlivě organizačně zahltí obce, školy, malé firmy“* a *„Řeší se tady problém, který v jádru neexistuje. Protože když data kradete, je to trestný čin a mají vás za to taky zavřít. To ale neznamená, že musíte ubuzerovat k smrti kdejakou malou školičku.“*[43]

Přestože se vybraní odborníci snažili tyto postoje mírnit a nesprávně vnímaný obraz GDPR interpretovat reálněji, dařilo se to omezeně. V této fázi zklamala především vláda a vybraná ministerstva, MŠMT nevyjímaje, což patologický přístup k obecnému nařízení jen podpořilo.

[42] MATOUŠOVÁ, M. *Konzultace pro pověřence pro ochranu osobních údajů, Praha 9. října 2018*. Praha: Úřad pro ochranu osobních údajů, 2018.
[43] ČESKÝ ROZHLAS. *GDPR je naprostá blbost, tvrdí naštvaný Václav Klaus ml.* [online]. [cit. 2021-01-30].

ETAPA II.

Druhá etapa započala 25. května 2018 dnem účinnosti GDPR a skončila 24. dubna 2019 přijetím ZZOÚ.

Klíčové je pro tuto etapu vysvětlení úlohy v té době 18 let starého zákona o ochraně osobních údajů. V médiích i z úst odborníků bylo možné slyšet chybnou informaci, že byl příchodem GDPR zákon č. 101/2000 Sb. zrušen. I v aktuálních materiálech mohou být v této souvislosti informace nepřesné, např. že byl ZOOÚ zrušen obecným nařízením částečně.[44] Byl však platný a účinný od roku 2000 až do příchodu zákona o zpracování osobních údajů v dubnu 2019, a to i přes nabytí účinnosti GDPR v květnu 2018.

Pouze ustanovení zákona o ochraně osobních údajů, jež byla upravena zároveň nařízením GDPR, nebyla v období paralelní účinnosti uplatnitelná. Při aplikaci práva se použila ustanovení z nařízení. Ostatní paragrafy nekolidující s články obecného nařízení nebo neupravující oblast řešenou nařízením GDPR se uplatňovaly nadále.

Rozhodovací praxe ÚOOÚ z tohoto meziobdobí také naznačuje, že příchod GDPR neznamenal pro správce osobních údajů v ČR zvýšená rizika drakonických sankcí, jak bylo predikováno. Z výsledků ukončených kontrol zahájených již podle GDPR vyplývá, že se ÚOOÚ v tomto období držel s výší pokut spíše zvyklostí z dřívějších let. Volil často nápravná opatření a nevyužil ustanovení čl. 83 obecného nařízení k exemplárním finančním postihům.[45] Kromě snahy uklidnit atmosféru okolo GDPR hrála pravděpodobně svou roli i absence adaptačního zákona, která vyvolávala obavy, zda je ÚOOÚ kompetentní ukládat finanční postihy dle obecného nařízení.[46]

ETAPA III.

Vzhledem k tomu, že tato etapa započala až 24. dubna 2019, tj. jedenáct měsíců po účinnosti GDPR, byla již situace v problematice ochrany osobních údajů výrazně klidnější. Postupně byly vyvráceny mnohé mýty a fámy a pozornost se koncentrovala na jiná témata. Přelomové změny zaznamenaly pouze OVM z důvodu jejich bezprecedentního zbavení sankční odpovědnosti za porušení nařízení GDPR.

Samotná aplikace GDPR od započetí této etapy nevyvolává příliš otázek. Dispozitivní ustanovení GDPR, která byla vnitrostátní legislativou upravena, přestala působit výkladový

[44] Janečková, E. *GDPR: řešení problémů v praxi škol*. Praha: Grada Publishing, 2020, s. 13 (zdroj nepřesné informace). Právo pro praxi.
[45] *Úřad pro ochranu osobních údajů: Ukončené kontroly* [online]. [cit. 2021-03-11].
[46] Pattynová, J. Šest měsíců s GDPR: novinky a průběh kontrol dozorového orgánu. *PRÁVNÍ PROSTOR* [online]. ATLAS CONSULTING spol. s.r.o. [cit. 2021-02-26].

rozkol a jasněji nastavená pravidla obecně přispěla k nápravě některých narychlo připravených návodů a metodik. Jako příklad je možné uvést novelu již představeného metodického doporučení MŠMT. Nová verze publikovaná v této etapě přehodnotila některá klíčová doporučení. Blíže o počinu MŠMT pojednává kapitola 4.9.

3.4 Terminologie v oblasti ochrany a zpracování osobních údajů

Správné osvojení si základních pojmů a principů je klíčovým krokem k pochopení předmětného tématu. V následujících podkapitolách je vysvětleno nejen názvosloví používané v GDPR. Je-li to pro naplnění cílů práce významné, případně jedná-li se o úzce související terminologii, zaměřuje se popis i na pojmy definované jinými právními předpisy. Jsou rovněž reflektována specifická pravidla vztažená na oblast ochrany osobních údajů vzniklá jako průsečík ostatních zákonných i podzákonný právních předpisů.

Vlastní část práce zasazuje velkou část teoretického konstruktu této kapitoly přímo do prostředí školy a prakticky popisuje význam či aplikaci v rámci procesů zpracování. Proto je vhled do problematiky v níže uvedených podkapitolách spíše obecný.

3.4.1 Osobní údaje a jejich nositelé

SUBJEKT ÚDAJŮ

Pojem „subjekt údajů“ označovaný také jako „subjekt osobních údajů“ je v obecném nařízení skryt do vysvětlení pojmu „osobní údaj“. Extrahovaná definice říká, že subjektem údajů je *„identifikovaná nebo identifikovatelná fyzická osoba, kterou lze přímo či nepřímo identifikovat“.*[47] V ZOOÚ byl subjekt údajů označen jako *„fyzická osoba, k níž se údaje vztahují“*[48].

Člověk je identifikovatelný, tedy určitelný, dokáže-li je pomocí zpracovávaných údajů správce, zpracovatel, nebo kdokoliv další, identifikovat. Údaje nutné pro identifikaci nemusí mít nutně v držení sám správce, mohou být součástí veřejné databáze.

Recitál č. 26 GDPR upřesňuje, že potenciální identifikace dané osoby, byť nepřímá, musí být rozumná, resp. rozumně předpokládatelná. Nemůžeme ji tedy vykládat jako hypotetickou možnost, jejíž realizace by vyžadovala nepřiměřené úsilí, náklady, či běžně nedosažitelné technické prostředky.

[47] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* 2016, článek 4.

[48] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů*. Praha, 2020, částka 32, číslo 101, § 4, písm. d).

V pojetí nařízení GDPR je subjektem vždy konkrétní žijící fyzická osoba, podnikající fyzickou osobu nevyjímaje, která je občanem/rezidentem EU, potažmo EHP (působnost byla blíže vysvětlena v kapitole 3.3.2). Subjektem údajů nemůže být osoba právnická, je jím ale nepochybně fyzická osoba zastávající konkrétní roli v rámci osoby právnické (např. jednatel či předseda představenstva apod.).

OSOBNÍ ÚDAJ

Obecné nařízení definuje osobní údaj jako *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě“.* Jako příklady uvádí v čl. 4, že určitý identifikátor je např. „*jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*.

Jde o výčet čistě demonstrativní. Pojem „osobní údaj“ je třeba chápat jako libovolný údaj (informaci nebo soubor údajů či informací), který sám o sobě nebo v kontextu s jinými údaji, byť správcem či zpracovatelem nezpracovávanými, vede k přímému ztotožnění osoby nebo k identifikaci subjektu alespoň nepřímo napomáhá.

Proto je zcela nemožné pokusit se optikou obecného nařízení o sestavení taxativního výčtu osobních údajů. Definice je natolik obecná, že správci musí tento fakt pečlivě zohlednit při analýze procesů zpracování. Je vhodné uvažovat logikou vyloučení zpracovávané informace z množiny údajů, nežli obráceným postupem zařazovat údaje až v případě, že prokazatelně naplňují definici osobního údaje. Teprve informace, která zcela nesporně nemůže ani při doplnění o další údaje napomoci k identifikaci fyzické osoby, není osobním údajem.

Je zjevné, že okruh osobních údajů dalece překračuje hranice obvyklého vnímání způsobilosti vypovídat o jedinečnosti subjektu. Pokud se omezíme na přímé identifikátory, jakými je například jméno, e-mail, telefonní číslo, rodné číslo, adresa, otisk prstu či vzorek DNA, uniknou nám souvislosti vzájemné kombinace nepřímých identifikátorů, které společně zajistí jednoznačnou identifikaci subjektu.[49] Typicky údaje o výšce, věku, barvě vlasů a modelu osobního automobilu s velkou pravděpodobností povedou k identifikaci osoby v rámci užší skupiny osob, přestože jednotlivě bez doplnění o další informaci tohoto schopny nejsou.

[49] Novák, D. *Zákon o ochraně osobních údajů a předpisy související*. Praha: Wolters Kluwer, 2014, s. 88. Komentáře (Wolters Kluwer ČR).

Osobní údaj však může mít charakter nejen informace objektivní (např. výška osoby či barva vlasů), ale i subjektivní (např. názor či hodnocení osoby), přičemž není nezbytné, aby informace byla přesná, prokázaná či pravdivá.[50]

Termín osobní údaj se ve smyslu soukromého práva hmotného do jisté míry prolíná s projevem osobní povahy, jedná se však o termín daleko širší, jelikož projev osobní povahy zahrnuje především údaje vytvořené fyzickou osobou. Ve vybraných situacích se paralelně s právem na ochranu osobních údajů použije i právo na ochranu soukromí řadící se dle občanského zákoníku mezi práva na ochranu osobnosti.[51] Vhodným příkladem, který bude popsán v praktické části, je zachycení podobizny člověka, kterou primárně upravuje HLAVA II, Oddíl 6, občanského zákoníku.

Identifikovat správně osobní údaj je pro správce naprosto zásadním úkolem, musí totiž správně určit, zda se nejedná o údaj z tzv. zvláštní kategorie, ke které přistupuje odlišně z důvodu velmi přísných pravidel zpracovávání těchto údajů.

ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ

Zvláštní kategorie, dříve označovaná jako „**citlivé osobní údaje**“, je podmnožinou osobních údajů. Pravidla pro zpracování těchto údajů jsou natolik specifická a pevně vymezená, že je třeba věnovat správnému zařazování osobních údajů do této kategorie obrovskou pozornost. V případě nejasností je vhodné zacházet s údajem jako s citlivým, resp. zařadit jej v případě pochybnosti do zvláštní kategorie.

Nařízení GDPR, jak již predikuje jeho název, tedy „obecné nařízení o ochraně osobních údajů“, je velmi obecné. Neobsahuje příliš taxativních výčtů, avšak čl. 9 *„Zpracování zvláštních kategorií osobních údajů“* je výjimkou. V odstavci 1 definuje zmíněnou kategorii údajů zcela taxativně, resp. kogentně stanovuje okruhy údajů a výjimky, podle kterých je jejich zpracování přípustné. Jedná se o údaje, které *„vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby“*.[52]

[50] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.1.4. Právní monografie (Wolters Kluwer ČR).
[51] Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2012, částka 33, číslo 89, HLAVA II, Oddíl 6 - Osobnost člověka.
[52] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* 2016, čl. 9, odst. 1.

Do českého právního řádu nevnáší GDPR ve vztahu ke zvláštní kategorii údajů žádnou podstatnou změnu. Směrnice 95/46/ES sice neobsahovala tento přesný výčet, absentovaly genetické a biometrické údaje, ovšem ty zahrnoval mezi citlivé údaje náš zákon o ochraně osobních údajů.[53]

Obecně lze zvláštní kategorii údajů, tedy citlivé údaje, charakterizovat jako množinu osobních údajů, které mohou subjekt údajů samy o sobě poškodit ve společnosti, zaměstnání, ve škole apod. a mohou zapříčinit jeho diskriminaci.[54]

V prostředí OVM obvykle nevyvolává zpracování citlivých údajů velké otázky, protože je naprostá většina osobních údajů ze zvláštní kategorie zpracovávána z důvodu plnění právní povinnosti. Důležité je nastavení přísnějších pravidel pro zabezpečení agend, ve kterých jsou tyto údaje zpracovávány a dohlížet na účely, pro které jsou zpracovávány. Ty jsou, stejně jako výčet typů citlivých osobních údajů, uvedeny v obecném nařízení taxativně.

Konkrétně je možné osobní údaje ze zvláštní kategorie zpracovávat, pokud:

a) *subjekt údajů udělil výslovný souhlas;*
b) *zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany;*
c) *zpracování je nutné pro ochranu životně důležitých zájmů;*
d) *zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle;*
e) *zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;*
f) *zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;*
g) *zpracování je nezbytné z důvodu významného veřejného zájmu;*
h) *zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče;*
i) *zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění*

[53] Pattynová, J., Suchánková, L., Černý, J., Růžička, M. *Obecné nařízení o ochraně osobních údajů (GDPR)*. Praha: Leges, 2019, s. 127. Komentátor.
[54] Nezmar, L. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017, s. 35. Právo pro praxi.

přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků;

j) zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely.[55]

Článek 9 obecného nařízení výjimky, pro které je zpracování citlivých údajů povoleno, ještě více detailizuje.

RODNÉ ČÍSLO

Rodné číslo je velmi specifický osobní údaj, který ovšem z pohledu nařízení GDPR nepožívá žádné zvláštní ochrany. Klíčová jsou pro správce pravidla stanovená zákonem o evidenci obyvatel, jenž upravuje podobu rodných čísel, způsob jejich přidělování, a především omezuje přípustné případy zpracování rodných čísel.[56] Je nutno uvést, že byť rodné číslo nepatří do zvláštní kategorie osobních údajů, je mezi citlivé údaje laickou veřejností občas mylně zařazováno.

I když obecné nařízení i adaptační zákon specifická pravidla pro nakládání s rodnými čísly nestanovují, je důležité při jejich zpracování přijmout vhodná opatření a zejména posoudit nezbytnost s jejich nakládáním, tedy zda neexistuje méně invazivní způsob identifikace osoby postačující naplnění účelu zpracování.

Z rodného čísla lze vyčíst nejen datum narození a s tím související věk fyzických osob, ale rovněž pohlaví subjektu. Ne vždy jsou všechny tyto údaje nezbytné a jejich zpracování porušuje zásadu minimalizace (blíže vysvětleno v kapitole 3.5.3).

Za základ zvláštních podmínek zpracování rodných čísel ve smyslu nařízení GDPR lze považovat ustanovení, podle něhož je možné rodná čísla využívat jen *„a) jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy a soudů vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřebu vedení Centrální evidence závětí, b) stanoví-li tak zvláštní zákon, nebo c) se souhlasem nositele rodného čísla nebo jeho zákonného zástupce“.*[57]

[55] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů*. 2016, článek 9, odst. 2.
[56] Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2000, částka 39, číslo 133.
[57] Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2000, částka 39, číslo 133, § 13c, odst. 1.

3.4.2 Zpracování osobních údajů, role ve zpracování

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Pro správce je mnohdy důležitější poznat, co není zpracováním osobních údajů, než co jím je. Je to zejména z těchto důvodů:

a) Není-li nějaká činnost prováděná správcem klasifikována jako zpracování osobních údajů, nevztahují se ni přísná pravidla daná nařízením GDPR či ZZOÚ (dopad jiné právní úpravy není pochopitelně vyloučen).
b) Zapojí-li správce do operací s daty externí subjekt, přičemž takto prováděná činnost není zpracováním osobních údajů ve smyslu nařízení GDPR, není nutné upravovat vztah zpracovatelskou smlouvou, která vzhledem ke konsekvencím spolupráce mezi správcem a zpracovatelem obvykle zvyšuje nároky na prováděné procesy a s tím mnohdy souvisí zvýšené náklady a nároky na čas.

Zpracováním osobních údajů je dle obecného nařízení *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. “*[58]

Za zpracování by mohlo být dle uvedené definice považováno téměř jakékoliv představitelné nakládání s osobními údaji. Jedná se navíc o demonstrativní výčet, který může v budoucnu doznat důsledkem rozvoje ICT dalších změn, které autoři GDPR v době jeho vniku nemohli předvídat.

Problematiku zpracování je však třeba vnímat v širším kontextu a spatřovat analogii s definicí uvedenou v ustanovení § 4 v dříve platném zákoně o ochraně osobních údajů. Praxe v posuzování operací prováděných s osobními údaji se dle aktuálního vyjádření dozorového úřadu významně s příchodem GDPR od tohoto pojetí neodklonila.[59]

Zpracování ve smyslu obecného nařízení nelze definovat jako libovolné nakládání s osobními údaji, je třeba jej chápat jako již sofistikovanější proces prováděný

[58] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4, odst. 2).
[59] Nejdůležitější pojmy: Definice pojmů jsou obsaženy v článku 4 odst. 1 obecného nařízení. *Úřad pro ochranu osobních údajů* [online]. kapitola "Co je zpracování osobních údajů?", 2. odstavec [cit. 2021-01-30].

správcem systematicky s určitým cílem, tedy pro naplnění konkrétního účelu zpracování. Nelze tak za zpracování paušálně označit veškeré nahodilé operace s daty. Nakládání s osobními údaji, které výkladem této definice za zpracování neoznačíme, nebude upravovat nařízení GDPR, avšak ochranu dat bude obvykle pokrývat jiný právní předpis, například občanský zákoník.[60]

Zcela praktickým případem nahodilého přístupu k osobním údajům, který není považován za zpracování osobních údajů, je nahlížení do osobních dokladů či různých průkazů za účelem ověření totožnosti subjektu. Při této činnosti je sice k osobním údajům přistupováno a je dle nich prováděna jednoznačná identifikace subjektu, nicméně nedochází-li k opisování údajů nebo dokonce ke kopírování dokladů, které je většinou dokonce nepřípustné, o zpracování dle GDPR nejde. Rovněž fotografování osob nebude obvykle zařazeno mezi operace zpracování, nedochází-li k následnému propojování zachycených subjektů s dalšími identifikátory nebo nejsou-li fotografie používány k systematickému ztotožňování osob (blíže viz kapitola 4.6).

Správná identifikace činností, které mají být klasifikovány jako zpracování osobních údajů, na které se aplikuje GDPR, je základem každé vstupní analýzy zpracování údajů.

SPRÁVCE OSOBNÍCH ÚDAJŮ

Správce má ve vztahu k činnostem prováděným s osobními údaji tu **nejdůležitější roli**, ostatně napříč celým nařízením GDPR je většina povinností a pravidel adresována právě správcům. Dle nařízení GDPR se za správce považuje *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů“*.[61]

Tímto vymezením tzv. osobní působnosti a rovněž upřesněním okruhu věcné působnosti jsou poměrně jednoznačně charakterizováni adresáti právního předpisu. V praxi to znamená, že dopadá na veškeré subjekty zpracovávající osobní údaje bez ohledu na jejich formu či zda taková osoba disponuje právní subjektivitou.[62]

To mj. vysvětluje nutnost určení vybraných orgánů veřejné moci za samostatné správce, i když jsou např. umístěny podřízeně v určité hierarchii, nemají vlastní právní

[60] Nejdůležitější pojmy: Definice pojmů jsou obsaženy v článku 4 odst. 1 obecného nařízení. *Úřad pro ochranu osobních údajů* [online]. [cit. 2021-01-30].
[61] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4, odst. 7).
[62] Janečková, E. *GDPR: řešení problémů v praxi škol*. Praha: Grada Publishing, 2020, s. 23. Právo pro praxi.

subjektivitu, ale fakticky jsou samostatným orgánem vykonávajícím vlastní působnost. **Správcem může být i čistě soukromá fyzická osoba, tedy osoba nepodnikající,** neprovádí-li zpracování výhradně pro osobní účely.

Je-li nějaká společnost, organizace či firma fyzicky rozdělena na menší části či umístěna na několika místech, vystupuje-li navenek jako jeden subjekt práva, je rovněž jedním správcem osobních údajů. Jednotlivá oddělení, odbory, pracoviště a všichni zaměstnanci jsou společně jedním uskupením a jedním správcem osobních údajů. Toto je třeba zdůraznit zejména pro správné označování zpracovatelů (pojem vysvětlen níže), kdy byli za zpracovatele toliko označovány chybně například ekonomická či účetní oddělení jedné společnosti, přestože nevystupovaly jako externí subjekt.

V souvislosti s rolí správce a níže popisovanou úlohou zpracovatelů je žádoucí zmínit ještě specifický režim spolupráce dvou subjektů podílejících se na zpravování. Tím je tzv. společné správcovství, tedy situace, kdy není ani jedna strana v postavení zpracovatele, na příslušné agendě zpracování tyto dva správci úzce spolupracují a vůči subjektům vystupují v podstatě jako jeden správce osobních údajů. Smluvně si ve smlouvě o společném správcovství rozdělí povinnosti a vymezí podíly na odpovědnosti.

ZPRACOVATEL OSOBNÍCH ÚDAJŮ

Zpracovatel je nařízením GDPR definován jako *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce“*.

Pokud se tedy správce rozhodne svěřit určitou činnost, při které bude docházet ne k nahodilému přístupu, ale k systematickému zpracovávaní údajů, stává se tento externí subjekt „zpracovatelem osobních údajů“. Není-li takový zpracovatel určen přímo právním předpisem, je nutné mezi správcem a zpracovatelem vytvořit smluvní vztah, a to písemný. Případnému zapojení dalšího zpracovatele ze strany již existujícího zpracovatele, tedy vzniku tzv. sub-zpracovatele, musí rovněž předcházet písemné schválení ze strany správce.

Správce je odpovědný za své zpracovatele, musí je vybírat pečlivě a kontrolovat, zda dodržují stanovená pravidla a zda poskytují odpovídající záruky.[63]

V praxi je někdy nesnadné kontrolovat velké zpracovatele poskytující například cloudové služby (typicky společnosti jako Google nebo Microsoft), nicméně není-li si správce jist, do zpracování je zapojit nesmí a musí hledat jiné technické prostředky či externí

[63] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 28.

poskytovatele služeb pro své procesy zpracování (praktická část je v kapitole 4.7 doplněna o zcela konkrétní příklady zpracovatelů v prostředí škol).

PŘÍJEMCE OSOBNÍCH ÚDAJŮ

Tento často opomíjený, přitom zcela klíčový pojem, mnohdy uniká odpovídající pozornosti pověřenců i samotným správcům. Přitom vnitřní předpisy tvořené jako jedny z technickoorganizačních opatření musí ve vztahu k zaměstnancům řešit aspekty poskytování informací, zejména pak osobních údajů, mnohem detailněji, než je třeba věnovat problematice určování zpracovatelů.

Poskytuje-li jakékoliv osobní údaje správce nebo zpracovatel na základě pověření jakémukoliv subjektu, stává se tento příjemcem. Výjimku tvoří pouze zákonem určení příjemci (vysvětlení je obsaženo přímo v níže uvedené definici). Drtivá většina zaměstnanců nemá v rámci plnění svých povinností v gesci tvorbu zpracovatelských smluv nebo obecnou kontrolu zpracovatelů. Dohled nad činnostmi správce je ještě více na odpovědnosti jen malé skupiny osob převážně z řad vedení. Poskytování informací je ovšem náplní práce někdy i většiny zaměstnanců pracujících pro konkrétního správce. Tito by měli být velmi dobře obeznámeni s pravidly pro předávání informací a měli by být schopni identifikovat, kdo je jejich oprávněným příjemcem, resp. zda subjekt, kterému údaje poskytují, je oprávněn je získat a zda neporuší pravidla, poskytnou-li taková data jménem správce, tedy jménem svého zaměstnavatele.

V nařízení GDPR se uvádí, že příjemcem je *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují“*.[64]

3.4.3 Profilování, pseudonymizace, anonymizace

PROFILOVÁNÍ

Tento pojem si zaslouží vysvětlení zejména z důvodu, že právě profilování je obecným nařízením relativně přísně regulováno. Problematika profilování je však natolik obsáhlá, že je pro potřeby této práce zobecněna jen pro pochopení navazujících doporučení v analyticko-praktické části popisem základních rozpoznávacích znaků profilování.

[64] *Ibid.,* čl. 4, odst. 9).

Dle nařízení je profilováním *„jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu“*.[65]

Za profilování můžeme tedy označit zpracování osobních údajů, splňuje-li dva pojmové znaky. Prvním je **automatizované zpracování**, kterým je v praxi jakékoliv zpracování prováděné pomocí technických prostředků, zejména prostřednictvím výpočetní techniky. Nevztahuje se na zpracování prováděné úplně nebo částečně manuálně v analogové (listinné) podobě. Druhým atributem je následné **použití zpracovaných dat k hodnocení** určitých osobních aspektů fyzické osoby, přičemž jejich výčet (viz výše uvedená definice) dává velký prostor pro celou škálu údajů.

Typicky se jedná o sledování aktivit uživatelů webových stránek (například pomocí tzv. cookies souborů[66]) a způsobu jejich chování. Provozovatel webu, zároveň správce osobních údajů, takto profiluje například údaje o návštěvnících e-shopů nebo zpravodajských webů s cílem ovlivnit jejich chování.

Ve vztahu k profilování je vhodné uvést, že definici nenaplňuje například profilování žáků škol ve smyslu hodnocení jejích výkonů slovně či běžným známkováním, leda že by bylo plně automatizováno, což je v současné době nepředstavitelné. Rovněž profilování uchazeče o zaměstnání nelze přímo slučovat s profilováním dle významu pojmu v GDPR. Jedná se sice o zpracování osobních údajů, avšak nikoliv plně automatizované.

PSEUDONYMIZACE

Pseudonymizace je jeden z mála pojmů GDPR, který nebyl upraven dřívější legislativou. Nebyl definován směrnicí 95/46/ES a nepracoval s ním ani ZOOÚ. To ovšem neznamená, že by se pseudonymizace dříve nevyužívala, jen se pro ni mnohdy nesprávně používal níže vysvětlený pojem anonymizace.

Obecné nařízení definuje pseudonymizaci jako *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická*

[65] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4, odst. 4).

[66] krátké textové soubory, který prostřednictvím internetového prohlížeče ukládá webová stránka do zařízení návštěvníka stránky

a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“.[67]

Pseudonymizace je hojně používaný a zcela přirozený postup při mnoha činnostech prováděných správci. Příkladem budiž situace, kdy jsou odesílány genetické vzorky do laboratoře, přičemž jméno subjektu je nahrazeno pořadovým číslem či jiným jedinečným identifikátorem. Po obdržení výsledku z laboratoře jsou tyto přiděleny zpět ke konkrétnímu subjektu osobních údajů. Během transportu/přenosu je tak zcela eliminováno riziko zneužití jakýchkoliv informací. Dalším obecným příkladem je šifrování dat nebo obdobné zabezpečení klíčem potřebným pro zpětné převedení.

Pseudonymizovaná data jsou chráněna, pokud je zajištěno oddělení konkrétních osobních údajů od klíčů, kterými jsou nahrazeny/zabezpečeny. Také pseudonymizovaná data tak lze za jistých podmínek zneužít, nebude-li zajištěna dostatečná ochrana prostředků či údajů nutných k jejich zpětnému spojení s konkrétními subjekty osobních údajů (např. zpřístupnění špatně zabezpečeného hesla k zašifrovanému souboru).

Praktické příklady pseudonymizace jsou uvedeny v kapitole 4.8.

ANONYMIZACE

Anonymizace je na rozdíl od předchozího pojmu zakotvena nepřímo v právní úpravě regulující nakládání s osobními údaji již od devadesátých let. Konkrétně při explanaci pojmu anonymní údaj vysvětluje směrnice 95/46/ES, že na anonymní údaje se již nevztahují zásady zpracování, tedy jedná se fakticky o opak pojmu „osobní údaj“.[68]

Zákon o ochraně osobních údajů definoval zcela konkrétně význam pojmu „anonymní údaj“ jako „*takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů“.*[69]

Protože se tato deskripce překrývá s již vysvětlenou pseudonymizací, upřesňuje nařízení ve svých recitálech anonymní informace jako „*informace, které se netýkají identifikované či identifikovatelné fyzické osoby“*, logicky se tak na ně nevztahují zásady

[67] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 4, odst. 5).
[68] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995. In: *EUR-Lex*. Lucemburk, 1995, Úř. věst. L 281, Svazek 015, 95/46/ES, recitál (26).
[69] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů*. Praha, 2020, částka 32, číslo 101, § 4, psím. c).

ochrany osobních údajů. Recitál 26 také výslovně uvádí, že se nařízení GDPR netýká zpracování anonymních informací.[70]

Proces anonymizace představuje úpravu osobních údajů způsobem, který je zbaví vypovídací hodnoty, tedy eliminuje všechny způsoby, jak vrátit těmto údajům identifikační schopnost napomáhající přiřazení informace ke konkrétní fyzické osobě.

Nelze pochopitelně tvrdit, že je toto zcela absolutní a nezvratný proces. Nařízení GDPR vychází z premisy, že za použití myslitelných a předpokládatelných technických a finančních prostředků včetně dostupných technologií nelze předpokládat proveditelnost rekonstrukce anonymizovaných dat do podoby osobních údajů. Pokud by taková obnova byla teoreticky možná, ať již ze strany správce nebo třetí osoby, bude se jednat nikoliv o anonymní či anonymizovaný údaj, ale o osobní údaj s atributem „pseudonymizovaný".

Praktické příklady pseudonymizace jsou uvedeny v kapitole 4.8.

3.4.4 Problematika pověřence a postavení školy jako orgánu veřejné moci

Pro pochopení důvodů, proč musí školy a školská zařízení povinně jmenovat pověřence, spojuje tato podkapitola dvě ne příliš související problematiky, a to pověřence pro ochranu osobních údajů a postavení škol a školských zařízení jako orgánů veřejné moci.

JMENOVÁNÍ POVĚŘENCE

Institut pověřence není vůbec nový, respektive neobjevil se až s příchodem GDPR. Pověřence, v originální anglické verzi GDPR označovaného jako „data protection officer" (DPO), znala již směrnice 95/46/ES. Ta jej definovala jako „personal data protection official", tedy jako osobu pověřenou ochranou osobních údajů. Její jmenování bylo dobrovolné, umožňovala-li to však vnitrostátní úprava.[71]

Zakotvení institutu pověřence v zákoně implementujícím dotčenou směrnici využilo pouze pět zemí, konkrétně Německo, Nizozemí, Švédsko, Lucembursko a Francie.[72]

Česká republika ve svém ZOOÚ s pověřencem nepočítala, místo toho byla zachována povinnost oznamovat zpracování osobních údajů dozorovému úřadu.

---

[70] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 26.

[71] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995. In: *EUR-Lex*. Lucemburk, 1995, Úř. věst. L 281, Svazek 015, 95/46/ES, čl. 18, odst. 2.

[72] Mole, A., Stella, D., Boardman, R. *DPO in Europe* [online]. Bird & Bird [cit. 2021-02-18].

Aktuální široký okruh správců povinných jmenovat pověřence byl s blížící se účinností GDPR velmi často kritizován, přitom kromě nepatrně zvýšených nákladů, které však nemusí být nijak vysoké, jak bude vysvětleno v analytické části, jde naopak o určité zjednodušení. Se zavedením funkce pověřence souvisí právě zrušení oznamovací povinnosti a správce má mnohem jednodušší situaci při zahajování činností zpracování.

Směrnice z 90. let dokonce výslovně hovořila o zjednodušení nebo o úplné výjimce z oznamovací povinnosti, *„pokud správce určí, v souladu s vnitrostátním právem, kterému podléhá, osobu pověřenou ochranou údajů, který je zejména pověřen“.*[73]

V nařízení GDPR je pověřenec zakotven kogentně pro vymezený okruh správců. Vzhledem k ne zcela jednoznačné definici okruhu toto téma vyvolávalo velké diskuse.

V článku 37 obecného nařízení je uvedeno, že správce nebo zpracovatel jmenují pověřence pro ochranu osobních údajů, pokud „*zpracování provádí orgán veřejné moci či veřejný subjekt“,* pokud *„hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů“*, nebo pokud „*hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů“*[74]

Interpretační nejasnosti vyvolával pro české právo ne zcela obvyklý pojem „veřejný subjekt“, který při extenzivním výkladu zahrnoval mezi správce povinné jmenovat pověřence v podstatě každou organizaci, společnost, příspěvkovou organizaci atp., pokud byla vlastněna či zřízena orgánem veřejné moci nebo financována většinově z veřejného rozpočtu. To v konečném důsledku směřovalo k povinnosti jmenování pověřence i ze strany obecních příspěvkových organizací, jako jsou muzea či knihovny, přestože tyto nejsou v postavení orgánu veřejné moci a jmenování pověřence z jejich strany nemá obvykle žádný praktický přínos.

Problematiku částečně vyjasnil adaptační zákon, který okruh povinných správců upravil na *„orgány veřejné moci a orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu“*.[75]

---

[73] viz 71

[74] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, článek 37.

[75] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 14.

POSTAVENÍ A ÚKOLY POVĚŘENCE

Nařízení GDPR vyžaduje po správci, aby pověřence zapojil do všech procesů souvisejících s ochranou osobních údajů dostatečně včas, musí mu poskytnout nezbytné zdroje pro plnění úkolů, zajistit přístup k údajům a podpořit jeho odborné vzdělávání. V souvislosti s plněním jeho úkolů ho správce či zpracovatel nesmí ovlivňovat, ani sankcionovat nebo zbavit funkce. Pochopitelně tím není vyloučen postih při nedodržování smluvních závazků či zákoníku práce, je-li pověřenec v pracovně-právním vztahu. V rámci plnění svých úkolů pověřenec poskytuje informace a poradenství účastníkům zpracování, sleduje soulad s obecným nařízením a dalšími právními předpisy. Je rovněž kontaktní osobou pro dozorový úřad a zejména pro subjekty údajů, přičemž se podílí na výkonu jejich práv.[76]

Při své činnosti se nesmí dostat do střetu zájmu, tedy nesmí se například podílet sám na zpracování, na které má dohlížet.

ŠKOLA V POSTAVENÍ ORGÁNU VEŘEJNÉ MOCI

Dle školského zákona mají ředitelé[77] škol a školských zařízení povinnost rozhodovat v souladu se správním řádem ve správním řízení. Tato povinnost se po novele školského zákona účinné od 1. května 2015 týká nejen veřejných škol, ale i škol soukromých a církevních.[78] Všechny školy a školská zařízení jsou tedy orgány veřejné moci ve smyslu zákon č. 111/2009 Sb., o základních registrech (dále také jako „zákon o základních registrech"), který definuje OVM jako *„státní orgán, územní samosprávný celek, fyzickou nebo právnickou osoba, byla-li jí svěřena působnost v oblasti veřejné správy, notáře, soudní exekutory a archiv*“.[79] V souladu s tímto zákonem jsou vedeny v základním registru práv a povinností školy jako orgány veřejné moci. [80]

POVINNOST ŠKOLSKÉHO ZAŘÍZENÍ JMENOVAT POVĚŘENCE

Vzhledem k výše uvedenému je nesporné, že jsou všechny školy (včetně mateřských) a školská zařízení povinny jmenovat pověřence. Je dokonce zřejmé, že pověřence musí

[76] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, článek 38-39.

[77] V zájmu genderově vyvážené kultury vyjadřování je pro účely této práce pojem „ředitel“ dále chápán vždy jako statutární zástupce školy, kterým je ředitelka či ředitel školy. Není-li výslovně uvedeno jinak, jsou analogicky vnímány i další označení osob bez ohledu na fakt, zda je v dané pozici, postavení či funkci žena nebo muž.

[78] Zákon č. 561/2004 Sb., o předškolním, základním středním, vyšším odborném a jiném vzdělávání (školský zákon). In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2004, částka 190, číslo 561, § 165, odst. 2).

[79] Zákon č. 111/2009 Sb., o základních registrech. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2009, částka 33, číslo 111, § 2, odst. c); § 50.

[80] *Správa základních registrů : Informační systém základních registrů (ISZR)* [online]. [cit. 2021-01-03].

jmenovat například i Dům dětí a mládeže (DDM), protože se jako školské zařízení pro zájmové a další vzdělávání nachází rovněž v pozici orgánu veřejné moci. Konkrétně mu přísluší rozhodování o přijímání ke vzdělávání a další rozhodování o právech a povinnostech dětí, žáků a studentů. Mezi samostatné OVM jsou dle záznamů v základních registrech zařazeny dokonce i školní jídelny, jsou-li samostatnou příspěvkovou organizací, tedy nejsou-li součástí školy. Vzhledem ke standardně přiřazeným činnostním rolím však fakticky veřejnou moc nevykonávají.

Že není v problematice jmenování pověřenců ze strany školských zařízení do dnešního dne zcela jasno, však dokládá stále publikované (i přes upozornění na chybu již v roce 2019) vyjádření ÚOOÚ ze dne 19. října 2018. Mezi zpracování, která nepodléhají povinnosti jmenovat pověřence, náleží dle ÚOOÚ *„běžné provozní činnosti domů dětí a mládeže, školních jídelen…“*.[81] Ani tato informace, byť je uveřejněna na oficiálních stránkách dozorového úřadu, však povinnosti jmenovat pověřence dotčené organizace nezbavuje a pozice DDM jako OVM je nesporná.

3.5 Zásady a zákonnost zpracování osobních údajů

V následujících podkapitolách budou vysvětleny hlavní zásady zpracování osobních údajů, které představují interpretační principy pro výklad dalších ustanovení obecného nařízení. Přestože porušení těchto zásad podléhá sankcím, neměla by hrozba postihu být tou primární motivací pro dodržování pravidel. Jejich pochopení ve vzájemných souvislostech je rozhodné pro reálné naplnění smyslu GDPR.

3.5.1 Zásada zákonnosti, korektnosti a transparentnosti

Tuto zásadu je vhodné rozdělit na tři samostatné zásady a vykládat je zcela odděleně. Klíčovou roli pro aplikaci celého obecného nařízení má zásada zákonnosti následovaná zásadou transparentnosti, což nijak zásadně nesnižuje význam korektnosti zpracování.

ZÁSADA TRANSPARENTNOSTI

Tuto zásadu je třeba vykládat jako povinnost správce transparentním způsobem informovat subjekty o zpracování jejich osobních údajů. V praxi se tato zásada naplňuje vydáním souboru informací a pravidel nazývaného obvykle jako „informační memorandum“, „zásady zpracování osobních údajů“, případně „poučení o zpracování

[81] *K povinnosti jmenovat pověřence vybranými městskými a krajskými organizacemi* [online]. [cit. 18. 02. 2021].

osobních údajů“. Tyto informace o zpracování jsou základním institutem pro realizaci práva subjektu na informace.[82] Detailněji je popsáno v podkapitole 3.6.1.

Transparentní přístup správce k subjektu vystihuje i způsob, jakým správce připravuje či distribuuje informace pro subjekty. Spočívá také ve správném poučení subjektu o rozsahu jeho práv a o možnostech jejich uplatnění. Poskytované informace by měly být srozumitelné i pro laika neorientujícího se v problematice práva (psány jednoduchými a jasnými jazykovými prostředky) a měly by být jednoduše dostupné – typicky dálkovým přístupem na webových stránkách správce nebo ve stručné listinné podobě při osobním kontaktu správce a subjektu.

ZÁSADA KOREKTNOSTI

Na zásadu korektnosti lze nahlížet jako na určitý morální statut správce. Smyslem není jen striktní dodržování kogentních ujednání právních norem, ale zejména etický a lidský přístup k problematice ochrany osobních údajů. Při zpracování osobních údajů je třeba zohlednit dopad na jednotlivé konkrétní fyzické osoby. Přestože by zpracování osobních údajů v rámci jedné agendy splňovalo veškeré zásady a náležitosti legislativy upravující ochranu a zpracování osobních údajů ve vztahu k 99 subjektům ze 100, je přístup správce nekorektní, pokud nepřiměřeně zasahuje do práv či svobod, byť jen jediného subjektu.

ZÁSADA ZÁKONNOSTI

Jde o nejobsáhlejší zásadu GDPR. Pro správce provádějící implementaci GDPR je pochopení této zásady doplněné o právní důvody zpracování kritické.

Pro dodržení zákonnosti zpracování je třeba posuzovat kombinaci tří aspektů nakládání s osobními údaji. Je nutno **určit účel**, pro který dochází ke zpracování, nalézt či **zajistit právní základ daného zpracování** a **vymezit okruh dotčených osobních údajů**, který musí být přiměřený tomuto účelu a podložený právním základem.[83]

V praxi to znamená, že zpracování osobních údajů je možné provádět na základě alespoň jednoho právního důvodu zpracování, a to transparentně vůči subjektu a zároveň korektně. Správce musí zacházet s údaji způsobem, který nemá pro subjekt nepříznivé důsledky.

[82] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 39.
[83] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.4.5. Právní monografie (Wolters Kluwer ČR).

Osobní údaje nelze zpracovávat, pokud tato obecná podmínka zákonnosti vystavěná na jednotlivých dále uvedených právních důvodech není splněna. Vzájemná kombinace některých z níže uvedených právních důvodů je běžná v rámci jediného zpracování, některé pro jedno zpracování naopak kumulovány být nesmí, typicky souhlas se zpracováním osobních údajů.

Problematika právních důvodů zpracování bývá někdy nesprávně zaměňována s účely zpracování. Pro detailnější pochopení prozatím postačí znalost základního principu započetí zákonného zpracování, pro které je třeba **mít účel** zpracování a legitimní **právní titul**.

Účely definuje správce a jsou jimi standardně určité cíle, ke kterým zpracování osobních údajů směřuje (například sběr údajů a jejich následné zpracování pro účely vedení mzdové agendy, pro účely přijímání do pracovního poměru, pro komunikaci s dodavateli, pro zajištění bezpečnosti osob a informací, pro výkon školní matriky atd.). Pro naplnění účelů je zapotřebí disponovat určitým rozsahem informací o subjektu, které budou zahrnovat téměř bez výjimky i osobní údaje.

Výčet účelů je prakticky nekonečný a těmi nejdůležitějšími ve vztahu k činnostem školy se práce věnuje v analyticko-praktické části v kapitole 4.1.

Právních titulů však není nekonečně mnoho. Nařízení GDPR jich taxativně definuje pouze šest a jejich správné určení je základních požadavkem pro legitimní zpracování osobních údajů.

ZÁKONNOST ZPRACOVÁNÍ DLE ČLÁNKU 6 OBECNÉHO NAŘÍZENÍ

Výčet právních důvodů zpracování je zde uveden bez detailního rozboru pouze pro návaznost na zásadu zákonnosti. Protože je identifikace právního důvodu zpracování prováděna obvykle v průběhu analýzy zpracování, je materie zákonnosti zpracování dle článku 6 obecného nařízení detailněji rozpracována spolu se zcela konkrétními a praktickými příklady v analytické části v kapitolách 4.1.1 až 4.1.6.

Nařízení GDPR označuje zpracování za zákonné, je-li splněna alespoň jedna z těchto podmínek a pouze v odpovídajícím rozsahu:[84]

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

[84] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1.

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

3.5.2 Zásada účelového omezení

Podle této zásady musí být osobní údaje *„shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný“*. [85]

Výjimku pro následné operace s osobními údaji, které nejsou považovány za neslučitelné, tvoří zpracování prováděné *„pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely“*.[86]

Správce tak musí již při shromáždění údajů jasně stanovit, pro jaký účel je shromažďuje. Tento účel musí mít legitimní charakter (v souladu s právním řádem[87]) a musí být rovněž určitý a výslovně vyjádřený. Z této zásady vyplývá, že s osobními údaji nesmí být následně nakládáno způsobem, který je s takto stanovenými účely neslučitelný a pro subjekty nepředvídatelný. Nařízení GDPR rozšiřuje podmínky zpracování bez posuzování slučitelnosti účelu, nicméně se jedná spíše o dispozitivní formulace, které by měly být upraveny vnitrostátním předpisem.

ZZOÚ reaguje na prostor pro úpravu dopadu obecného nařízení výjimkami z povinnosti posuzování slučitelnosti, je-li zpracování osobních údajů prováděno při zajišťování chráněných zájmů, kterými jsou například ochranné a bezpečnostní zájmy České republiky, veřejný pořádek, vnitřní bezpečnost, veřejný zájem EU nebo členského státu EU atd. Důležitá je explicitně uvedená výjimka při ochraně veřejného zdraví nebo

[85] *Ibid.*, čl. 5, ods. 1, písm. b).
[86] *Ibid.*, čl. 6, odst. 1.
[87] právní řád v širokém významu, tedy včetně veškerých zákonných i podzákonných norem, vyhlášek, nálezů Ústavního soudu a ústavních principů

v rámci sociálního zabezpečení, což je obzvláště v době nutnosti přijímání tvrdých opatření při boji s infekčními chorobami klíčový institut. ZZOÚ rovněž připouští prolomení zásady účelového omezení při zpracování v rámci úkolu prováděného ve veřejném zájmu, stanoveného právním předpisem nebo při výkonu veřejné moci, kterým je správce pověřen.[88]

3.5.3 Zásada minimalizace údajů

Minimalizací osobních údajů je myšleno přiměřené a relevantní omezení na zcela nezbytný rozsah ve vztahu k účelu, pro něž jsou zpracovávány.[89] Tato zásada je typickým příkladem navazujícím na samu podstatu obecného nařízení, tedy na princip odpovědnosti správce za zpracování a na přístupu založeném na riziku zpracování. Správce sám rozhoduje o tom, jaký rozsah osobních údajů považuje za přiměřený a odpovídající a musí přitom zvážit veškerá rizika a případné důsledky plynoucí ze zpracování. Musí být mj. schopen prokázat relevantnost stanoveného rozsahu. Na tuto otázku navazuje kapitola 3.6.7 věnovaná právu vznést námitku při deskripci testu proporcionality (podkapitola „BALANČNÍ TEST“).

Zásada minimalizace se aplikuje na zpracování na základě všech šesti právních titulů zpracování. V praxi má největší dopad na zpracování údajů na základě souhlasu například v oblasti marketingu.

Povinnost minimalizace údajů ale není absolutní, jde spíše o povinnost minimalizovat shromažďování údajů na odpovídající úroveň ve vztahu k účelům zpracování. Je tedy vyžadováno vyhodnocení přiměřenosti předpokládaných činností zpracování. Správci i zpracovatelé by si měli položit otázku, zda jsou shromážděné údaje nezbytné pro dosažení účelu zpracování. **Cílem minimalizace dat je snížení sběru dat na nejnižší možnou úroveň pro stále odpovídající naplnění účelu zpracování**.[90]

Jak bude upřesněno v druhé části práce u právních důvodů zpracování (kapitola 4.1), případný sběr nadbytečných údajů nelze legitimizovat ani aplikací souhlasu se zpracováním osobních údajů. I kdyby takový souhlas splňoval veškeré další náležitosti a subjekt údajů by jej správci aktivně poskytl, neexistuje-li pro zpracování dotčených údajů účel či nejsou-li tyto údaje pro naplnění účelů potřebné, jedná se o porušení zásady minimalizace.

---

[88] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 6.

[89] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 5, odst. 1, písm. c).

[90] Voigt, P., Bussche, A. *The EU General Data Protection Regulation (GDPR)* [eBook]. Cham: Springer International Publishing AG, 2017, s. 90-91.

Nejsou-li například pro účely poskytnutí služby nebo výkonu veřejné moci určité údaje nutné a správce je fakticky pro naplnění účelu nepotřebuje, ale rozhodne se je zpracovávat, jde o nedodržení zásady minimalizace a porušení GDPR, a to bez ohledu na existenci vědomého souhlasu subjektu.

3.5.4 Zásada přesnosti

Pro dodržení této zásady je správce povinen přijmout veškerá rozumná opatření, aby údaje byly přesné a aktualizované, přičemž nutnost aktualizace vyplývá z účelu zpracování.[91]

Povinnost zpracovávat pouze přesné osobní údaje ale neznamená, že je vždy nezbytné zpracovávat jen absolutně správné údaje. Nepřesnosti mohou vzniknout už při samotném shromažďování údajů a z toho nelze vyvozovat odpovědnost daného správce. Opatřením k tomu, aby byly údaje správné a aktuální, je zajištění práva na opravu (viz kapitola 3.6.3), které se zásadou přesnosti úzce souvisí.[92]

V této souvislosti je třeba zdůraznit nezbytnou součinnost samotného subjektu. Pokud dojde ke změně osobních údajů, které získává správce od subjektu, a ten tuto změnu správci nenahlásí, není správce odpovědný za zpracovávání nepřesných osobních údajů, neukládá-li jiný právní předpis pravidelnou aktualizaci vybraných osobních údajů z jinak dostupných zdrojů (např. ze základních registrů).

3.5.5 Zásada omezení uložení

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Pokud se zpracování provádí výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely lze osobní údaje uložit po delší dobu, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.[93]

Správce musí stanovit lhůty pro pravidelný přezkum nebo výmaz. K tomu v praxi slouží zejména u správců s postavením OVM povinně vedené archivační a skartační řády.

---

[91] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 5, odst. 1. písm. d).

[92] Nulíček, M., Nonnemann, M., Lichnovský, B., Tomíček, J. *Obecné nařízení o ochraně osobních údajů (GDPR): Praktický komentář* [Systém ASPI]. Praha: Wolters Kluwer, 2018, komentář čl. 5 GDPR. Praktický komentář.

[93] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 5, odst. 1. písm. e).

Obvykle je tento proces zapracován do celkového řešení výkonu spisové služby, jejíž správné vedení a neduplikování fyzických analogových i digitálních dokumentů či jejich správná evidence v případě duplicit je základním předpokladem pro dodržování této zásady.

3.5.6 Zásada integrity a důvěrnosti

Nařízení GDPR výslovně uvádí, že zpracování musí být prováděno způsobem, *„který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením“*.

Tato opatření musí být stanovena přiměřeně v souladu s finančními a technickými možnostmi správce a odpovídajícím rizikům příslušných zpracování. Takový přístup je velmi důležitý, neboť nelze očekávat, že pro absolutní eliminaci rizika přijme správce nebo zpracovatel až likvidační opatření, tedy opatření svými náklady převyšující jeho reálné možnosti. Jiná opatření logicky přijímá nadnárodní korporace s miliardovými obraty a jiná přijme malá mateřská škola. Úroveň nastavených pravidel a bezpečnostních mechanismů musí tedy korelovat s potenciálním dopadem na subjekty údajů v případě kompromitace nebo poškození dat. Není-li správce schopen bezpečnost a integritu zajistit, musí zpracování zanechat. Je-li však takovým zpracováním povinován zákonem nebo v rámci výkonu veřejné moci, musí zajistit dostatečnou eliminaci rizik zpracování, byť s tím souvisí určitá investice nebo vyšší administrativní zátěž.

S touto zásadou úzce souvisí ustanovení uvedená v čl. 32 obecného nařízení zabývající se zabezpečením zpracování osobních údajů, která mj. navrhují aplikaci pseudonymizace (viz kapitola 3.4.3) a šifrování.[94] Doporučení v analyticko-praktické části na tuto zásadu navazují a šifrování jako velmi účinný prostředek s relativně nízkými implementačními náklady zahrnují.

V případě, že dojde k prolomení této zásady, tedy k narušení důvěrnosti nebo integrity osobních údajů, je správce povinován řídit se zejména ustanovením čl. 33 obecného nařízení. Tuto problematiku shrnují kapitoly 3.7 a 4.4 popisující zabezpečení zpracování a ohlašování jeho případného porušení.

Porušení zásady integrity a důvěrnosti má závažné důsledky na samu zákonnost zpracování a zakládá správci povinnosti přijmout neprodlená opatření na snížení následků

[94] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 32.

porušení ochrany zabezpečení osobních údajů včetně povinnosti informovat o některých těchto porušeních dozorový úřad či dokonce subjekt zasažený bezpečnostním incidentem.

3.5.7 Zásada odpovědnosti a vedení záznamů o činnostech zpracování

Zásada odpovědnosti byla zmíněna v rámci deskripce základního principu GDPR, tedy přístupu založenému na odpovědnosti správce a riziku zpracování. Je uvedena v čl. 5 odst. 2 obecného nařízení a zcela jednoznačně směřuje k zavedení dokumentování svých postupů i postupů najatých zpracovatelů. V praxi tento princip doložitelné odpovědnosti za zpracování znamená, že správce své zpracování i zpracování prováděné smluvními zpracovateli kontinuálně monitoruje, aby dokázal v budoucnu doložit legitimitu nejen probíhajícího, ale i v minulosti prováděného, zpracování.

Obecné nařízení v rámci svých recitálů doporučuje správcům a zpracovatelům, aby pro doložení souladu s obecným nařízením vedli záznamy o prováděných činnostech zpracování. Dále uvádí, že *„každý správce a zpracovatel by měl být povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány“*.[95]

Záznamy o činnostech zpracování představují určitou dokumentaci dodržování zásad zpracování uvedených v čl. 5 odst. 1 obecného nařízení (viz kapitoly 3.5.1 - 3.5.7).

Je třeba připomenout **povinnost udržovat všechny záznamy aktuální**, tj. zejména v dokumentaci promítat legislativní změny a průběžně doplňovat nové agendy zpracování. Záznamy jsou ve své podstatě interní dokumentací. Není a z bezpečnostních důvodů by ani neměla být bez odpovídající úpravy poskytována přímo subjektům údajů nebo dokonce zveřejnována například na webových stránkách, jak nesprávně někteří správci činí[96].

S ohledem na zásadu integrity a důvěrnosti lze důvodně předpokládat, že záznamy mohou konkretizovat opatření pro zajištění bezpečnosti informací, přičemž jejich zveřejněním může dojít ke snížení účinnosti vybraných opatření nebo přímo k narušení bezpečnosti poskytnutím informací o způsobu ochrany dat. V odpovídajícím rozsahu, nevylučuje-li to jiný právní předpis, jsou záznamy o činnostech zpracování dostupné dozorovému úřadu.

[95] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 82.

[96] Pro ověření postačí do internetového vyhledávače Google zadat dotaz „záznamy o činnostech zpracování škola“

Vedení zmíněných záznamů však neprobíhá pouze s cílem být schopen doložit soulad s nařízením GDPR, jde i o užitečný nástroj pro pověřence, kterému poskytuje vhled do zpracování, tedy jakousi orientační mapu. Ta je užitečná zejména při vyřizování žádostí subjektů nebo v případě bezpečnostních incidentů.

V konečném důsledku poskytují tyto záznamy cenné podklady pro tvorbu informačního memoranda určeného subjektům údajů (blíže viz kapitola 3.6.1 věnující se informační povinnosti a 4.2.1 popisující výkon práva na informace).

Pravděpodobně nejúčinnější cesta ke vzniku těchto záznamů je inventura procesů zpracování a identifikace jednotlivých činností, při kterých dochází ke zpracování osobních údajů (blíže postup vysvětlen v rámci tvorby vstupní analýzy zpracování v procesu implementace GDPR, zejména v kapitole 4.10.2).

3.6 Práva subjektů údajů

Právům subjektů a pravidlům výkonu těchto práv se věnuje podstatná část obecného nařízení, především články 12 až 23 v KAPITOLE III a články 77 až 79 a 82 v KAPITOLE VIII.[97] Představují práva fyzické osoby, o níž jsou zpracovávány osobní údaje, a tato mohou být dle své povahy subjektem uplatněna vůči správci, dozorovému úřadu nebo u soudu.

Protože je pro naplnění cílů této práce předmětná role správce, detailizuje kapitola 3.6 práva subjektu uplatnitelná přímo u správce, nikoliv u dozorového úřadu nebo soudu.

Subjekt údajů může požívat svých práv

a) **proaktivně**, například dotazuje-li se aktivně správce či uplatňuje svá práva, aniž by z informací od správce vyplývalo, že jeho údaje tento zpracovává, nebo si preventivně vyžádá kopii svých osobních údajů zpracovávaných správcem či upřesňující informace k rozsahu zpracování,
b) **reaktivně**, uplatní-li svá práva na základě podnětu, tedy reaguje-li na vzniklou situaci, dozví se například, že správce zahájil zpracování jeho osobních údajů, které nemohl důvodně očekávat,
c) **pasivitou**, zahájí-li správce zpracování, které subjekt neinicioval ani ho nemohl důvodně očekávat a má tedy právo být správcem informován o započetí takového zpracování.

[97] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, KAPITOLA III a VIII.

Některá práva musí být správcem vůči subjektu vykonávána aktivně, a to i směrem k těm pasivním. Částečně bychom tedy o těchto právech mohli hovořit jako o zásadách zpracování, kterými se správci musí obecně řídit.

Práva subjektů údajů mají za cíl především zvýšit informovanost o operacích týkajících se jejich údajů a případně jim dát možnost určité míry kontroly nad formou a rozsahem tohoto nakládání.[98]

Správce odpovídá za kontrolu oprávněnosti požadavků subjektů, uplatňují-li tito svá práva, jelikož například poskytnutí informací (osobních údajů) o subjektu údajů neoprávněné třetí osobě na základě její žádosti představuje porušení zabezpečení zpracování osobních údajů se všemi svými důsledky (viz kapitola 3.7 „Zabezpečení osobních údajů, porušení zabezpečení a jeho ohlašování“).

S ohledem na objem materie výkonu práv subjektů je část rozhodná pro soulad s nařízením GDPR přesunuta do vlastní části práce. Teoretická část dále stručně přibližuje pouze obecný popis jednotlivých práv. Detailizuje pouze prioritní „právo na informace“ a „právo na přístup k osobním údajům“, jehož výkon při nesprávném ztotožnění subjektu představuje pro správce velké riziko. Vyšší pozornost je poskytnuta ještě právu na podání námitky z důvodu určité nejednotnosti v postupu vyřizování námitek po schválení adaptačního zákona a rovněž s cílem přiblížit princip balančního testu.

Nařízení GDPR přímo hovoří o těchto základních právech subjektů údajů[99]:

a) *právo na informace,*
b) *právo na přístup k osobním údajům,*
c) *právo na opravu, resp. doplnění,*
d) *právo na výmaz (být zapomenut),*
e) *právo na omezení zpracování,*
f) *právo na přenositelnost údajů,*
g) *právo vznést námitku,*
h) *právo nebýt předmětem automatizovaného individuálního rozhodování s právními, či obdobnými účinky, zahrnujíce i profilování,*
i) *právo podat stížnost u dozorového úřadu,*

[98] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.4.11. Právní monografie (Wolters Kluwer ČR).
[99] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, KAPITOLA III a VIII.

j) *právo na účinnou soudní ochranu vůči dozorovému úřadu,*
k) *právo na účinnou soudní ochranu vůči správci nebo zpracovateli,*
l) *právo subjektu být zastupován (právo pověřit neziskový subjekt, organizaci nebo sdružení vyvíjejí činnost v oblasti ochrany práv a svobod subjektů údajů k podání stížnosti či uplatnění práv)*
m) *právo na náhradu újmy a odpovědnost*

Právo „j“, „k“ a „l“ nebude vzhledem k povaze této práce detailizováno.

V souvislostí s možným uplatněním práv je vhodné připomenout, že orgány veřejné moci zpracovávající osobní údaje například na základě právního důvodu „plnění smlouvy“ (viz kapitola 4.1.2) se obvykle v rámci smluvního vztahu nenacházejí v postavení svrchovaného orgánu autoritativně rozhodujícího o právech a povinnostech fyzických či právnických osob. Jako soukromoprávní subjekty například při nákupech služeb, zboží, pronájmu, prodeji majetku či v rámci pracovněprávních vztahů apod. totiž v drtivé většině situací nevykonávají svou působnost ani nechrání veřejný zájem. Tento aspekt je třeba vzít v potaz při posuzování žádostí subjektu ve snaze realizovat vybraná práva. Nařízení GDPR připouští v mnoha případech nevyhovění žádostem subjektů, jedná-li se o zpracování prováděné ve veřejném zájmu nebo při výkonu veřejné moci, případně při plněná právní povinnosti.

3.6.1 Právo na informace

Toto právo představuje zcela elementární institut celého nařízení GDPR a je výchozím právem subjektu údajů. V úvodu explanace tohoto podstatného nároku subjektu „být informován o zpracování“ jeho osobních údajů je třeba zdůraznit, že jej nelze zaměňovat ani slučovat s právem na informace podle informačního zákona, zákona č. 106/1999 Sb. Bohužel se někdy uplatnění obou práv prolíná, avšak častou chybou správců, kteří jsou zároveň v postavení povinného subjektu ve smyslu informačního zákona, je chybná identifikace podání či žádosti subjektu a vyřízení dle nevhodné právní úpravy.

Lze konstatovat, že právo na informace ve smyslu právní úpravy ochrany a zpracování osobních údajů je nejdůležitějším a nejsledovanějším právem subjektů údajů nejen dle nařízení GDPR, ale také podle ZZOÚ. Je třeba mu věnovat náležitou pozornost v kontextu s veškerými prováděnými operacemi zpracování osobních údajů, protože způsob realizace práva na informace je velmi snadno kontrolovatelný. Je to z důvodu obvykle

veřejného publikování informací o zpracování, navíc způsobem umožňujícím dálkový přístup.

Celková úroveň informací poskytnutých subjektům (určitých zásad zpracování), o správci někdy prozradí mnohem více než samotný věcný obsah dokumentu.

Smyslem realizace práva na informace je však naplnění zásady transparentnosti, nikoliv neopodstatněné zahlcení subjektu údajů, ani nepřiměřené zatížení správce. Není nutné poskytovat informace, kterými již subjekt disponuje, které vyplývají přímo z právních předpisů nebo jejichž poskytnutí by vyžadovalo nepřiměřené úsilí ze strany správce.[100]

Forma a rozsah realizace práva na informace je odvislá od zdroje osobních údajů, tedy zda jsou osobní údaje získávány přímo od subjektu údajů nebo od třetí osoby.

Při získávání údajů přímo od subjektu údajů je povinností správce poskytnout subjektu v okamžiku získání jeho údajů přehled o základních parametrech užití dat, zejména pak o účelu zpracování, totožnosti správce včetně kontaktních údajů svých i pověřence, byl-li tento jmenován. Rovněž musí být poskytnuty informace o dalších případných příjemcích. Podrobný seznam povinně poskytovaných informací obsahuje článek 13 nařízení GDPR. [101]

V případě, že osobní údaje poskytla správci třetí osoba, musí být okruh informací poskytovaných subjektu dle předchozího bodu rozšířen, je-li to pro zajištění spravedlivého a transparentního zpracování významné, o zdroj, ze kterého správce tyto údaje získal.

Na rozdíl od některých níže uvedených práv nebo od práva na poskytování informací podle informačního zákona, kde je ve vybraných případech odpovídající zpoplatnění akceptovatelné, je právo na informace podle GDPR a ZZOÚ vykonáváno zásadně bezplatně.

3.6.2 Právo na přístup k osobním údajům

Právo na informace o zpracování (viz předchozí kapitola) je komplementárním právem k právu na přístup k osobním údajům. Představuje právo subjektu údajů získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány. Pokud zpracování údajů skutečně probíhá, má subjekt právo získat přístup ke svým osobním

[100] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 13, odst 4; recitál 62.
[101] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.4.11. Právní monografie (Wolters Kluwer ČR).

údajům, a to buď potvrzením o zpracovávání nebo obdržením přesně vymezené informace o současném i dosavadním zpracování. Může jít o doplňující informace o základních parametrech zpracování (např. kategorie zpracovávaných osobních údajů, účely zpracování a dostupné informace o zdroji údajů). Alternativou je také vyžádání si kopie zpracovávaných údajů od správce, přičemž jednu bezplatnou kopii je správce povinen vyhotovit.[102]

Omezující pro aplikaci práva na přístup je v celé v řadě situací podmínka, že tím nesmí být nepřiměřeně a nepříznivě dotčena práva jiných osob. U komplikovanějších systémů a složitějších datových struktur obsahujících vzájemně provázané či agregované údaje různých skupin osob není zřejmé, jak bez vynaložení nepřiměřeného úsilí nebo nákladů vyčlenit odvozené osobní údaje, tedy údaje přímo či nepřímo se vztahující k subjektu uplatňujícímu právo na přístup, a to bez zásahu do práv či svobod jiných osob.[103]

Praktický příklad poskytování údajů na žádost subjektu, konkrétně předávání kamerových záznamů, je uveden v kapitole 4.6.

Výkon tohoto práva je pro správce tím nejrizikovějším, protože vyžaduje naprosto nezpochybnitelné ztotožnění subjektu využívajícího právo, resp. je zcela zásadní zajistit poskytnutí údajů právě tomu subjektu, kterému opravdu náleží. Eliminace rizika podvržení identity žadatele o uplatnění práva na přístup tak musí být v procesu realizace práva na prvním místě.

Neoprávněné využívání práva na přístup, tzv. *blagging*, je v kombinaci s krádeží identity při nedostatečném zabezpečení zpracování ze strany správce potenciálně velmi úspěšné. Třetí osobě předstírající nárok subjektu údajů umožní získat od správce soubor jeho zpracovávaných údajů.[104] V analytické části v kapitole 4.3 jsou pospány pravidla komunikace se subjekty snižující toto riziko.

3.6.3 Právo na opravu, resp. doplnění

Právo na opravu, právo na doplnění a zásada správnosti a přesnosti zpracování osobních údajů spolu velmi úzce souvisí (viz kapitola 3.5.4). Subjekt má v kontextu těchto pravidel právo požadovat po správci bezprostřední opravu či doplnění nepřesných údajů.

[102] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, článek 15.
[103] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.4.11. Právní monografie (Wolters Kluwer ČR).
[104] Cormack, A. Is the Subject Access Right Now Too Great a Threat to Privacy?. *European Data Protection Law Review* [online]. 2016, č. 1 [cit. 2021-01-05].

Nařízení GDPR k právu na opravu uvádí, že *„subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení“*.[105]

Vycházíme-li z premisy, že subjekt ani správce nemají zájem na zpracovávání nepřesných a neúplných informací, nemělo by za běžných okolností činit uplatňování těchto práv komplikace.

3.6.4 Právo na výmaz (být zapomenut)

Smyslem práva na výmaz je možnost subjektu údajů domoci se v duchu zásady minimalizace rozsahu (viz kapitola 3.5.3) a doby uchovávaných údajů odstraněním osobních údajů, které již neslouží k přiměřenému či legitimnímu zpracování.

Výstižně k tomuto právu doc. Polčák dodává: *„Je tedy nutné mít na paměti, že toto právo není mocnou gumou, která skryje z paměti internetu či jiných databází nechtěnou minulost jedince, ale veskrze toliko smetáčkem, se kterým lze uklidit některé opomenuté záznamy, které již ztratily na významu.“*[106]

Uvedený princip je výkladem posledního odstavce článku 17 obecného nařízení, který obsahuje poměrně rozsáhlý přehled situací vyňatých z možné aplikace práva na výmaz.

Z možnosti výkonu práva na výmaz je vyňato například zpracování nezbytné pro výkon práva na svobodu projevu či práva na informace, pro splnění právní povinnosti, pro plnění úkolů prováděných ve veřejném zájmu či v rámci výkonu veřejné moci, jakož i pro určení, výkon nebo obhajobu právních nároků.[107]

Uvážíme-li, že pro realizaci výmazu na základě předmětného práva musí být splněna alespoň jedna z následujících podmínek, a to nepotřebnost pro původní účel, protiprávnost zpracování či odvolání souhlasu, je okruh případů reálného uplatnění práva na výmaz citelně redukován.

---

[105] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, článek 16.

[106] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.4.11. Právní monografie (Wolters Kluwer ČR).

[107] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 17, odst. 3.

3.6.5 Právo na omezení zpracování

Využití tohoto práva iniciuje přerušení a zakonzervování většiny forem zpracování údajů stižených buďto námitkou oprávněnosti (viz právo vznést námitku v kapitole 3.6.5), případně výtkou nepřesnosti (viz právo na opravu, resp. doplnění, v kapitole 3.6.3). Práva lze využít rovněž u zpracování údajů určených k likvidaci pro nepotřebnost (v souladu se zásadami minimalizace, resp. omezení uložení, viz kapitola 3.5.3, resp. 3.5.5) či v případě protiprávnosti zpracování (nedodržení zásady zákonnosti – viz kapitola 3.5.1). Subjekt uplatněním tohoto práva projevuje zájem na zachování údajů, avšak nesouhlasí s jejich dalším zpracováním, a to zejména pro potřeby výkonu či obhajoby svých právních nároků.[108]

3.6.6 Právo na přenositelnost údajů

Právo na přenositelnost údajů je specifickou a novou formou práva na kopii údajů. Původní legislativa toto právo nepřipouštěla. Dává subjektu údajů možnost za určitých podmínek spustit přenos údajů vztažených k jeho osobě od stávajícího správce ke správci jinému. Již sama povaha práva na přenositelnost však zjevně vylučuje jeho aplikaci na údaje zpracovávané správcem v rámci výkonu veřejné moci nebo při plnění úkolu ve veřejném zájmu.

Výkonem práva na přenositelnost nesmí být, stejně jako v případě práva na přístup k údajům, dotčena nepříznivě práva a svobody dalších subjektů. Kumulativně musí být splněny i další podmínky, například musí jít o data, které správci poskytl v minulosti sám subjekt a musí jít o zpracování založeném na právním titulu „souhlas se zpracováním osobních údajů“ (viz kapitola 4.1.1) či na základě smlouvy uzavřené mezi správcem a subjektem údajů (viz právní důvod plnění smlouvy v kapitole 4.1.2).

Rozsah práva je také redukován neuplatnitelností na údaje, které nezískal správce přímo od subjektu, ale pocházejí z jiných zdrojů. Rovněž je použití práva limitováno ve vztahu k odvozeným a vyvozeným údajům.[109]

3.6.7 Právo vznést námitku

V souladu s nařízením GDPR může subjekt údajů podat námitku proti zpracování prováděném na základě právních titulů "oprávněný zájem" či "plnění úkolů ve veřejném

[108] Polčák, R. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, kapitola 9.4.11. Právní monografie (Wolters Kluwer ČR).
[109] Pattynová, J., Suchánková, L., Černý, J., Růžička, M. *Obecné nařízení o ochraně osobních údajů (GDPR)*. Praha: Leges, 2019, s. 207. Komentátor.

zájmu nebo při výkonu veřejné moci". Námitka je přípustná rovněž proti zpracování prováděném pro účely vědeckého či historického výzkumu nebo při statistickém zpracování.[110]

Obdrží-li správce námitku subjektu proti zpracování a je-li tato přípustná, tedy zejména je-li podaná proti odpovídající kategorii zpracování, musí správce v prvé řadě přezkoumat zákonnost zpracování, námitku posoudit a zvážit, má-li pro takové operace s daty legitimní důvody, které převažují nad určitým zásahem do práv a svobod subjektu údajů. **Do doby prokázání zákonnosti a oprávněnosti musí správce předmětné zpracování přerušit.** V tomto případě je nepochybně důkazní břemeno prokázání oprávněnosti zpracování na správci. V návaznosti na případnou námitku je toliko nucen zvážit provedení tzv. **balančního testu** blíže vysvětleného na konci této podkapitoly.

Trochu jiná situace nastává, je-li námitka podána vůči zpracování pro novinářské, akademické, umělecké nebo literární účely. Subjekt údajů musí za uvedených okolností relevantně zdůvodnit a prokázat, že jeho zájem na nezpracovávání osobních údajů převáží nad zájmy správce, tedy že zásah do jeho práv a svobod zjevně překračuje přiměřenost korelující s veřejným zájmem dotčené údaje zpracovávat a zveřejňovat.

Tento obrácený postup, tedy výměna strany zatížené důkazním břemenem, je reakcí na výjimku, kterou připouští čl. 85 obecného nařízení, a které ZZOÚ v § 17 využil.[111]

ZZOÚ tak otáčí zmíněné důkazní břemeno ze správce na subjekt vznášející námitku, navíc připouští podání námitky až ve chvíli, kdy správce údaje zveřejní nebo zpřístupní.[112]

Na právo podat námitku včetně kontaktních údajů pro podání musí být subjekt údajů specificky upozorněn v rámci první komunikace se správcem, ideálně formou informačního memoranda, poučením či seznámením se zásadami zpracování (viz kapitola 3.6.1).

BALANČNÍ TEST neboli test proporcionality je testem přiměřenosti, v rámci něhož porovnává správce svůj zájem na zpracovávání s vylíčeným zájmem dotčené osoby nebýt předmětem zpracování. V případě převážení zájmu subjektu, resp. v situaci zjevně nepřiměřeného zásahu do jeho práv a svobod, který není převážen nesporným oprávněným

[110] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, článek 21.
[111] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 17, § 22.
[112] Nulíček, M., Donát, J., Lichnovský, B., Nonnemann, F., Habarta, ,., Kašpárková, K. *Zákon o zpracování osobních údajů* [E-KNIHA]. Praha: Wolters Kluwer, 2019, § 17, § 22. Praktický komentář.

zájmem správce nebo třetí osoby či nezpochybnitelným veřejným zájmem, musí správce zpracování ukončit.

Zpracovává-li správce osobní údaje na základě právního důvodu "oprávněný zájem", musí nejdříve (před zahájením zpracování) vyhodnotit, zda nad jeho oprávněným zájmem nepřevažují zájmy (práva, svobody) subjektu osobních údajů, soukromé fyzické osoby, jejíž osobní údaje jsou takto zpracovávány. Test proporcionality se provádí automaticky, nikoliv až v reakci na výkon práv subjektů. V případě zpracovávání při plnění úkolů ve veřejném zájmu nebo při výkonu veřejné moci se balanční test použije pouze v případě námitky subjektu, neprovádí se před zahájením zpracování, jako je to u oprávněného zájmu.

Nařízení GDPR ve svých recitálech vysvětluje, že existence oprávněného zájmu musí být důsledně vyhodnocena, a to včetně posouzení důvodného očekávání subjektu, že ke zpracování pro dané účely může dojít. [113]

Test proporcionality musí obsahovat minimálně:

- záznam o omezení/pozastavení zpracování do vyhodnocené testu (bylo-li již zpracování zahájeno),
- vyjádření oprávněného zájmu správce,
- rizika vyplývající ze zpracování a dopadající potenciálně na subjekt údajů,
- popis zabezpečení a opatření pro snížení rizik,
- vyjádření očekávání subjektu na zpracovávání jeho osobních údajů,
- vyhodnocení testu a posouzení pověřence, je-li jmenován,
- rozhodnutí o spuštění/nespuštění zpracování, resp. o pokračování či nepokračování zpracování.

3.6.8 Právo nebýt předmětem automatizovaného rozhodování a profilování

Toto právo definované konkrétně jako „*Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování včetně profilování*“[114] představuje jakýsi „zajišťovací institut“, který ukládá, aby se o právních účincích nerozhodovalo automatizovanými postupy bez lidského zásahu. Snaží se tedy o zmírnění rizik automatizace přiměřeným doplněním procesních kroků o lidský faktor. Nařízení GDPR za tím účelem

[113] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 47.
[114] *Ibid.*, čl. 22, odst. 1.

uvádí, že jednotlivým osobám musí být umožněno uplatnit vůči správci právo na lidský zásah, na vyjádření svého názoru a právo napadnout rozhodnutí vzešlé z automatizovaného zpracování.[115]

Ustanovení § 39 ZZOÚ zakazuje zásah na základě automatizovaného zpracování se závažnými právními důsledky pro subjekt údajů s výjimkou případů, kdy by tak zvláštní zákon výslovně umožňoval. Opatření ovlivňující právní postavení subjektů nebo podobně závažné jiné opatření s dopadem na subjekt nelze přijmout pouze na základě počítačového profilování.

Pro naplnění tohoto práva je třeba zajistit, aby subjekt údajů mohl požádat o přezkoumání rozhodnutí k tomuto účelu správcem poučenou a pověřenou osobou a mohl vyjádřit svůj názor ve vztahu k automatizovanému rozhodnutí.

V praktickém životě se tento typ zpracování vyskytuje především v rámci cíleného marketingu (personalizace reklam).

3.6.9 Právo podat stížnost u dozorového úřadu

Aniž by to jakkoliv omezilo další práva subjektu, může se tento obrátit se svou stížností na dozorový úřad, domnívá-li se, že byly při zpracování osobních údajů porušeny právní předpisy.[116] Tento institut se v praxi využívá zejména nekomunikuje-li či nespolupracuje-li správce při pokusu o realizaci práv ze strany subjektu, případně v situacích, kdy správce není znám. V této souvislosti je správcům důrazně doporučeno, aby se snažili situaci vždy řešit vzájemnou dohodou a pokusili se zamezit eskalaci problémů až k ÚOOÚ.

3.6.10 Právo na náhradu újmy a odpovědnost

Nařízení výslovně uvádí, že *„kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy“*.[117]

Uplatnění tohoto práva přiznaného subjektům článkem 82 obecného nařízení je ze strany subjektu značně komplikované. Subjekt musí prokázat onu vzniklou újmu a je-li tato finančně nevyčíslitelná, nastává velmi abstraktní výpočet újmy nemajetkové.

---

[115] *Ibid.*, čl. 22, odst. 3.
[116] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, článek 77.
[117] *Ibid.*, článek 82.

Této problematice se cíleně nevěnuje nařízení GDPR, čerpat se však dá z občanského zákoníku a pro potřeby této práce je vhodné alespoň přiblížit možné závažné důsledky přehlížení uvedeného ustanovení.

Pokud činností správce nebo zpracovatele vznikne subjektu vyčíslitelná škoda na majetku, může subjekt nárokovat kompenzaci dle ustanovení čl. 82 po správci. Nebude-li úspěšný, může se obrátit na soud. Obdobně bude postupovat v případě ušlého zisku, tedy doložitelné ztráty, která by jinak nevnikla, neporušil-li by správce či zpracovatel nařízení GDPR. Nebude-li subjekt schopen výši škody doložit, tedy půjde-li například o hypotetický ušlý zisk nebo nemajetkovou újmu (zejména porušením osobnostních práv), bude nástup satisfakce ležet na vzájemné dohodě subjektu a správce nebo na rozhodnutí soudu.

Jak již bylo uvedeno v průběhu předchozích kapitol a jak je dále uvedeno v kapitole 3.8 věnující se sankcím, nemůže být orgán veřejné moci, kterými jsou i školy, v souvislosti s porušením GDPR pokutován. **Právo subjektu na náhrady újmy ze strany správce tím však není dotčeno.** Snižovat dopad tohoto institutu na správce, případně ho zcela ignorovat, není přes jeho složitější vykonatelnost ve vybraných případech na místě. Budoucí rozhodovací praxe soudu jistě určí směr pro uplatňování předmětného práva.

3.7 Zabezpečení osobních údajů, porušení zabezpečení a jeho ohlašování

ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ A RIZIKA ZPRACOVÁNÍ

Problematika zabezpečení osobních údajů v širším významu se prolíná napříč celým nařízením GDPR a ZZOÚ, je to stěžejní myšlenka v přístupu ke zpracování informací. V užším významu, tedy ve vztahu ke konkrétnímu přístupu k ochraně osobních údajů, je otázka zabezpečení detailněji upravena článkem 32 obecného nařízení a současně v ustanovení § 40 ZZOÚ. Na zabezpečení osobních údajů je oběma těmito předpisy kladen velký důraz, přesto jsou pravidla pro dosažení bezpečnosti upravena vesměs obecně, konkretizována jsou spíše možná rizika doplněná o vybrané cíle k jejich eliminaci.

Spravující orgán a obdobně zpracovatel mají povinnost přijmout adekvátní opatření a využít odpovídající prostředky na zabezpečení zpracování osobních údajů. Úroveň příslušných technickoorganizačních opatření musí korelovat zejména s povahou, rozsahem, okolnostmi zpracování, s účely a jmenovitě s riziky, které s sebou každé zpracování nese. Povaha opatření do značné míry vychází z analýzy rizik předmětných zpracování, přičemž nařízení GDPR hovoří o posuzování vhodnosti a přiměřenosti nastavených pravidel eliminujících hrozící porušení zabezpečení.

Zabezpečení osobních údajů představuje trvalý proces, nemůže být jednorázovým aktem, nejedná-li se o zcela nahodilé zpracování. Správce musí zohlednit neustále se měnící prostředí, technologie a s tím i související vývoj rizik. Dle nových okolností musí přizpůsobovat technická a organizační opatření pro udržení adekvátní úrovně zabezpečení. Zpracování osobních údajů musí provádět pouze oprávněné osoby, resp. nesmí mít k osobním údajům přístup jiný pracovník správce, není-li k tomu objektivní důvod plynoucí z předmětu jeho činnosti. Je třeba přijmout opatření v oblasti fyzické bezpečnosti, administrativní bezpečnosti a bezpečné archivace i skartace dokumentů.[118]

Dospěje-li správce či zpracovatel v kontextu přijatých opatření k závěru, že zpracování představuje stále nepřiměřené riziko pro práva a svobody osob, je povinen provést v souladu s čl. 35 obecného nařízení tzv. DPIA – *Data Protection Impact Assessment,* tedy Posouzení vlivu na ochranu osobních údajů. Dozorový úřad pro tyto účely připravil velmi kvalitní návod.[119]

Výčet dále uvedených oblastí hodných řešení je pouze demonstrativní a slouží jako vodítko pro správce či zpracovatele, jejichž odpovědností je hledat cesty k odpovídajícímu snížení rizik zpracování. Není ani úlohou GDPR poskytovat odpověď na každý typ zpracování a na veškeré druhy představitelných rizik.

PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ A JEHO OHLAŠOVÁNÍ

Porušení zabezpečení dle definice obecného nařízení *„vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“.*[120]

Subjektu může takové porušení zabezpečení způsobit majetkovou i nemajetkovou újmu (k případné náhradě újmy viz kapitola 3.6.10), zejména pak ztrátu kontroly nad jeho osobními údaji, v některých případech i krádež či dokonce zneužití identity.

Nařízení GDPR ukládá všem správcům povinnost hlásit bezpečnostní incidenty, resp. porušení zabezpečení, prolomení ochrany, kompromitaci dat atp., dozorovému úřadu, a to neprodleně, nejdéle však do 72 hodin od zjištění, že k takovému incidentu došlo. Výjimka je přípustná pouze v případě, že povaha incidentu nebo následně přijatá

[118] Nulíček, M., Donát, J., Lichnovský, B., Nonnemann, F., Habarta, ,., Kašpárková, K. *Zákon o zpracování osobních údajů* [E-KNIHA]. Praha: Wolters Kluwer, 2019, koment. § 40. Praktický komentář.
[119] *Úřad pro ochranu osobních údajů: Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA)* [online]. [cit. 06. 03. 2021].
[120] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 32, odst. 2.

opatření minimalizují rizika dopadu do práv a svobod dotčených osob, tedy že je nepravděpodobné, že by mohla subjektu vzniknou jakákoliv újma.

Naopak v případě, kdy je **riziko zásahu do práv či svobod subjektů vysoké, musí příslušný správce ohlásit takové porušení i dotčenému subjektu či subjektům**.

Vzhledem k tomu, že správce má povinnost zavést vhodná bezpečnostní a technickoorganizační opatření, musí s ohledem na zpracovávané osobní údaje před zahájením zpracování zvážit, zda by součástí zabezpečení neměly být různé formy detekce incidentů. Je nezbytné edukovat veškeré zaměstnance, najaté zpracovatele a spolupracující osoby, jak mají v případě podezření na incident postupovat, aby byl proces řešení efektivní a dostatečně rychlý. Tlak na zkrácení lhůty potřebné pro identifikaci a šetření incidentů nelze vnímat jen ve vztahu ke splnění 72 hodin dlouhé lhůty na oznámení porušení zabezpečení. **Primárním cílem je zkrátit dobu, po kterou jsou data subjektů ohrožena a zejména potlačit rizika dopadu na nositele údajů, na fyzické osoby.**

Postup řešení incidentů a jejich hlášení je v praktické části v kapitole 4.4.

3.8 Sankce a pravomoci ÚOOÚ

Na sankce spojené s porušováním nařízení GDPR je možné se dívat z mnoha pohledů. Detailní analýza rozhodovací praxe dozorového úřadu a s ní souvisejících pravidel pro udělování sankcí by vydala na samostatnou práci, proto se tato kapitola omezí na přiblížení sankčních ustanovení v nařízení GDPR, na rekapitulaci výjimky v možnosti ukládání sankcí OVM a na vybrané pravomoci ÚOOÚ. Pojem „sankce“ nelze rozhodně zužovat výlučně do oblasti finančních postihů, proto jsou v třetí části této kapitoly přiblížena nápravná opatření vydávaná dozorovým úřadem.

FINANČNÍ SANKCE

Nařízení GDPR značně posunulo obvyklou hranici výše pokut, a to ve snaze o zvýšení účinnosti represivních finančních postihů na společnosti s velkými zisky, pro které běžná pokuta není dostatečným impulzem k nápravě přístupu k ochraně osobních údajů.

S blížící se účinností GDPR sílily tendence k dramatizování likvidačních následků GDPR na správce. Záznamy v registru smluv[121] z první poloviny roku 2018 dokládají, že v obavách z příchodu obecného nařízení a souvisejících vysokých sankcí byly základními i

[121] MINISTERSTVO VNITRA. *Registru smluv* [online]. [cit. 2021-03-02].

mateřskými školami schvalovány jindy neakceptovatelné investice do diskutabilních řešení ochrany sítí, informačních systémů, ale i fyzické bezpečnosti.

ÚOOÚ[122] a veřejnoprávní média[123] se ve spolupráci s oborníky na problematiku ochrany osobních údajů pokoušeli ještě před účinností GDPR vyvracet mýtus o riziku astronomických sankcí (horní hranice finančních postihů uvedených v článku 83 obecného nařízení je nastavena na 20 milionů EUR nebo 4 % z globálního obratu společnosti). I samo nařízení definuje, že sankce nemají být likvidační, ale adekvátní k povaze a závažnosti konkrétního porušení.

Pokuta má být odrazující, účinná, nicméně přiměřená.[124]

Zabývat se dále vysokými pokutami je pro naplnění cílů práce bezpředmětné, jejich užití v nepřiměřené výši je nejen zhusta nepravděpodobné, ale ve vztahu ke školám a školským zařízením dokonce úplně nemožné. Jak již bylo vysvětleno v úvodu, a především v rámci kapitoly 3.2.1 věnované ZZOÚ, nemůže být od účinnosti adaptačního zákona pokutován v ČR žádný OVM za porušení obecného nařízení a školy se v postavení OVM nacházejí (blíže viz kapitola 3.4.4).

JINÉ TYPY SANKCÍ

Každý správce včetně OVM by si měl být vědom, že absence hrozby finančního postihu není impulzem pro laxní přístup k nakládání s osobními údaji. Dopad na správce i na osoby, které jsou se správcem v pracovněprávním vztahu, je díky dalším pravomocím úřadu uvedeným zejména v čl. 58 GDPR, dále díky právu subjektů na náhradu újmy (viz kapitola 3.6.10) a v neposlední řadě díky § 180 trestního zákoníku (viz kapitola 3.1.3) zcela reálné.

Způsobí-li zaměstnanec správce či zpracovatele natolik závažnou situaci, že bude kvalifikována jako trestný čin „neoprávněné nakládání s osobními údaji“, případná výjimka ze sankcionování OVM je irelevantní a hrozbou je kromě peněžitého trestu uloženého soudem i zákaz činnosti nebo dokonce trest odnětí svobody na jeden rok až pět let.[125] Toto ustanovení se vztahuje i na neoprávněné zveřejnění nebo zpřístupnění osobních údajů, a to i nedbalostní, nikoliv úmyslné.

---

[122] Základní příručka k ochraně: Sankce, pokuty. *Úřad pro ochranu osobních údajů* [online]. [cit. 2021-01-21].
[123] ČESKÁ TELEVIZE. *Největší mýty o GDPR. Kvůli špatné přípravě je nová ochrana dat zahalena nejasnostmi* [online]. [cit. 2021-03-06].
[124] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 83, odst. 1.
[125] Zákon č. 40/2009 Sb., trestní zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2009, částka 11, číslo 40, § 180.

Rovněž hrozící realizace práva subjektu na náhradu újmy v kombinaci ustanoveními zákoníku práce upravujícím náhradu vzniklé škody svému zaměstnavateli, a to dokonce „pouze“ v rámci nedbalostního zavinění, nelze podceňovat.[126]

PRAVOMOCI ÚOOÚ

Vážný dopad, mnohdy citelnější než přiměřená pokuta, má na správce či zpracovatele případné uložení nápravných opatření ze strany ÚOOÚ. S těmi se pojí negativní publicita. ÚOOÚ totiž pravidelně zveřejňuje výsledky svých kontrol i druhoinstančních rozhodnutí.

V souladu s nařízením GDPR může ÚOOÚ po správci i zpracovateli vyžadovat poskytnutí veškerých informací o zpracování a přístup k datům, systémům i fyzický vstup do prostor pro provedení auditu. Ve smyslu obecného nařízení jde o určitý typ **inspekce**.

V případě zjištění pochybení může kromě již popsaného finančního postihu uložit nápravná opatření, a to od upozornění na porušování obecného nařízení přes udělení napomenutí až k nařízení vyhovění žádostem subjektů a uvedení zpracování do souladu s obecným nařízením. V případě zjištění protiprávního zpracování osobních údajů může ÚOOÚ dokonce vyslovit zákaz pro další zpracování a vydat s tím související příkaz k výmazu údajů.

3.9 Teorie implementace GDPR

Implementace GDPR, případně revize dříve provedené implementace, je velmi komplexní disciplína a pro její úspěšnou realizaci nedostačuje pouze seznámení se s legislativou v oblasti ochrany a zpracování osobních údajů. Zcela klíčová je znalost dalších právních předpisů, které se na předmětného správce vztahují. Neméně důležitá je také znalost metodických pokynů a vzorových projektů z oblasti ochrany a zpracování osobních údajů vztahujících se na konkrétní typ správce. Rovněž je vhodné mít alespoň základní povědomí o řízení projektů a analýze rizik.

V této poslední kapitole teoretické části budou stručně shrnuty další právní předpisy upravující činnosti škol, které je třeba při implementaci GDPR, resp. při revizi implementace, analyzovat a uplatnit, a to při vstupní analýze zpracování, při aplikaci technickoorganizačních opatření a při tvorbě záznamů o činnostech zpracování.

[126] Zákon č. 262/2006 Sb., zákoník práce. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2006, částka 84, číslo 262, § 257.

3.9.1 Analýza právních předpisů upravujících činnost správce

Častou chybou, kterou při aplikaci právních předpisů přímo upravujících ochranu a zpracování osobních údajů správci či zpracovatelé činí, je omezení se právě jen na ony předpisy, tedy v tomto případě pouze na obecné nařízení a na adaptační zákon. Každá právnická osoba, každý orgán veřejné moci, každá organizace se musí řídit celou řadou právních norem, veřejnoprávní subjekty obzvlášť, a nařízení GDPR a ZZOÚ jsou jen jedny z mnoha těchto předpisů.

Stejná pravidla, tedy znalost souboru předpisů dopadajících na subjekt činící zpracování, platí i pro pověřence pro ochranu osobních údajů, je-li správcem jmenován. Toto mj. zdůrazňuje v rámci svých seminářů i vrchní rada pro vládní agendy, doktorka Matoušová, z Úřadu pro ochranu osobních údajů.[127]

Proto je velmi žádoucí, aby implementaci prováděl přímo správce sám, resp. se svým pověřencem, případně pouze s pomocí odborníků, a nikoliv formou externího nákupu služby. Správce zná nejlépe vlastní prostředí, systémy a právní předpisy, které upravují jeho činnost. V organizacích, jako jsou školy, toto platí dvojnásob.

PRÁVNÍ PŘEDPISY UPRAVUJÍCÍ CHOD ŠKOLY

Při zavádění pravidel pro zajištění souladu s obecným nařízením je třeba znát kromě nařízení GDPR a adaptačního zákona minimálně tyto další právní předpisy. Výčet není taxativní, pouze názorně přibližuje ty legislativní dokumenty, bez kterých není možné vytvořit relevantní prvotní vstupní analýzu zpracování a z ní vyplývající sestavení záznamů o činnostech zpracování. Rovněž by nebylo možné zdůvodnit přiřazování právního základu zpracování „právní povinnost“, který je nejčastějším zákonným důvodem zpracování osobních údajů v prostředí škol.

Demonstrativní přehled právních předpisů, které je třeba analyzovat při zavádění pravidel pro zajištění souladu s obecným nařízením (abecední řazení, nikoliv dle významu):

- NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- Nařízení vlády č. 201/2010 Sb., o způsobu evidence úrazů, hlášení a zasílání záznamu o úrazu

[127] MATOUŠOVÁ, M. *Konzultace pro pověřence pro ochranu osobních údajů, Praha 9. října 2018*. Praha: Úřad pro ochranu osobních údajů, 2018.

- Nařízení vlády č. 341/2017 Sb., o platových poměrech zaměstnanců ve veřejných službách a správě
- Nařízení vlády č. 75/2005 Sb., o stanovení rozsahu přímé vyučovací, přímé výchovné, přímé speciálně pedagogické a přímé pedagogicko-psychologické činnosti pedagogických pracovníků
- Vyhláška č. 114/2002 Sb., Ministerstva financí o fondu kulturních a sociálních potřeb
- Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby
- Vyhláška č. 263/2007 Sb., kterou se stanoví pracovní řád pro zaměstnance škol a školských zařízení zřízených Ministerstvem školství, mládeže a tělovýchovy, krajem, obcí nebo dobrovolným svazkem obcí
- Vyhláška č. 27/2016 Sb., o vzdělávání žáků se speciálními vzdělávacími potřebami a žáků nadaných
- Vyhláška č. 317/2005 Sb., o dalším vzdělávání pedagogických pracovníků, akreditační komisi a kariérním systému pedagogických pracovníků
- Vyhláška č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky
- Vyhláška č. 64/2005 Sb., o evidenci úrazů dětí, žáků a studentů
- Vyhláška č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských zařízeních
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla)
- Zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů
- Zákon č. 262/2006 Sb., zákoník práce
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 309/2006 Sb., o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci

- Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) (je-li škola povinným subjektem pro zveřejňování smluv v registru smluv)
- Zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí
- Zákon č. 435/2004 Sb., o zaměstnanosti
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
- Zákon č. 500/2004 Sb., správní řád
- Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)
- Zákon č. 563/1991 Sb., o účetnictví
- Zákon č. 563/2004 Sb., o pedagogických pracovnících a o změně některých zákonů

Zpracování v rámci provozních agend, tedy mimo hlavní předmět činnosti a při výkonu působnosti, ovlivňuje pochopitelně ještě celá řada dalších zákonů a podzákonných norem, například zákony upravující zdravotní, sociální a důchodové pojištění, vyhláška o požární prevenci atd., je však nad akceptovatelný rozsah práce se jimi při analýze zabývat a není to ani nezbytné pro naplnění cílů práce. Uvedeny byly pro zdůraznění rozsahu legislativy vztahující se na školská zařízení a významu orientace v platných předpisech pro následné správné přiřazení právních titulů zpracování, především zákonného důvodu „plnění právní povinnost“.

3.9.2 Další podpůrné materiály pro zavádění GDPR

Kromě právních předpisů uvedených v předchozí podkapitole, je k dispozici celá řada podpůrných materiálů usnadňujících aplikaci, resp. revizi aplikace GDPR ve školství.

1) **Metodické pokyny a doporučení zřizovatele** – zde hraje zásadní roli aktivita a přístup zřizovatele. Je-li škola zřizovaná krajem nebo větším krajským městem, jsou obvykle zpracovány velmi komplexní podklady. Některé příspěvkové organizace díky centrálnímu uchopení problematiky ze strany zřizovatele vzájemně spolupracují a výrazně tím zkvalitňují praktický přístup k ochraně osobních údajů spolu s úsporami nákladů.

2) **Webové stránky dozorového úřadu** – www.uoou.cz, které obsahují obrovské množství přehledně strukturovaných informací a v sekci „GDPR (obecné nařízení)“[128] v části „Základní informace“ rovněž velmi praktické rubriky[129]:
    a. Obecné nařízení (GDPR) stručně
    b. Základní příručka k ochraně údajů
    c. Desatero omylů
    d. Otázky a odpovědi k obecnému nařízení (GDPR)
    e. Role ÚOOÚ.

3) **Webové stránky ministerstva vnitra, sekce GDPR** – www.mvcr.cz/gdpr, které kromě celé řady vypořádaných dotazů, různých dokumentů a podkladů ze seminářů či školení obsahují dvě důležité sekce:
    a. Systémové analýzy[130] – jde o vzorové analýzy zpracování osobních údajů a připravenosti na obecné nařízení.
    Tato rubrika nabízí výstupy dvou rozsáhlých projektů:
        i. Systémová analýza krajů
        ii. Systémová analýza obcí – byť to z názvu projektu není patrné, obsahuje v souboru „Příloha č. 6 – Podřízené organizace“[131] částečnou vzorovou analýzu agend zpracování v příspěvkových organizacích obcí, mj. i mateřských a základních školách.
    b. Metodická podpora a konzultace

4) **Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR)[132]** – jedná se o rozsáhlý materiál popisující velmi komplexně problematiku ochrany a zpracování osobních údajů ve školství. Jak vysvětlí ve vlastní části práce kapitola 4.9, jedná se o značně kontroverzní dokument, který, byť to není ze stránek MŠMT na první pohled zřejmé, doznal po necelých dvou letech své existence velmi zásadních změn.

[128] *Úřad pro ochranu osobních údajů: GDPR (obecné nařízení)* [online]. [cit. 2021-01-13].
[129] *Úřad pro ochranu osobních údajů: Základní informace* [online]. [cit. 2021-01-13].
[130] *Ministerstvo vnitra: Systémové analýzy* [online]. [cit. 2020-12-28].
[131] *Ministerstvo vnitra: Systémové analýzy - Příloha č. 6 Systémové analýzy působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů* [online]. [cit. 01.03.2021].
[132] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) (aktuální web)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021].

3.9.3 Řízení projektu implementace, resp. revize implementace GDPR

Proces zavádění GDPR či revize souladu s tímto nařízením je relativně náročným projektem. Musí být tedy adekvátním způsobem řízen. Přes existenci mnoha principů řízení projektů se vždy určité prvky projektového managementu shodují. Návrh implementace GDPR pro potřeby naplnění cílů této práce původně vznikal na základě principu pro sestavení logického rámce dle projektového řízení IPMA.[133]

Dle této teorie je před zahájením obdobných projektů je obecně doporučeno[134]:

1. definovat cíl projektu,
2. stanovit konkrétní výstupy projektu,
3. stanovit okruhy nezbytných činností pro dosažení jednotlivých výstupů projektu,
4. určit záměr projektu,
5. ověřit dodržení vertikální logiky testem "jestliže – pak",
6. stanovit požadované předpoklady na každé úrovni,
7. definovat objektivně ověřitelné indikátory na úrovni: cíl; výstupy, záměr, činnost (časový a finanční rámec),
8. definovat prostředky a způsoby pro mentoring a ověřování,
9. sestavit rozpočet a určit zdroje (vytvořit kalkulaci nákladů na provedení jednotlivých činností),
10. realizovat ověřovací test návrhu pomocí kontrolního soupisu dotazů,
11. provést redesign návrhu projektu dle zkušeností z minulých projektů.

Pro čistě teoretické vymezení kroků a jejich posloupnost je projektové řízení IPMA dobrým vodítkem, nicméně ve vlastní části práce v kapitole 4.10 je navržen trochu odlišný postup než v této podkapitole uvedený.

Lze důvodně předpokládat, že osoby provádějící aplikaci GDPR ve školství budou buď přímo z vedení školy, případně budou na tuto nejvyšší složku řízení organizace tak úzce napojeni, že je neznalost nebo neschopnost koordinace kolektivu osob ani nezkušenost s řízením administrativních procesů nepravděpodobná. Proto je ve vlastní části práce navrženo zjednodušení procesního managementu při aplikaci GDPR. Jednotlivé kroky jsou

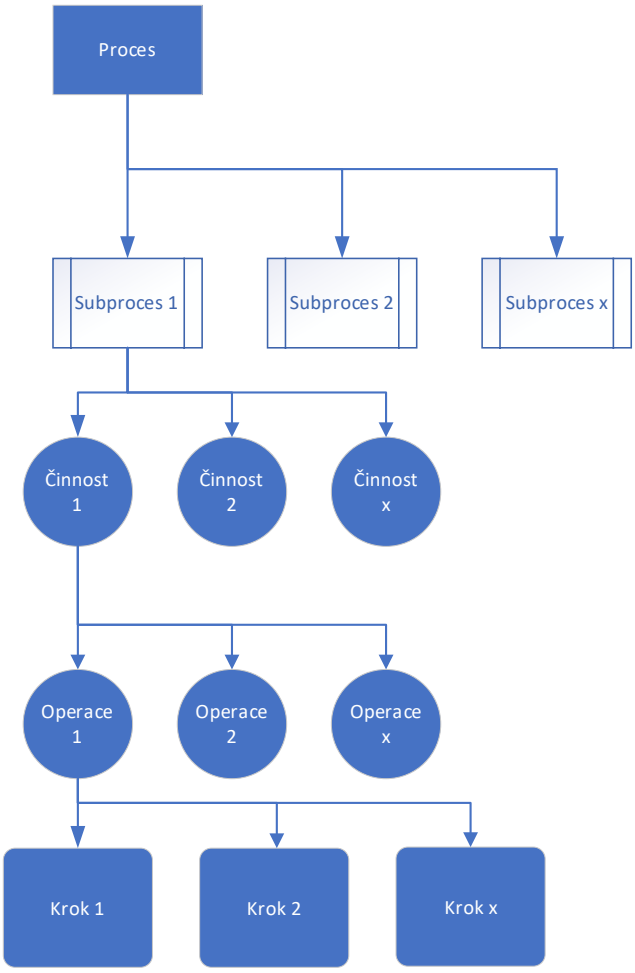
[133] Mezinárodní sdružení národních asociací projektových manažerů – International Project Management Association (IPMA), https://www.ipma.world/

[134] Doležal, J., Máchal, P., Lacko, B. *Projektový management podle IPMA*. Praha: Grada, 2012, s. 67-78. Expert (Grada).

voleny a chronologicky řazeny pro co nejširší pokrytí problematických oblastí administrativních i vzdělávacích procesů ve školských zařízeních. Pro efektivní naplnění cílů práce bez ohrožení úspěšnosti realizace celého procesu uvádění činností zpracování do souladu s GDPR svépomocí jsou ve vybraných oblastech přiměřeně detailizovány.

HIERARCHIE PROCESU

Pro účely orientace v hierarchii procesu jsou zejména v části práce popisující proces implementace (kapitola 4.10) používaná především označení „proces“, „subproces“, „činnost“, okrajově pak „operace“ a „krok“, přičemž užití těchto pojmů v procesní hierarchii je vyjádřeno na následujícím obrázku.[135]



Obrázek 2: Hierarchie procesu[136]

[135] Kříž, J. *Řízení administrativních a správních procesů*. V Praze: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2012, s. 12.
[136] Vlastní zpracování dle: Kříž, J. *Řízení administrativních a správních procesů*. V Praze: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2012, s. 12.

4 Vlastní práce

Tato analyticko-praktická část přebírá teoreticky vymezené, byť v mnoha případech již konkrétněji popsané, konstrukty z první části a zasazuje přímo do reálného prostředí základních a základních uměleckých škol. Vysvětluje tak nejen samotný postup implementace nařízení GDPR, ale zároveň zcela praktický pohled na dennodenně prováděné operace zpracování.

V rámci naplňování cílů práce, především cíle hlavního, je proveden detailní rozbor právních titulů zpracování, a to s cílem edukovat osoby provádějící implementaci (revizi implementace) GDPR za pomoci zde navržených postupů natolik, aby zvládli k jednotlivým identifikovaným procesům zpracování korektně přiřazovat nejen obecně známé účely zpracování, které jsou v prostředí školy v drtivé většině zákonem určeny, ale především právní tituly zpracování.

Obsahem této části je rovněž rozbor metodického doporučení MŠMT zmíněného mj. v kapitole 3.9.2 v bodu 4). Komparací dvou verzí metodického dokumentu, přičemž jedna z nich sehrála významnou úlohu v uvádění školských zařízení do souladu s GDPR, jsou získávány informace cenné pro naplňování dílčího cíle práce.

Před přípravou na samotnou implementaci, jejíž deskripce je rozdělena do jednotlivých kroků v závěru analyticko-praktické části, je třeba detailizovat a na praktických příkladech vysvětlit vybrané pojmy a principy nařízení GDPR, především pak nejdůležitější a nejrozsáhlejší zásadu zákonnosti (teoreticky vymezena v kapitole 3.5.1). Po zasazení pravidel do praktického prostředí přestanou být oním suchým abstraktním výkladem. Vedení školy v týmu s vybranými kmenovými zaměstnanci by tak nemělo činit velké komplikace provedení implementace obecného nařízení svépomocí.

Analyticko-praktická část již téměř nečerpá z dostupné literatury. Závěry v ní uvedené jsou výsledkem analýzy právních předpisů při znalosti reálného prostředí škol. Na rozdíl od teoretické části již není většinou aplikován obecný pohled na problematiku, téměř vše je viděno optikou školního prostředí. Byť se některé podkapitoly, například ty věnující se právním titulům zpracování, jeví hodny zařazení do teoretické části, bylo po pečlivém uvážení rozhodnuto o začlenění do vlastní části práce. Přínos plynoucí z jejich struktury a neoddělitelné provázanosti s praktickým prostředí školy by integrací mezi teorii dosti utrpěl.

4.1 Zákonnost zpracování dle čl. 6 obecného nařízení v praxi

Kapitola 3.5.1 teoreticky vymezila princip zákonnosti a představila šest právních důvodů definovaných čl. 6 obecného nařízení. Jejich znalost a představitelnost je zcela rozhodná pro pochopení smyslu nařízení, pro jeho implementaci a pro výkon práv subjektů.

Je zcela běžné, že v rámci jediné agendy, dokonce i jednoho procesu zpracování, je užití konkrétního údaje legitimizováno současně více právními důvody. V případě školy se může jednat například o prolínání veřejného a oprávněného zájmu při provozu kamerového systému (viz kapitola 4.6) nebo překrývání právního základu plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci s plněním právní povinnosti.

Detailní popis právních titulů zpracování spolu s praktickým použitím je v následujících šesti podkapitolách. Řazeny nejsou na základě své významnosti, chronologie byla převzata z příslušného článku GDPR.[137]

4.1.1 Souhlas se zpracováním osobních údajů

ZÁKLADNÍ PRAVIDLA PRO APLIKACI SOUHLASU SE ZPRACOVÁNÍM

Právní důvod zpracování *„subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů“*[138] je obecně nadužívaným právním titulem, ve školství obzvlášť. Důvodů je více. V prvé řadě jsou to zvyklosti dle původního zákona o ochraně osobních údajů. Dále je to domněnka, že fotografování osob lze tzv. přikrýt souhlasem se zpracováním osobních údajů ve smyslu nařízení GDPR, přičemž tato mylná hypotéza se stala pomalu axiomem. V prostředí škol je to také chybnými instrukcemi v metodickém materiálu MŠMT, které byly opraveny až v září 2019 (blíže viz kapitola 4.9).

Souhlas by měl být oproti tomu využíván okrajově a v podstatě až ve chvíli, kdy neexistuje jiná cesta k legitimizaci zpracování. Aby mohlo být zpracování založeno na souhlasu subjektu, musí být souhlas jednoznačným svobodným vědomým konkrétním projevem jeho vůle.[139]

Subjekt tedy musí mít vlastní zájem na zpracování, souhlasu nelze využívat v situaci, kdy škola údaje potřebuje pro efektivní vykonávání činnosti, nicméně je raději podpoří souhlasem. Takový přístup porušuje nařízení GDPR, v důsledku jde

[137] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1.
[138] *Ibid.*, čl. 6, odst. 1., písm. a).
[139] *Ibid.*, čl. 4, odst. 11).

o nepravdivé a nedostatečné naplnění informační povinnosti. **Nadbytečné souhlasy jsou deliktem, který může vyústit ve správní řízení s ÚOOÚ.** V subjektech vyvolávají falešný dojem, že mají zpracování svých osobních údajů pod kontrolou a mohou ho zastavit odvoláním souhlasu. Patologické pojetí tohoto právního titulu potvrzují i zástupci ÚOOÚ.[140]

Forma souhlasu není pevně stanovena, nemusí být tedy písemná, souhlas lze uzavřít i konkludentně, avšak důkazní břemeno leží na správci osobních údajů. Z toho důvodu je doporučeno uzavírat souhlasy písemně (v elektronické či listinné podobě).

V prostředí školy bychom se se souhlasy měli setkávat minimálně, protože absolutní většina zpracování probíhá v rámci plnění právní povinnosti v kombinaci s veřejným zájmem a výkonem veřejné moci.

Použití souhlasů je administrativně náročné a zpracování na nich založené neposkytuje škole silný právní základ pro zpracování. **Případné odvolání souhlasu musí být pro subjekt stejně snadné jako jeho poskytnutí a případné neposkytnutí souhlasu ze strany subjektu pro něj nesmí mít nepříznivý dopad.** Škola tedy nemůže podmínit poskytnutí nějaké služby, účast na nějaké akci či čerpání určitých výhod udělením souhlasu se zpracováním osobních údajů. **Souhlas lze kdykoliv odvolat a zpracování na něm postavené musí být neprodleně ukončeno a osobní údaje příslušného subjektu, neexistuje-li pro ně jiný legitimní právní důvod zpracování, musí být zlikvidovány.** Proto se právní důvod „souhlas se zpracováním osobních důvodů“ aplikuje až v případě, že neexistuje jiná cesta, tedy jiný zákonný důvod zpracování (viz podkapitoly 4.1.2 až 4.1.6).

Obecně platí, že existuje-li jiný zákonný důvod pro zpracování, nesmí být za žádných okolností využíván institut souhlasu.

VĚKOVÁ HRANICE ZPŮSOBILOSTI ŽÁKA K UDĚLENÍ SOUHLASU SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ A SLUŽBY INFORMAČNÍ SPOLEČNOSTI

V praxi se ukazuje, že určení věkové hranice způsobilosti dítěte k poskytnutí souhlasu se zpracováním není vůbec snadné. Je to mj. dispozitivním ustanovením obecného nařízení definujícím pravidla pro poskytnutí souhlasu dítětem, ovšem pouze ve vztahu ke službám informační společnosti.

Konkrétně článek 8 v kontextu těchto služeb nabízených dítěti definuje jako legitimní zpracování osobních údajů *„je-li dítě ve věku nejméně 16 let“*. V případě, že je mladší, *„je*

[140] MATOUŠOVÁ, M. *Konzultace pro pověřence pro ochranu osobních údajů, Praha 9. října 2018*. Praha: Úřad pro ochranu osobních údajů, 2018.

takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti“, přičemž GDPR připouští, že *„členské státy mohou pro uvedené účely právním předpisem stanovit nižší věk, ne však nižší než 13 let“*.[141]

Problematické je období mezi účinností GDPR a přijetím ZZOÚ (viz „ETAPA II“ v kapitole 3.3.4), ale i samotný pojem „služby informační společnosti“. Takové služby poskytuje i škola a v praxi jsou nejčastějším prostorem, mnohdy dokonce jediným, pro případný souhlas se zpracováním. Přitom je právě v tomto případě mnohdy opomíjený.

Ve smyslu evropského práva je službou informační společnosti služba poskytovaná zpravidla za úplatu, ne však výlučně (školy je pochopitelně nezpoplatňují), dále poskytovaná na dálku a elektronicky.[142] Zejména v období pandemie covidu-19, kdy je elektronizace školních systémů a výukových kanálů na vzestupu, je vhodné při revizi souladu s GDPR učinit inventuru zpracování a posoudit pravidla pro zakládání účtů žákům do těchto systémů.

Jde například o tyto vzdáleně přístupné školní, či školou řízené, systémy:

- školní e-mailové schránky (mnohdy navázané na další služby),
- cloudové služby zprostředkované školou, například od společností Microsoft (Microsoft 365 či Office 365 Education[143]) nebo Google (G Suite či Google Apps pro vzdělávání[144]), včetně účtů pro online úložiště, jako jsou Microsoft OneDrive, Google Disk či Apple iCloud,
- systémy pro distanční výuku, ve kterých je žákům vytvořen školní účet (mezi nejznámější patří například Google Meet, Microsoft Teams, Zoom Meeting),
- školní systémy pro testování žáků, pro organizaci výukových materiálů, případně pro poskytování informací o prospěchu žákům i jejich zákonným zástupcům (například Moodle, Google Classroom a Bakaláři),
- systémy pro elektronické žákovské knížky,
- další webové aplikace, školní portály apod.

[141] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 8. odst. 1.
[142] EVROPSKÁ UNIE. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (kodifikované znění). In: *EUR-Lex*. Štrasburk, Úř. věst. L 241/1, 2015/1535, čl. 1, odst. 1., písm. b).
[143] *Microsoft: Office 365 Education (https://www.microsoft.com/cs-cz/education/products/office)* [online]. [cit. 2021-03-07].
[144] *Google Workspace for Education (https://edu.google.com/products/workspace-for-education/education-fundamentals)* [online]. [cit. 2021-03-07].

Pokud však bude škola aplikovat právní titul „souhlas se zpracováním osobních údajů“ žáků na zpracování, která nejsou službou informační společnosti, pravidla jsou upravena odlišně. Nebude-li z oficiálních stanovisek dozorového úřadu a z rozhodovací praxe soudu naprosto zřejmé, že bude akceptován níže uvedený výklad § 31 občanského zákoníku, tedy že bude legitimní čistě subjektivní posuzování rozumové a volní vyspělosti dětí poskytujících škole souhlas, nelze v žádném případě doporučit školám se k tomuto právnímu důvodu jakkoliv upínat. Aktuálně by souhlas se zpracováním nespadajícím mezi služby informační společnosti měla poskytovat pouze osoba vykonávající rodičovskou povinnost (jde-li o zpracování osobních údajů nezletilých). **Osoba mladší 18 let k poskytnutí souhlasu není způsobilá.**

I v případě, že jde nesporně o souhlas se zpracováním v rámci služeb informační společnosti, je přesto určení správné věkové hranice komplikované. V období mezi 25. květnem 2018 (den účinnosti GDPR) do 24. dubna 2019 (den účinnosti adaptačního zákona) byla konkrétní věková hranice velmi nejasná a její určení bylo spíše na subjektivním posouzení správce. Byť nařízení GDPR stanovilo příslušný věk na 16 let, i přes absenci adaptačního zákona existovalo, a stále existuje, ustanovení občanského zákoníku, které je na tuto problematiku v rámci „správného“ odvážnějšího právního výkladu uplatnitelné. Adekvátnost aplikace § 31 občanského zákoníku mj. potvrdil opakovaně i dozorový úřad[145].

Ustanovení *„má se za to, že každý nezletilý, který nenabyl plné svéprávnosti, je způsobilý k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jeho věku“*[146] v podstatě znamená, že žák, který je s to posoudit následky poskytnutí souhlasu se zpracováním osobních údajů škole například při zakládání školního e-mailu, jej může toliko poskytnout. Lze pochopitelně doporučit obezřetné aplikování tohoto způsobu opatřování souhlasů a podpořit jej vždy kvalitním informováním zákonných zástupců. V celé této problematice hraje velkou úlohu i povědomí rodičů o online prostředí, kdy nejsou tito mnohdy schopni objektivně posoudit, s čím vlastně souhlas udělují, protože virtuálnímu světu informačních a komunikačních technologií rozumí méně než jejich nezletilí potomci.

[145] *Rozhovor moderátora ČT Tomáše Drahoňovského s Veronikou Křížovou v pořadu 90’ ČT24* [online]. čas videa 01:10.
[146] Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2012, částka 33, číslo 89, § 31.

S účinností ZZOÚ je předmětný problém upraven ustanovením *„dítě nabývá způsobilosti k udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku“*[147].

Pokud tedy škola souhlasy dětí ve zde uvedených případech používá, a především aplikovala-li je před účinností ZZOÚ nebo dokonce před příchodem GDPR, měla by provést revizi na soulad se stávající právní úpravou s retroaktivním účinkem a respektovat hranici 15 let věku.

PRAKTICKÉ PŘÍKLADY SPRÁVNÉHO POUŽITÍ SOUHLASŮ ŠKOLOU

Souhlas se zpracováním osobních údajů škola může škola použít

(a) **ve vztahu ke zpracování osobních údajů žáků** zpravidla jen ve třech případech:

- při zřizování přístupů k online službám (viz výše)
- při následném zpracování jinak legitimně pořízených fotografií, časově omezených audiovizuálních záznamů či oprávněně získaných uměleckých prací (např. výkresy) opatřených identifikací žáka nebo umožňující jeho identifikaci, a to pro jiné než běžné účely – například bude-li chtít škola tyto údaje využít pro reklamní účely nebo komerční činnost (blíže viz také kapitola 4.6 věnovaná fotografování)
- zpracování údajů při dobrovolných akcích, např. dotazníkových šetřeních

(b) **Ve vztahu k pedagogům** se souhlasy aplikují ojediněle, příkladem může být:

- zveřejnění fotografií spolu se jmény učitelů na webových stránkách školy
- vyslání zaměstnance školy na zahraniční služební cestu a předávání jeho osobních údajů na základě jeho souhlasu se zpracováním osobních údajů dalším správcům (například za účelem uzavření cestovního pojištění či odbavení zavazadel u leteckého přepravce)

(c) **Ve vztahu návštěvníkům webových stránek**:

- souhlas s rozšířeným zpracováním tzv. cookies při sledování aktivit uživatelů webových stránek

V této souvislosti je doporučeno zpracovávat pouze nezbytné informace, např. technické cookies soubory, neboť Evropský sbor pro ochranu osobních údajů (EDPB) se již

[147] Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 110, § 7.

vyjádřil k zákonnosti velmi rozšířené praxe tzv. *„cookie walls“* a označil ji za nepřípustnou. Jde o vyskakovací okno umístěné přes webovou stránku za účelem informování návštěvníka www stránky o použití souborů cookies, a to bez možnosti odmítnutí. Jedinou cestou k zobrazení obsahu je kliknutí na tlačítko „přijmout“, „souhlasím“ apod. Tuto techniku vynuceného souhlasu využívá celá řada webů a bude se pravděpodobně stávat předmětem šetření ÚOOÚ.[148]

PŘÍKLADY CHYBNÉHO POUŽITÍ SOUHLASŮ ŠKOLOU

Při prakticky prováděných analýzách byly zaznamenány až kuriózní případy aplikace souhlasů se zpracováním osobních údajů. Jejich výčet by vydal na samostatnou práci, nicméně ty nejčastěji opakované je vhodné pro příklad uvést.

Příklad **nesprávného** použití institutu „souhlas se zpracováním“:

- souhlas s fotografováním – nařízení GDPR ani navazující adaptační zákon neřeší samu podstatu pořizování fotografií (blíže vysvětleno v kapitole 4.6)
- souhlas se zpracováním osobních údajů zákonných zástupců dětí pro potřeby kontaktovat je školou (disponovat kontaktními údaji na nositele rodičovské povinnosti je i v zájmů dětí)
- souhlas se zpracováním osobních údajů osob vyzvedávajících děti ze školní družiny (je povinností školy takové údaje zpracovávat, nelze na ně aplikovat souhlas)
- souhlas se zpracováním jména dítěte na kresbách umístěných například na nástěnce ve škole
- souhlas s využitím fotografií pro reportážní činnost (např. oznámení jména vítěze v matematické olympiádě spolu s uveřejněním fotografie v místním tisku či na školním webu)
- souhlas se zpracováním údajů v rámci poradenských služeb (např. při spolupráci s Pedagogicko-psychologickou poradnou)
- souhlas se zpracováním při uschování průkazů pojištěnce u pedagoga například na školním výletě, škole v přírodě apod. (**jde o depositum, ne o zpracování**, uschování osobních dokladů i dalších cenností, bez ohledu na jejich obsah, tedy zda obsahují osobní údaje, upravuje občanský zákoník v § 2402–2408)

[148] Guidelines 05/2020 on consent under Regulation 2016/679. *European Data Protection Board Guidlines* [online]. 2020, č. 05 [cit. 2021-02-19].

- souhlas se zpracováním údajů poskytovaných OČTŘ nebo zdravotnickým pracovníkům při testování žáků na přítomnost návykových látek
- souhlas se jmenovkami na skřínkách žáků
- generální obecné souhlasy s rozsáhlým výčtem údajů definované na dobu školní docházky – s ukončením docházky v 9. třídě takový souhlas automaticky exspiruje a škola musí likvidovat veškeré údaje zpracovávané pod tímto souhlasem i bez jeho odvolání.

V praxi byly zachyceny i velmi absurdní souhlasy se zpracováním sestavené ve smyslu nařízení GDPR, proto je důrazně doporučeno jim spolu s informacemi pro subjekty nastavit při revizi souladu s GDPR vysokou prioritu.

4.1.2 Plnění smlouvy nebo opatření před uzavřením smlouvy

Na základě tohoto právního titulu, v obecném nařízení definovaného jako zpracování *„nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů“*[149], je možné zpracovávat osobní údaje nezbytné pro uzavření smlouvy či pro její plnění.

Osobní údaje smluvních stran je možné zpracovávat ještě před samotným uzavřením smlouvy, pokud je to pro její přípravu nezbytné, proto je v rámci toho zákonného základu zmíněno „*opatření před uzavřením smlouvy na žádost subjektu“*. Pokud k uzavření smlouvy nakonec nedojde, je třeba osobní údaje zlikvidovat, neexistuje-li pro ně další právní důvod zpracování. Je běžné, že jsou údaje zpracovávané během procesu přípravy smluv ukládány přiměřenou dobu i v případě následného neuzavření smluv. Je to pro případné dokazování transparentnosti a zákonnosti jednání školy, jakožto OVM a subjektu financovaného z veřejného rozpočtu, a pro případnou obhajobu právních nároků.

V situacích, kdy smlouvy exspirují či jsou vypovězeny, zaniká právní důvod zpracování „plnění smlouvy“, avšak velká část osobních údajů přechází standardně pod jiné tituly zpracování. Existuje celá řada legitimních důvodů, proč jsou smlouvy a v nich uvedené nebo na základě nich zpracovávané osobní údaje uloženy či zpracovávány i po vypršení/ukončení smlouvy. Jedná se například o povinnost archivace, prokázání nároku na uplatnění záruky a v oprávněném zájmu také jako podklady pro přípravu nové smlouvy.

[149] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1., písm. b).

PŘÍKLADY ZPRACOVÁVÁNÍ NA ZÁKLADĚ SMLUV:

- pracovní smlouvy (zpracování na základě pracovních smluv probíhá většinou z důvodu plnění právní povinnosti, jedná se například o přípravu těchto smluv)
- smlouvy s dodavateli služeb nebo zboží
- nájemní smlouvy
- prodej nepotřebného majetku
- smlouvy s pojišťovnami
- smlouvy s pořadateli různých akcí (např. umělecká vystoupení)

Při revizi souladu s GDPR je vhodné zkontrolovat platné smlouvy proti evidenci ve spisové službě a revidovat nastavení skartačních lhůt, nikoliv za účelem jejich likvidace přesně s uplynutím doby uložení, ale naopak pro správné nastavení data skartace, aby nebyla zlikvidována smlouva, kterou si v oprávněném zájmu potřebuje škola ponechat.

4.1.3 Plnění právní povinnosti

Ustanovení „*zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje*“[150] je nejsnáze aplikovatelným a nejčistěji používaným právním titulem zpracování v prostředí správců z veřejného sektoru, školy nevyjímaje. Použije se na zpracování osobních údajů nezbytná pro splnění zákonné povinnosti, která se na školu vztahuje. Tento právní důvod je však u orgánů veřejné moci velmi úzce provázaný s právním důvodem „veřejný zájem nebo výkon veřejné moci“ (viz podkapitola 4.1.5.).

Poměrně rozsáhlý přehled právních předpisů upravujících činnosti školy je uveden v kapitole 3.9.1, pro představu je zde pouze několik příkladů. V praxi probíhá zpracování absolutní většiny osobních údajů právě na základě tohoto právního základu.

Zpracováním údajů žáků je škola povinována především na základě školského zákona a vyhlášce o základním vzdělávání, níže uvedené názvy agend v podstatě odpovídají účelům zpracování.

PŘÍKLADY ZPRACOVÁVÁNÍ NA ZÁKLADĚ PRÁVNÍ POVINNOSTI:

- zápisy k povinné školní docházce a rozhodování o odkladech
- školní matrika

[150] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1., písm. c).

- třídní kniha
- evidence omluvenek a žádostí o uvolnění
- evidence úrazů
- IVP (individuální vzdělávací plány)
- poskytování podpůrných opatření
- přestupy žáků na jinou školu
- organizace akcí konaných mimo školu (např. školní výlety, umělecká vystoupení, sportovní soutěže, školy v přírodě, lyžařské výcviky apod.; zde je typický překryv s právním titulem v kapitole 4.1.5)
- povinná školení zaměstnanců (BOZP, PO)[151]
- vedení účetnictví
- mzdová agenda
- personalistika
- spisová služba
- agenda informačního zákona
- agenda registru smluv
- … desítky dalších procesů zpracování při plnění zákonných povinností

Zpracování osobních údajů prováděné na základě právní povinnosti můžeme zjednodušeně vnímat jako téměř neomezitelné ze strany legislativy vztahující se na ochranu a zpracování osobních údajů a ze strany subjektů v rámci výkonu jejich práv. Je však třeba dodržovat základní principy, především bezpečnost zpracování, ochranu údajů před zneužitím a zajištění důvěryhodnosti a integrity těchto údajů. Tato obecná pravidla ovšem platila dávno před účinností obecného nařízení.

4.1.4 Ochrana životně důležitých zájmů

Je-li zpracování *„nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby“*,[152] půjde pravděpodobně o situace, kdy je okamžité posuzování souladů s obecným nařízením zcela irelevantní, nicméně právní důvod takového potenciálního zpracování může být pro vybrané agendy deklarován předem.

[151] Bezpečnost a ochrana zdraví při práci, požární ochrana
[152] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1., písm. d).

Životně důležitý zájem iniciující zpracování osobních údajů nastává v případě nezbytnosti zpracovávání **za účelem předejití vzniku závažné újmy subjektu údajů** nebo jiné osoby a právo na ochranu těchto zájmů stojí nad právem na ochranu osobních údajů dalších osob, případně přímo ohroženého subjektu. Typicky jde o ohrožení života a zdraví.

Tohoto právního titulu je obvykle využíváno náhle a přirozeně a vždy **jen za situací neumožňujících aplikaci jiného právního titulu zpracování.**

PŘÍKLADY ZPRACOVÁNÍ PŘI OCHRANĚ ŽIVOTNĚ DŮLEŽITÝCH ZÁJMŮ (VE VZTAHU K OSOBNÍM ÚDAJŮM ŽÁKŮ):

- Žák utrpěl úraz nebo je z jiného důvodu ve stavu vyžadujícím lékařskou pomoc – v takovém případě dochází k nelimitovanému zpracování údajů nutných pro naplnění účelu zpracování, kterým je odvrácení nepříznivého, zdraví či život ohrožujícího stavu. Může jít o údaje z osobních dokladů, průkazu pojištěnce nebo citlivých informací o zdravotních omezeních, alergiích apod., tedy údajů ze zvláštní kategorie osobních údajů (viz kapitola 3.4.1).
- Žák nízkého věku se nachází ve školní družině a zákonní zástupci se náhle ocitnou v situaci zabraňující jeho vyzvednutí. Telefonicky nahlásí osobě odpovědné za provoz družiny osobní údaje jiné osoby, která bude schopná dítě vyzvednout. Účelem zpracování bude ověření totožnosti osoby při převzetí dítěte z družiny.

Byť druhý uvedený případ nevyvolává pochybnosti o právu dítěte neutrpět neopodstatněnou újmu, které nesporně převyšuje právo jiné osoby na ochranu osobních údajů, je zde uveden z důvodu, že k takové situaci skutečně došlo. V rámci konzultací s pověřenci to potvrdili pracovníci ÚOOÚ.

S odůvodněním, že škola nemá souhlas se zpracováním osobních údajů osoby, která převezme dítě v družině, byla situace eskalována na OSPOD[153] a dítě nebylo náhradní osobě určené rodiči s odvoláním na GDPR předáno.

Obecně a přirozeně se předmětný právní základ uplatní, nachází-li se fyzická osoba v takovém zdravotním stavu, že není s to poskytnout souhlas se zpracováním, případně subjekt, jehož údaje mají být zpracovány, není přítomen, a vyžádání si souhlasu se

[153] Orgán sociálně-právní ochrany dětí

zpracováním prováděným v zájmů ochrany života či zdraví jiné fyzické osoby by vyžadovalo nepřiměřené úsilí.

4.1.5 Plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci

Právní důvod *„zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce“*[154] je, jak již bylo uvedeno v podkapitole 4.1.3, velmi úzce provázán s plněním právní povinnosti.

Důvody, proč je nutné tyto právní tituly správně identifikovat a oddělovat, jsou především zásada transparentnosti (viz kapitola 3.5.1) a právo subjektu podat námitku proti zpracování (viz kapitola 3.6.7). Subjekt musí obdržet relevantní informace o právním základu, aby nebyl zkrácen na výkonu svých práv. Právo na podání námitky je totiž u zpracování prováděném při plnění právní povinnosti potlačeno.

OVM jsou nuceny při výkonu své působnosti velmi často zpracovávat širokou škálu osobních údajů, které jsou klíčové pro správné rozhodování a efektivní výkon veřejné moci. Taxativní výčet takových údajů by nebyl v rámci právních předpisů zřizujících příslušný OVM či řídících jejich činnost prakticky realizovatelný.

V prostředí základních škol je příkladem výkonu veřejné moci rozhodování ředitele školy o přijetí/nepřijetí dítěte k základnímu vzdělávání. Rozhodování probíhá dle správního řádu a v souladu se školským zákonem, ovšem tyto předpisy nikdy nemohou predikovat a taxativně uvést celé penzum osobních údajů nezbytných pro rozhodování. To se projevuje obzvláště při rozhodování o negativních kázeňských opatřeních, tedy například o podmíněném vyloučení, případně vyloučení (pochopitelně aplikovatelné až po splnění devíti let školní docházky). Ředitel musí v takto závažných případech posuzovat pečlivě celou řadu okolností, rozhodnutí má velmi závažné důsledky na takto vyloučeného žáka. Pokud je pro správné rozhodnutí a jeho zdůvodnění důležité, bude škola zpracovávat osobní údaje dalších osob v kontextu s jejich rolí v konkrétním řešeném případu porušení školského zákona, případně dojde k opodstatněnému rozšíření rozsahu zpracovávaných informací o účastnících správních řízení a není nutné hledat oporu přímo v právních předpisech.

[154] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1., písm. e).

Pojem „veřejný zájem“ je poněkud abstraktnější než „výkon veřejné moci“. Přestože jsou oba pojmy součástí jediného ustanovení, jejich aplikace je dle okolností odlišná. Veřejný zájem lze chápat jako *„soubor všech zájmů, které se slučují a potkávají v pojmu obecné dobro“*[155]. Úloha veřejné školy v rámci systémů bezplatného vzdělávání je pro tzv. „obecné dobro“ celé společnosti nezpochybnitelná.

Posláním škol, umělecké školy nevyjímaje, je děti nejen „plnit“ vědomostmi, ale vzdělávat je rovněž kulturně, vychovávat je, socializovat, integrovat je do společnosti a připravovat na celý budoucí život. V rámci těchto úkolů je nutné řešit předem nespecifikovatelné situace, se kterými přirozeně souvisí zpracovávání osobních údajů. Je-li takové zpracování prováděno právě v duchu veřejného zájmu, je zcela legitimní a není pro ně třeba hledat jiný právní důvod.

Přestože nařízení GDPR nevyžaduje provádění tzv. balančního testu (blíže popsán v kapitole 3.6.7 „Právo vznést námitku“) před započetím zpracování, jako je to u dále popisovaného právního titulu „oprávněný zájem správce či třetí strany“, je vhodné spatřovat v těchto titulech určitou paralelu. Zpracování je vhodné zrychleně posoudit analogicky s postupy pro balanční test ještě před spuštěním zpracování, u kterého není zcela zjevné, že k narušení práv a svobod osob nemůže dojít.

PŘÍKLADY ZPRACOVÁNÍ PŘI PLNĚNÍ ÚKOLU VE VEŘEJNÉM ZÁJMU NEBO PŘI VÝKONU VEŘEJNÉ MOCI:

- Veškerá rozhodování podle správního řádu[156, 157, 158]

  <u>Základní školy – rozhodování o:</u>

  - výchovných opatření
    - pochvaly nebo jiná ocenění
    - napomenutí, důtky
    - rozhodnutí o podmíněném vyloučení nebo o vyloučení (podmíněno splnění povinné školní docházky)
  - přeřazení žáka do vyššího ročníku

[155] Rychetský, P., Langášek, T., Herc, T., Mlsna, P. *Ústava České republiky*. Praha: Wolters Kluwer, 2015, odstavec 3. komentáře čl. 30. Komentáře (Wolters Kluwer ČR).
[156] Zákon č. 561/2004 Sb., o předškolním, základním středním, vyšším odborném a jiném vzdělávání (školský zákon). In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2004, částka 190, číslo 561.
[157] Puškinová, M., Rigel, F. *Správní řízení v praxi škol a školských zařízení* [PDF]. Praha: Wolters Kluwer, 2016, s. 286, 535, 573. Řízení školy (Wolters Kluwer).
[158] Vyhláška č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2005, částka 11, číslo 48.

- zamítnutí žádosti o přeřazení žáka do vyššího ročníku
- povolení/nepovolení vzdělávání podle individuálního vzdělávacího plánu (žák se speciálními vzdělávacími potřebami)
- povolení/nepovolení odkladu povinné školní docházky
- povolení „dodatečného" odkladu povinné školní docházky
- přijetí/nepřijetí k základnímu vzdělávání
- povolení/nepovolení přestupu do jiné základní školy
- převedení/nepřevedení žáka do jiného vzdělávacího programu
- povolení/nepovolení pokračování v základním vzdělávání
- povolení/nepovolení opakování ročníku
- povolení/nepovolení individuálního vzdělávání žáka
- ukončení individuálního vzdělávání žáka
- zařazení/nezařazení dítěte do přípravné třídy základní školy
- zařazení/nezařazení dítěte do přípravného stupně základní školy speciální

<u>Základní umělecké školy – rozhodování o:</u>

- výchovných opatření
  - pochvaly nebo jiná ocenění
  - napomenutí, důtky
  - rozhodnutí o podmíněném vyloučení nebo o vyloučení
- přijetí/nepřijetí k základnímu uměleckému vzdělávání
- prominutí/nepovolení prominutí, snížení úplaty za základní umělecké vzdělávání

<u>Školní družiny – rozhodování o:</u>

- výchovných opatření
  - rozhodnutí o podmíněném vyloučení nebo o vyloučení
- přijetí/nepřijetí k zájmovému vzdělávání ve školní družině či školním klubu
- prominutí/nepovolení prominutí, snížení úplaty za zájmové vzdělávání

- Pořizování záznamů kamerovým systémem za účelem ochrany dětí a zvýšení bezpečnosti ve škole (systém není provozován v oprávněném zájmu např. pro kontrolu zaměstnanců – blíže viz kapitola 4.6)

- Používání fotografií žáků a časově omezených audiovizuálních záznamů a jejich přiměřené zveřejňování, a to pro účely reportážní činnosti, informování o činnostech školy, dokumentování pedagogických postupů apod.)
- Používání a přiměřené zveřejňování autorských děl žáků (typicky umělecká, akademická a literární činnost)
- Zpracování údajů při pořádání akcí mimo školu (např. školní výlety, umělecká vystoupení, sportovní soutěže, školy v přírodě, lyžařské výcviky apod.)
- Zpracování údajů v souvislosti s opatřeními přijímanými v rámci boje s infekčními chorobami a při ochraně veřejného zdraví (velmi aktuální téma v souvislostí s globální pandemií covidu-19)
- Další zpracování prováděná za účelem vzdělávání a organizace vzdělávání, nejsou-li explicitně určena právním předpisem

Jak bylo vysvětleno v úvodu této kapitoly, zpracování dle zde popisovaného právního titulu je úzce svázáno s plněním právní povinnosti a u mnoha agend budou uvedeny oba tyto právní důvody. Jejich odlišení by bylo možné pouze v případě analýzy zpracování nikoliv na úrovni agend, ale na úrovni jednotlivých činností v rámci procesů zpracování, a to detailně k jednotlivým osobním údajům, což je prakticky nereálné. Takto zevrubné monitorování a analyzování by bylo nepřiměřené a v konečném důsledku by bylo administrativně a technologicky náročnější než samo zpracování.

4.1.6 Oprávněný zájem správce či třetí strany

Tento právní titul se použije na zpracování, které je *„nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě“*[159]. Vyznačuje se obecně velmi širokým právním základem, avšak s nemalou mírou rizika, v prostředí školy umocněnou dovětkem v názvu právního titulu „pokud je subjektem údajů dítě“. Přesto zpracování prováděných v oprávněném zájmu není v prostředí škol málo (viz praktické příklady níže).

Riziko spočívá ve velmi snadném napadení zpracování prováděném v oprávněném zájmu, protože případná námitka subjektu přeruší zpracování do doby vypořádání námitky.

[159] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1., písm. f).

Oním vypořádáním je mj. povinné provedení testu proporcionality, tzv. balančního testu, blíže popsaného v kapitole 3.6.7 „Právo vznést námitku“.

Školy sahají k tomuto právnímu základu zpracování v situacích, kdy se nenacházejí ve vrchnostenském postavení orgánu veřejné moci, ale např. v roli zaměstnavatelů v pracovním právu nebo vystupují-li jako soukromoprávní subjekt v rámci dodavatelsko-odběratelských vztahů. Nejčastěji jde o zpracování v tzv. provozních agendách při zajišťování běžného provozu školy, které ovšem není explicitně stanoveno zákonem.

Často jde o nezbytně nutné zpracování osobních údajů pro účely zamezení podvodům, krádežím, vyzrazení tajemství, ochrany majetku a efektivní komunikace.

PRAKTICKÉ PŘÍKLADY ZPRACOVÁNÍ PROVÁDĚNÝCH ŠKOLOU NA ZÁKLADĚ OPRÁVNĚNÉHO ZÁJMU:

- Pořizování záznamů kamerovým systémem provozovaným primárně za účelem ochrany majetku a kontroly osob (kamery umístěny obvykle na plášti budovy či v provozních prostorech, systém není primárně určen pro ochranu dětí)
- Marketingová činnost a propagace školy komerčního charakteru
- Sledování služebních vozidel (např. GPS pro omezení zneužívání vozidel k soukromým účelům)
- Docházkové systémy (evidence pracovní doby je zákonná povinnost, ale provoz např. elektronického docházkového systému je oprávněným zájmem školy, nikoliv povinností)
- Provoz zabezpečovacích systémů (při aktivací/deaktivaci dochází ke sběru informací o osobě, která tak činí, a to spolu s geolokačním údajem – tedy kde se v danou chvíli osoba nachází)
- Sledování provozu počítačových sítí (např. sběr bezpečnostních logů a sledování přístupu do informačních systémů)
- Sledování telekomunikačního provozu (např. podrobné výpisy pro kontrolu případného zneužívání služebních telefonů)
- Přiměřené monitorování zaměstnanců v souladu se zákoníkem práce (bez nepřiměřeného zásahu do soukromí je přípustné)
- Sběr kontaktních údajů (blíže rozvedeno na konci této podkapitoly)
    - obchodních partnerů (např. dodavatelů zboží a služeb)

    - zákonných zástupců dětí nad rámec povinného rozsahu (telefonní číslo a e-mailová adresa; adresa bydliště je povinným údajem)
    - vlastních zaměstnanců (soukromá telefonní čísla a e-mailové adresy)
    - na další osoby (např. z jiných škol či spolupracujících organizací)
- Obchodní korespondence v rámci soukromoprávních vztahů (v situaci, kdy škola nevystupuje ve vrchnostenském postavení OVM)
- Uchování životopisů neúspěšných uchazečů o zaměstnání (možnost obhajovat případné právní nároky při prokazování transparentnosti výběrového řízení; použití v případě uvolnění pracovního místa v horizontu několika měsíců po výběrovém řízení; přiměřená doba uložení bývá stanovována na 1 rok)
- Záznamy o provedených školeních (obecně dobrovolných, tedy ne zákonem určených školeních; příkladem je záznam o absolvování školení v oblasti ochrany a zpracování osobních údajů nebo kybernetické bezpečnosti).

Výčet je velmi ilustrativní, potenciálně existuje mnoho dalších agend, které škola nevede v rámci výkonu veřejné moci nebo z důvodu uloženého právním předpisem, ale činí tak v oprávněném zájmu a v dobré víře, že její zájem převažuje nad zájmy subjektů nebýt předmětem zpracování a nezasahuje nepřiměřeně do jejich práv a svobod. O zpracování osobních údajů žáků se však jedná zřídka, s výjimkou kamerových systémů, u kterých nejde zamezit jejich zachycení, pohybují-li se ve střeženém prostoru.

KONTAKTY NA SUBJEKTY – TELEFONNÍ ČÍSLA, E-MAILOVÉ ADRESY

Protože dochází k častým diskusím ohledně sběru kontaktních údajů na rodiče dětí, případně jejich další příbuzné (např. kvůli přebírání dětí ze školy nebo školní družiny), ale i na zaměstnance školy, jakou jsou soukromá telefonní čísla a e-mailové adresy, je v této souvislosti vhodné vyvrátit dvě zcela protichůdné domněnky.

Jsou názory, že je nutné opatřit například kontakty na rodiče žáků nebo na vlastní zaměstnance souhlasem se zpracováním osobních údajů, naproti tomu stojí přesvědčení, že sběr těchto údajů je právní povinností a škola je zpracovávat musí. **Ani jeden z těchto konceptů není správný**.

Uchování této kategorie kontaktních údajů na rodiče a další rodinné příslušníky (typicky telefonní čísla a e-maily) není zákonnou povinností, ale **oprávněným zájmem školy**. Ve vybraných případech může jít i o zájem veřejný, který lze dovodit ze zájmu dětí, aby v případě nenadálých situací mohla škola s rodiči a dalšími osobami efektivně a rychle

komunikovat. O veřejný zájem půjde i v případě kontaktů na specifickou skupinu zákonných zástupců spolu s údaji o zaměstnání pro případ krizového řízení a pro nenadálé situace. Při živelních katastrofách může vyvstat potřeba zvláštního přístupu k dětem, jejichž rodiče jsou členy integrovaného záchranného systému či ozbrojených složek.

Argumentem, proč není možné telefonní číslo a e-mailovou adresu na rodiče ani zaměstnance zpracovávat pod právním titulem „právní povinnost", je absence právního předpisu, který by v ČR ukládal osobám disponovat telefonním číslem nebo e-mailovou adresou. Odmítne-li rodič tyto údaje poskytnout, musí to škola respektovat bez ohledu na to, zda zákonný zástupce telefonní číslo a e-mail má či nikoliv. Jedná se o dva z údajů, na které lze jednoduše aplikovat i právo na výmaz.

U zaměstnanců připadá v úvahu zpracování těchto kontaktních údajů pod právním titulem „plnění smlouvy", definují-li si obě strany podmínky pro předmětné osobní údaje v pracovní smlouvě. Evidence služebních telefonních čísel a e-mailových adres je nesporně oprávněným zájmem a zde o oprávněnosti školy nikdy pochyb nebude, dokonce ani při uveřejnění na stránkách školy.

Ostatní kontaktní údaje (rodiče ani zaměstnanců) nejsou žádnými úvahami o aplikaci správného právního titulu dotčeny. Zpracování adres bydliště a jmen osob je povinností školy. Nařízení GDPR k tomuto ještě uvádí, že *„existenci oprávněného zájmu je v každém případě třeba pečlivě posoudit"*, tedy provést již zmíněný test proporcionality (viz kapitola 3.6.7 „Právo vznést námitku) *„včetně toho, zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít."*[160] Je nepravděpodobné, že by v dnešní době nějaký subjekt nepředpokládal, že ve výše uvedených případech budou zpracovávány soukromá tel. čísla a e-mailové adresy.

4.2 Praktický výkon práv subjektů v prostředí veřejných škol

Tato kapitola úzce navazuje na teoretické vymezení práv subjektů údajů v kapitole 3.6 a rozvádí dále práva uplatnitelná subjektem přímo u správce, tedy školy. Pro správné nastavení pravidel zajišťujících legislativní soulad je pochopení výkonu práv subjektů v praktickém prostředí školy velmi důležité, obzvláště právo na informace, kterému je zde věnována největší pozornost, představuje pro školy určitou výzvu.

[160] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, recitál 47.

Obecně lze doporučit, aby výkon veškerých práv koordinovalo nejvyšší vedení školy spolu s pověřencem. S výjimkou práva na informace by se na jejich realizaci neměly podílet jiné osoby, nejsou-li vedením školy přímo pověřeny.

4.2.1 Realizace práva na informace

Povýšení tohoto práva na nejdůležitější ze všech zde popsaných nedovozuje méněcennost dále uvedených. Praxe nicméně ukazuje, že kvalitní informování subjektů účinně předchází snaze o uplatnění dalších práv a snižuje rizika konfliktů. V subjektech precizně a srozumitelně vyhotovené poučení o zpracování vyvolává opodstatněný dojem solidnosti správce. V případě pozdějších pochybností volí subjekty smírnější řešení, nikoliv uplatňování zpracování omezujících práv (typicky právo na námitku, na omezení zpracování, výmaz nebo právo podání stížnosti k dozorovému úřadu).

Transparentní a korektní přístup školy k dětem a rodičům v souvislosti se zpracováním jejich osobních údajů je tedy vnímán jako samozřejmost, ne jako povinnost.

To je mj. důvod škodlivosti souhlasů se zpracováním údajů v situacích, kdy jsou údaje fakticky pro zpracování nutné. Právo na informace je tím značně narušeno a subjekt je uváděn v omyl. **Domněnka, že souhlas se zpracováním nahradí efektivněji informování subjektů je lichá, přestože byl ze strany MŠMT tento postup dlouho doporučován[161]**.

Právo být informován o zpracování osobních údajů je typickým příkladem práva, které škola v postavení správce osobních údajů vůči dětem, jejich rodičům, vlastním zaměstnancům, ale i dalším subjektům, naplňuje nejen reaktivně, tedy až na základě jejich jednání, požadují-li například informace v souvislosti se zahájením důvodně očekávaného zpracování, nebo o zpracování, o kterém byli informováni. Rovněž se nejedná o právo, jehož výkon je podmíněn proaktivním přístupem subjektů, tj. zejména při preventivním využití práva za stavu, kdy ke zpracování osobních údajů nedochází, ale subjekty se mohou domnívat, že správce jejich údaji disponuje, či v situaci, kdy se obávají, že zpracování již není zákonné nebo dochází k nedovolené změně účelů zpracování. **Toto právo musí být naplňováno zcela automaticky bez ohledu na pasivitu subjektu.**

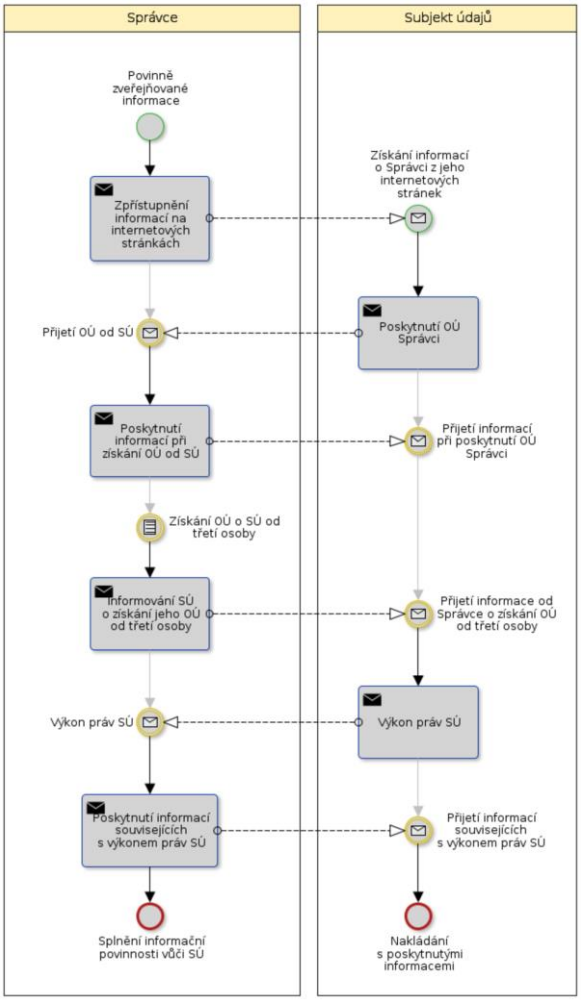
K primární automatické realizaci práva na informace o zpracování dochází nejčastěji při prvním kontaktu žáků, jejich zákonných zástupců a dalších subjektů se školou, kdy jsou jim toliko poskytnuty informace o rozsahu zpracování, o jeho účelu, totožnosti správce,

[161] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) (aktuální web)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021].

o případných oprávněných zájmech a příjemcích osobních údajů. Aktivita je zde obvykle na straně školy, která naplnění práva docílí transparentním zveřejněním zásad zpracování osobních údajů, případně vydáním memoranda s informacemi o zpracování, a to na své webové stránce, na elektronické úřední desce, prostřednictvím aplikace nebo například zasláním elektronickou poštou, tedy obecně tzv. způsobem umožňujícím dálkový přístup.

Při osobním kontaktu v prostorách školy může být subjekt seznámen s analogovou podobou zásad viditelně umístěnou standardně u vchodu na sekretariát, na nástěnce nebo na jiném viditelném místě v prostoru, kde ke kontaktu dochází.

Rodičům může být také poskytnuto tzv. poučení o zpracování osobních údajů již při procesu jejich sběru, které bude obsahovat obvykle velmi podobné informace jako zmíněné memorandum poskytované elektronicky. Nabízí se v něm však příležitost ke specifičtějšímu zaměření informací, tedy ke konkrétnějšímu poučení.



Obrázek 3: Informační povinnost správce[162]

[162] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

Přesný proces poskytování informací není stanoven. „Obrázek 3“ se snaží interpretovat výkon práva subjektu na informace o zpracování prostřednictvím webové stránky školy (pro případy získávaní údajů přímo od subjektu i pro získávání od třetí osoby).

V souvislosti s tímto právem je vhodné upozornit, že jej naplňují všichni zaměstnanci školy, získávají-li v rámci své pracovní činnosti od subjektů (žáků, osob vykonávajících rodičovskou povinnost nebo dalších subjektů) osobní údaje. Analogicky postupují, zahajují-li zpracování již v minulosti získaných údajů (podmínkou je pochopitelně dodržování zásady účelového omezení). Ostatní níže uvedená práva subjektů v praxi vyřizují či realizují pouze vybraní pracovníci školy, obvykle osoby přímo z vedení školy či osoby vedením pověřené. Není vyloučeno, že tak činí pověřenec pro ochranu osobních údajů.

Všichni ostatní zaměstnanci školy by vyřizování dotazů subjektů osobních údajů či žádostí na uplatnění jejich práv provádět neměli.

Na konkrétní provedení informací o zpracování se názory různí. Ani v jejich nazývání není shoda. Lze doporučit, aby **nekonkrétní obecné informace nabízené subjektu** (např. na webu školy nebo na nástěnkách) byly **označeny jako „Zásady zpracování osobních údajů“**. **Verze určené pro specifičtější zpracování nebo předávané subjektům osobně** je vhodné prezentovat jako **„Poučení o zpracování osobních údajů“**.

Z hlediska struktury a dostupnosti mají být tyto dokumenty stručné, srozumitelné a subjektům jednoduše přístupné. Obecné nařízení výslovně požaduje použití jasných a jednoduchých jazykových prostředků[163].

V obsahové stránce se informační memoranda liší podle zdroje zpracovaných údajů (blíže viz kapitola 3.6.1) a podle kategorie subjektů. **Škola by měla vytvořit minimálně dvě různé verze informací pro subjekty, a to pro žáky a jejich zákonné zástupce a dále pro vlastní zaměstnance.** Doporučeno je vydání ještě specifické verze pro uchazeče o zaměstnání a pro subjekty dodavatelsko-odběratelských vztahů.

V rámci hlavní činnosti, tedy při organizaci vzdělávání, by měly informace o zpracování pro žáky a zákonné zástupce v prostředí škol obsahovat[164]:

- informace o škole (vč. kontaktních údajů)

[163] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 12, odst. 1.
[164] *Ibid.,* čl. 13-22, 33-34.

- informace o pověřenci (vč. kontaktních údajů)
- přehled účelů, pro které probíhá zpracování
- aplikované právní tituly zpracování
- vyjádření oprávněných zájmů (používá-li se tento právní základ zpracování)
- informace o příjemcích osobních údajů
- platnou dobu uložení nebo kritéria pro stanovení této doby
- informace o případném automatizovaném rozhodování, včetně profilování
- poučení o existenci práv subjektů a o možnosti jejich uplatnění
    - právo požadovat přístup k osobním údajům
    - právo na opravu a doplnění
    - právo na výmaz
    - právo na omezení zpracování
    - právo na přenositelnost údajů
    - právo vznést námitku proti zpracování
    - právo podat stížnost u dozorového

Součástí informací pro subjekt musí být také transparentní informování žáků, především pak jejich zákonných zástupců, jakým způsobem a při jakých příležitostech budou pořizovány fotografie a audiovizuální záznamy a jaká pravidla jsou školou nastavena pro využití tzv. opt-out[165], tedy bude-li zákonný zástupce žádat o jejich nezveřejňování a další nezpracovávání (blíže viz kapitola 4.6 věnovaná fotografování).

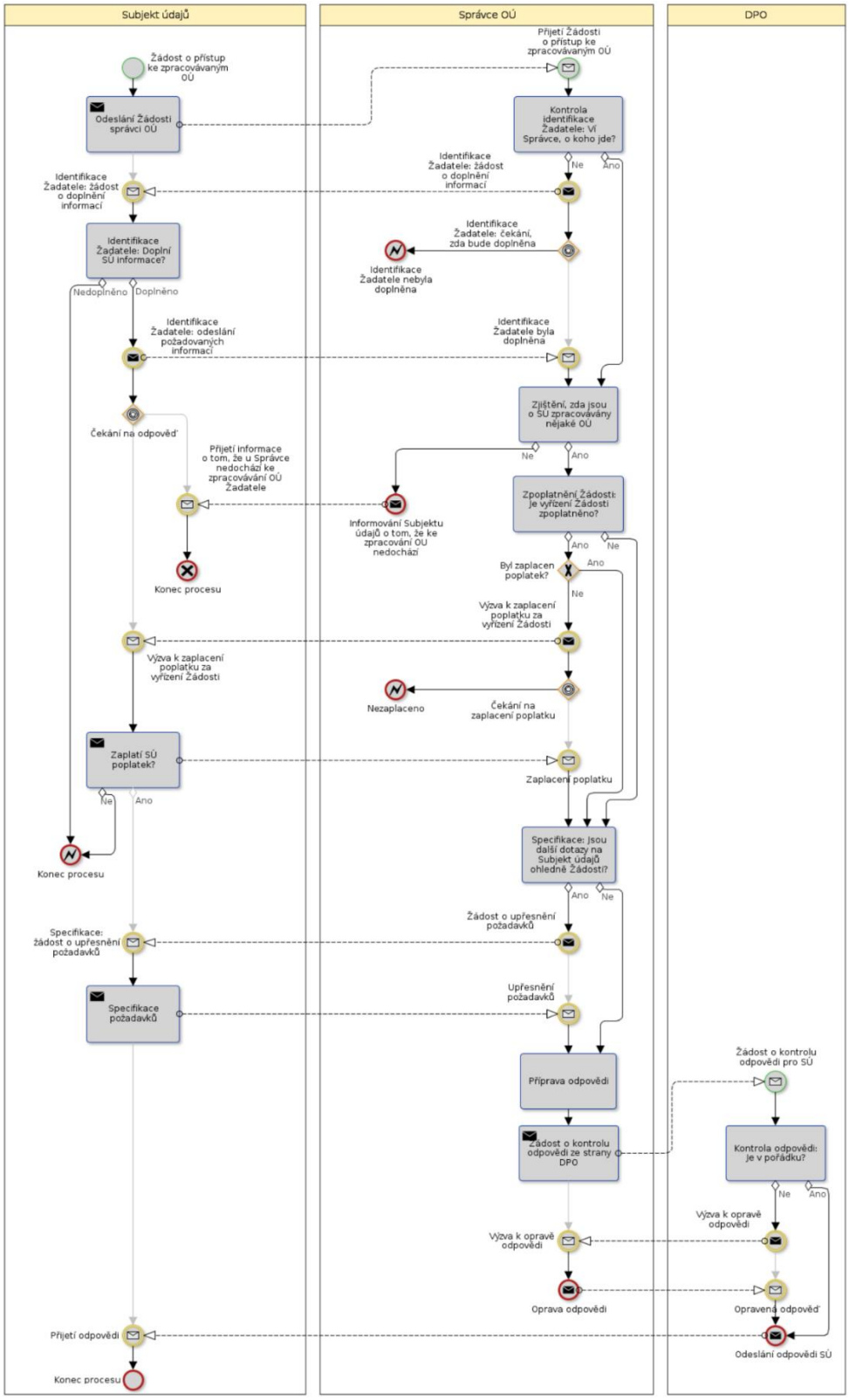
Požadavek na jednoduchost, stručnost a srozumitelnost informačního memoranda je v opozici s výčtem informací, které by mělo obsahovat, proto je doporučeno ve vztahu k žákům a zákonným zástupcům žáků tvořit zestručněnou verzi spolu s instrukcemi pro uplatnění práv a způsobu vyžádání si detailnějších informací. Takto sestavený vzor je přílohou této práce („Příloha 1 - Vzor informací pro subjekty“ na straně 180).

4.2.2 Realizace práva na přístup k osobním údajům

Požádá-li subjekt školu o výkon tohoto práva, musí škola vyloučit pochybnosti o jeho totožnosti, tedy že budou informace (osobní údaje žáků nebo jejich zákonných zástupců)

[165] Opt-out představuje princip vyjádření či rozhodnutí osoby nebýt předmětem nebo účasten určité činnosti

poskytnuty neoprávněnému příjemci, a to bez ohledu na možný úmysl (podvržení identity) nebo pouhý omyl. Detailní pravidla důvěryhodné komunikace jsou uvedena v kapitole 4.3.



Obrázek 4: Právo na přístup k osobním údajům[166]

[166] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

Případné žádosti o přístup k osobním údajům musí posoudit pověřenec, a o způsobu vyřízení rozhodnout ředitel školy. Je nepřípustné, aby uplatnění tohoto práva vyřizoval ve škole jiný nežli pověřený pracovník, přičemž právo na informace mnohdy nevědomky vykonávají řadoví zaměstnanci v rámci běžných telefonních hovorů nebo e-mailové komunikace, a to obvykle bez možnosti prokazatelně ztotožnit subjekt.

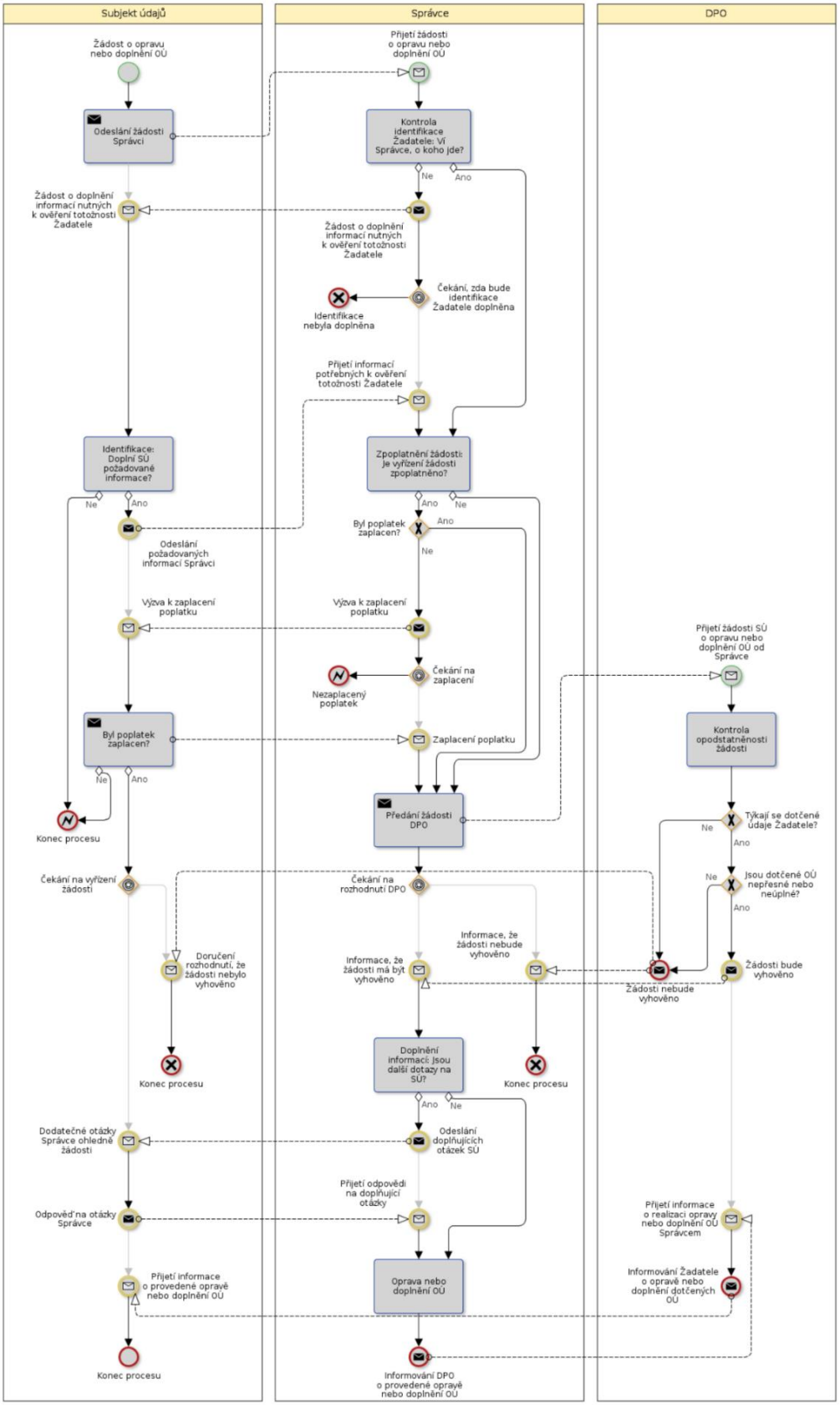
Poskytování konkrétních osobních údajů je v prostředí škol značně omezeno v závislosti na právním důvodu zpracování. Do procesu (viz Obrázek 4) je již v jeho počátku vhodné doplnit krok „vyjádření pověřence o oprávněnosti žádosti subjektu o přístup k údajům“.

4.2.3 Realizace práva na opravu, resp. doplnění

Požádá-li subjekt o doplnění informací nebo o opravu vybraných údajů, je také třeba subjekt ztotožnit, nicméně ve většině případů toto právo neznamená při chybné identifikaci subjektu závažné dopady do práv a svobod fyzických osob.

Relevantnost doplnění údajů nebo provedení jejich oprav by měl posoudit pracovník odpovědný za příslušnou agendu. Oprávněnost žádosti subjektu posuzuje pověřenec, proto je vhodné v procesu výkonu tohoto práva (viz Obrázek 5) doplnit krok, v němž pověřenec provede kontrolu náležitostí žádosti, přičemž způsob vyřízení je opět na řediteli školy.

V praxi bývají tyto žádosti vzácné, protože ke korekcím chyb v údajích či k jejich doplňování dochází obvykle přirozeně bez nutnosti uplatnění institutu z obecného nařízení.



Obrázek 5: Právo na opravu a doplnění[167]

[167] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

4.2.4 Realizace práva na výmaz (být zapomenut)

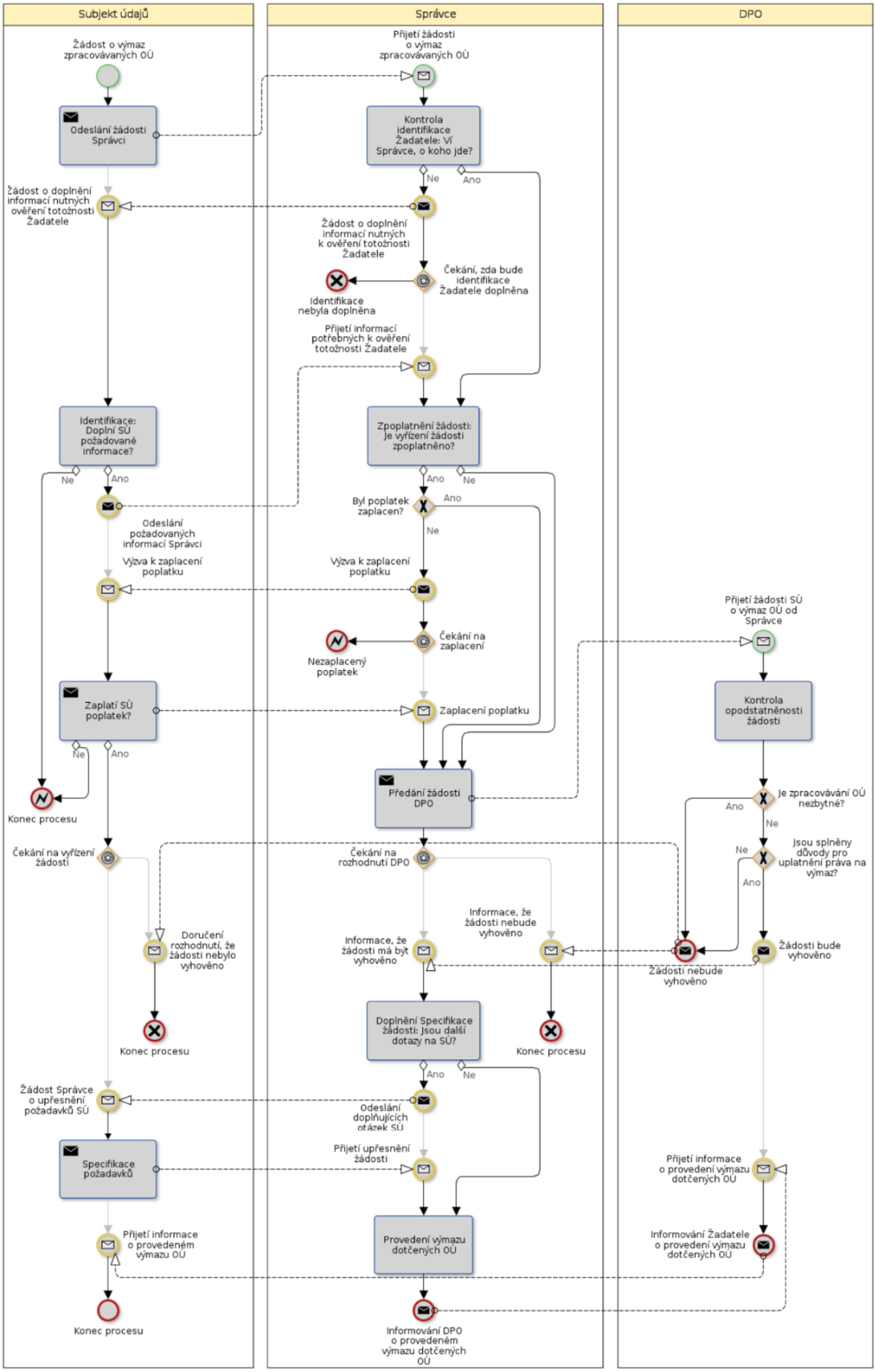
Vycházíme-li z předpokladu, že škola nezpracovává údaje nezákonným způsobem nebo bez podložení právním titulem zpracování (zásada zákonnosti), že je neuchovává déle, než je pro daný účel nutné (zásada omezení uložení) nebo v neadekvátním rozsahu (zásada minimalizace), lze uplatnit toto právo na naprosté minimum údajů.

Předpokladem je rovněž automatické smazání údajů ze strany školy, které byly zpracovávány na základě souhlasu a tento byl odvolán.

V praxi se tak v prostředí školy můžeme setkat s oprávněnou žádostí o výmaz soukromých telefonních čísel a e-mailových adres žáků nebo jejich zákonných zástupců (blíže vysvětleno v kapitole 4.1.6 v podkapitole „KONTAKTNÍ ÚDAJE NA SUBJEKTY – TELEFONNÍ ČÍSLA A E-MAILOVÉ ADRESY“), které škola zpracovává v oprávněném zájmu za účelem zvýšení efektivity a rychlosti komunikace. V takovém případě však postačuje, aby subjekt podal námitku proti zpracování a případná nepřiměřenost bude zodpovědně posouzena.

Proto se lze s oprávněným výkonem tohoto práva setkat ve školách jen velmi vzácně, obvykle jsou žádosti o výmaz pro neznalost problematiky ze strany subjektů nedůvodné. Jsou-li validní a přeci jen dojde k jejich realizaci, posuzuje oprávněnost nároku subjektu pověřenec, způsob a rozsah výkonu práva určuje ředitel školy.

I u tohoto práva je pochopitelně nutné odpovídajícím způsobem, ztotožnit subjekt, aby nedošlo k mylnému výmazu dat jiného subjektu nebo o pokus žadatele s podvrženou identitou poškodit skutečný subjekt.



Obrázek 6: Právo na výmaz – být zapomenut[168]

[168] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

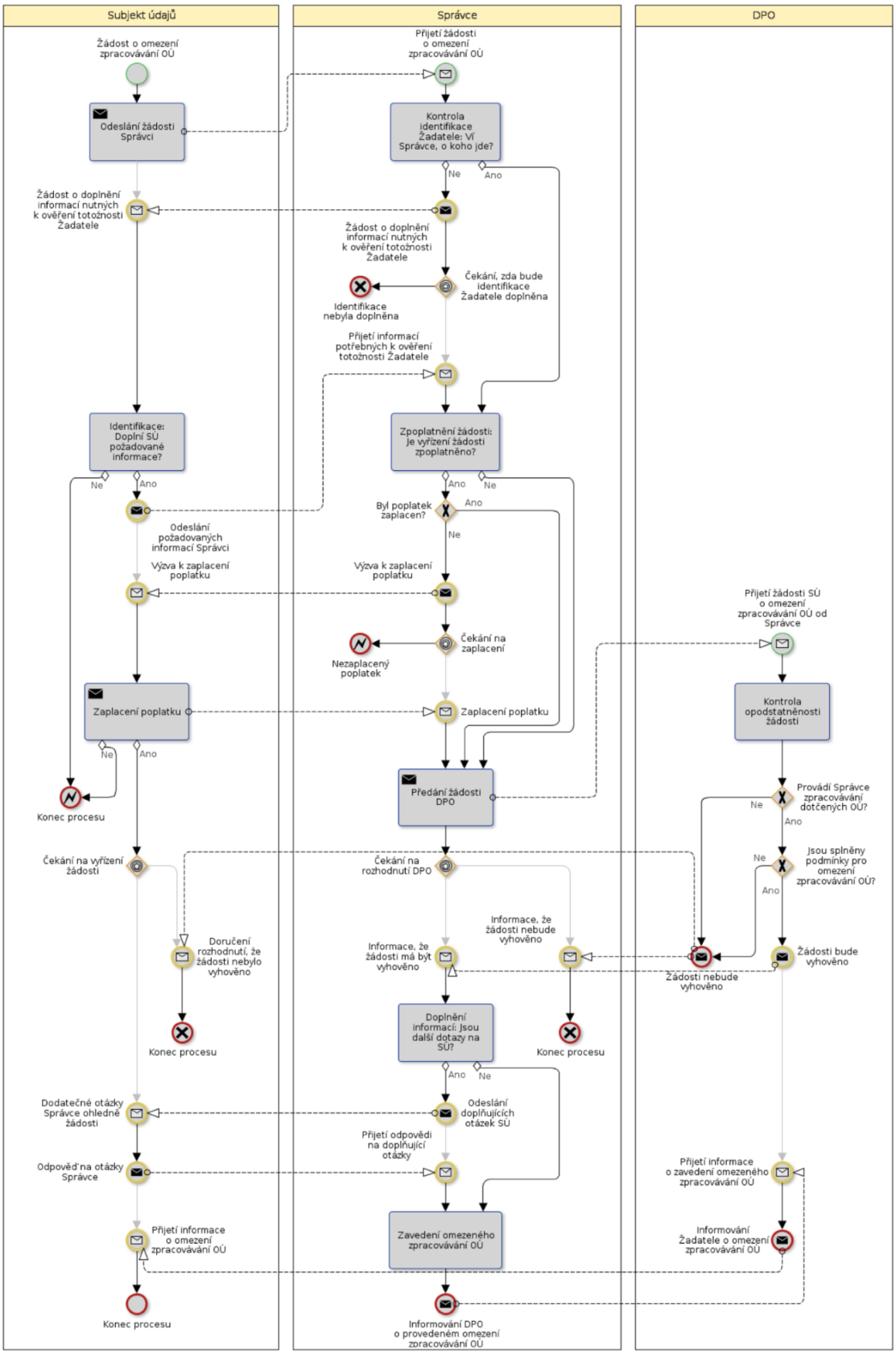
4.2.5 Realizace práva na omezení zpracování

Obdrží-li škola platnou žádost o omezení zpracování, je vhodné důkladně zvážit veškeré dopady takového omezení bude-li omezení vyhověno, a zejména prověřit veškerá školou prováděná zpracování osobních údajů konkrétního žadatele o využití tohoto práva.

Nejedná se o často uplatňované právo, v prostředí škol je spíše raritní, ale dojde-li k jeho využití, má to obvykle konsekventní následky. Pravděpodobně tak subjekt činí, protože se domnívá, že jsou jeho údaje zpracovávány neoprávněně. Za snahou zamezit výmazu takových dat se může skrývat záměr zachování důkazů pro následné šetření dozorového úřadu, ke kterému dá subjekt podnět, nebo dokonce pro případný soudní spor. V prostředí škol je omezením zpracování postižitelná jen velmi omezená skupinu údajů.

Postup vyřízení žádosti je třeba konzultovat s pověřencem, proto je vhodné již v začátku procesu (viz Obrázek 7) doplnit jeden krok, ve kterém bude mít pověřenec prostor na vyhodnocení relevantnosti omezení zpracování. Následně musí být vyžádáno stanovisko osob odpovědných za příslušné agendy, tedy za ta zpracování, která mají být omezením zasažena. Rozhodnutí o vyhovění či nevyhovění je, jako obvykle, na statutárním zástupci.

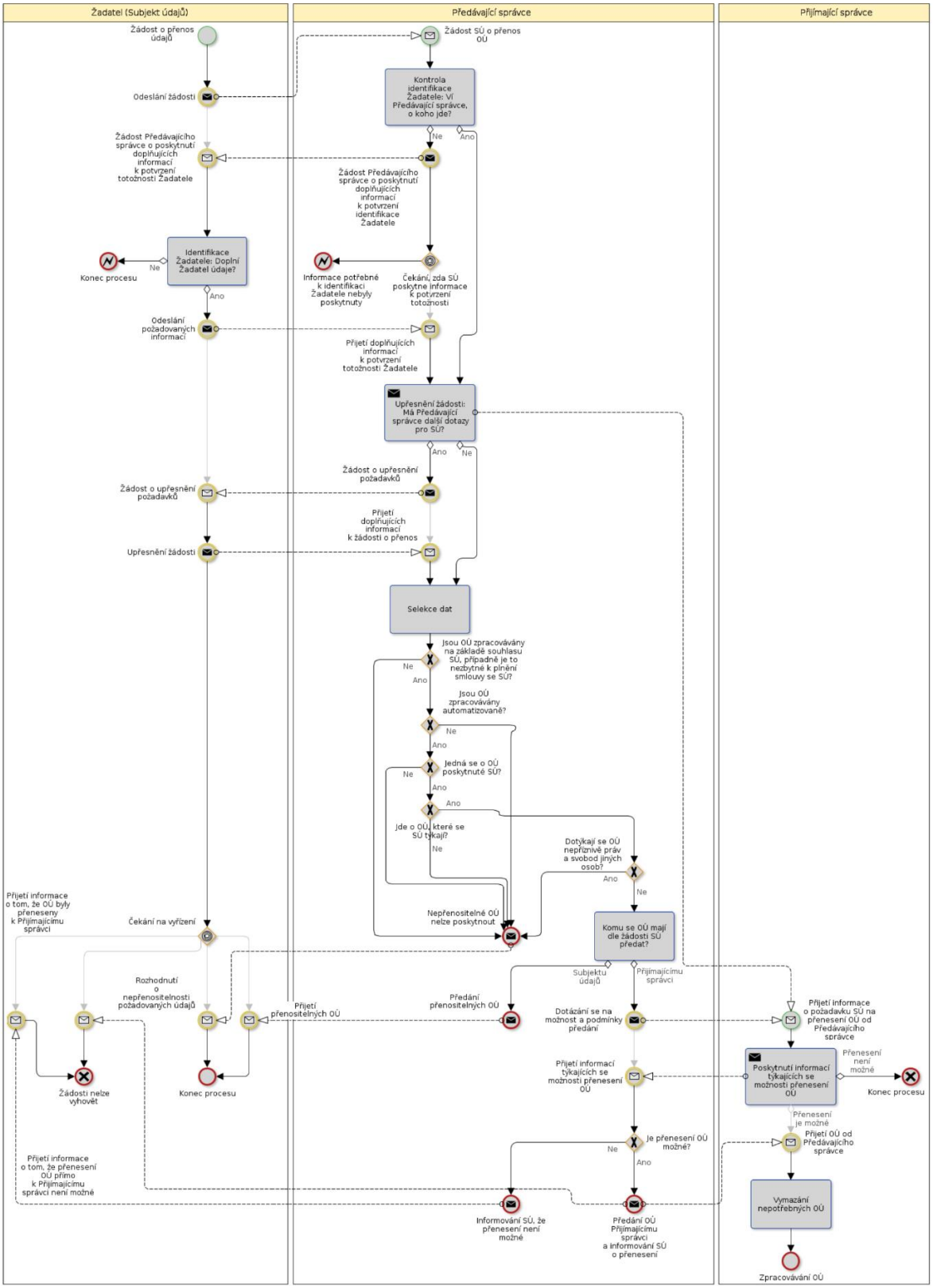
Data, jejichž zpracování je omezeno, musejí být školou ve všech systémech a fyzických úložištích blokována proti dalšímu zpracovávání a proti výmazu. V praxi toto mnoho informačních systémů nedokáže, proto je nezbytné přijmout vhodná technickoorganizační opatření, která nahradí chybějící funkcionalitu aplikace odpovídajícím přístupem zaměstnanců školy.



Obrázek 7: Právo na omezení zpracovávání[169]

[169] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

4.2.6 Realizace práva na přenositelnost údajů



Obrázek 8: Právo na přenositelnost osobních údajů[170]

[170] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

Obrázek 8 znázorňuje procesní mapu výkonu práva na přenositelnost. V prostředí škol může dojít k přenosu údajů naprosto přirozeně při přestupu žáka na jinou základní školu. V takovém případě se však nejedná o využití práva na přenositelnost údajů ve smyslu obecného nařízení.

Proces výkonu tohoto práva se sice od práva na přístup k osobním údajům liší, nicméně obecná pravidla pro aplikaci přenositelnosti údajů jsou prakticky shodná. Údaje se pouze neposkytují přímo subjektu, ale jinému správci, kterého subjekt určí.

Pokud subjekt tohoto práva využije, je vhodné si vyžádat upřesňující informace o požadovaném formátu a struktuře dat a snažit se o dohodu se subjektem na změnu požadavku z „práva na přenositelnost“ na „právo na přístup“. Subjektu tak budou poskytnuty všechny požadované údaje, avšak za přenos k novému správci již přebírá odpovědnost sám.

K realizaci tohoto práva v prostředí škol odchází velmi zřídka, proto není nezbytné pro něj vytvářet složitá pravidla. V případě jeho využití je optimální požádat pověřence o individuální vyřízení žádosti a koordinaci procesu.

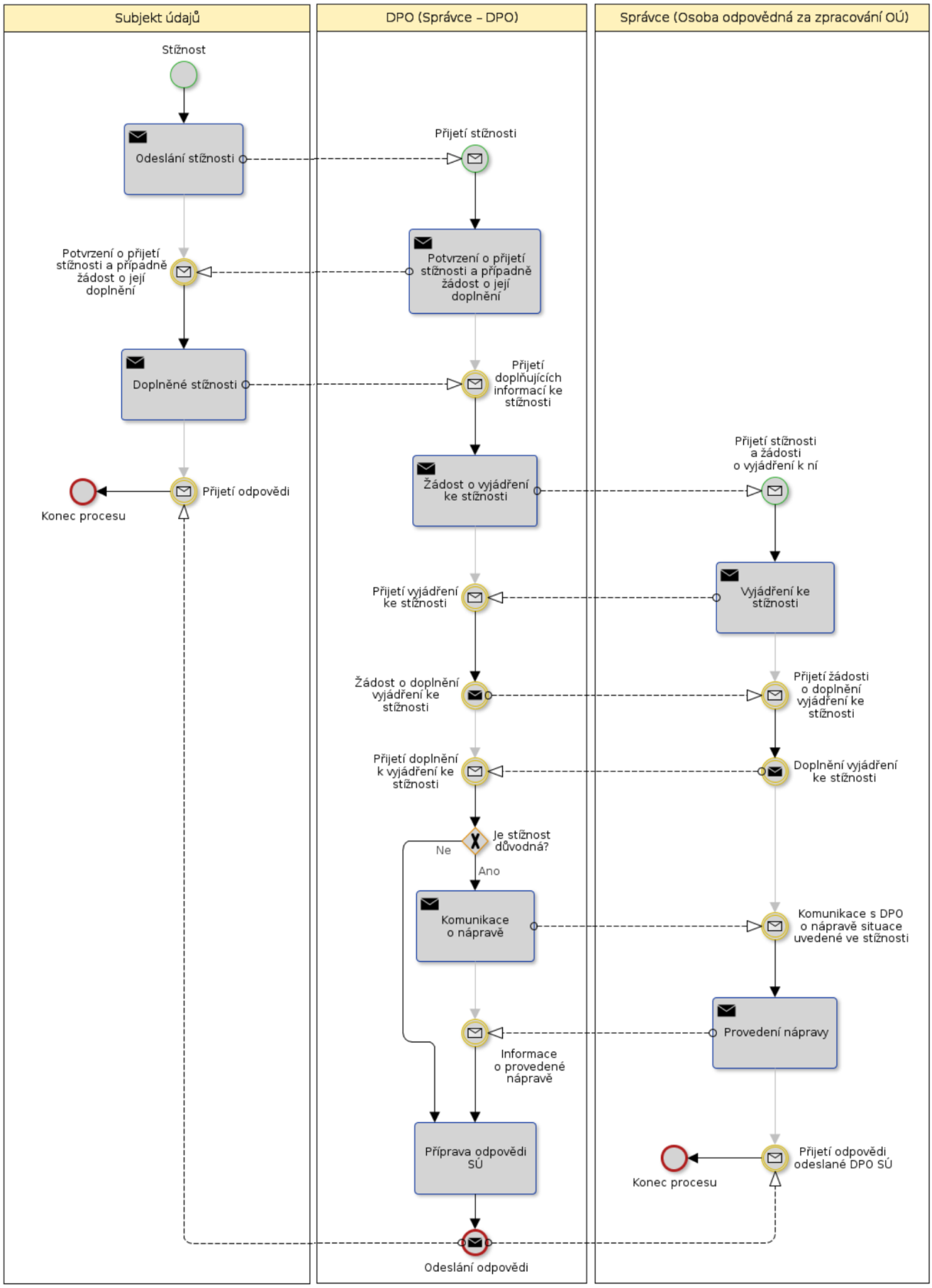
4.2.7 Právo subjektu vznést námitku, stížnosti subjektů v praxi

Podá-li subjekt námitku proti zpracování, případně stížnost, je nutné ji velmi rychle posoudit, protože je ve většině případů nepřípustné ve zpracování pokračovat před vypořádáním námitky (stížnosti). Proces posouzení zahrnuje provedení testu proporcionality (viz kapitola 3.6.7, podkapitola „BALANČNÍ TEST“).

Námitku i stížnost posuzuje pověřenec, rozhodnutí o případném pozastavení zpracování, resp. o vyhovění/nevyhovění námitce, činí ředitel školy na doporučení pověřence. Vyřízení stížnosti je rovněž v gesci ředitele, nicméně se doporučuje, aby případné stížnosti subjektů řešil pověřenec a v celém procesu důsledně dbal na přesné dodržování obecného nařízení. V případě zamítnutí stížnosti či námitky jako neodůvodněné je vhodné postupovat v souladu s pravidly pro správní řízení.

Úspěšné uplatnění tohoto práva je v prostředí veřejných škol vzácné, je velmi nepravděpodobné, že by škola cíleně prováděla zpracování postavené na křehkém právním základu „oprávněný zájem“ bez předchozího vyhodnocení testu proporcionality takového zpracování. V případě zpracovávání ve veřejném zájmu je akceptovatelnost námitky subjektu ještě abstraktnějším institutem.

Proces vyřizování stížností, podnětů a námitek ilustruje „Obrázek 9“.



Obrázek 9: Vyřizování námitek, podnětů a stížností[171]

[171] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

4.3 Důvěryhodná komunikace se subjekty (nejen) při výkonu práv

Komunikace mající právní důsledky vyžaduje nastavení striktních pravidel. Je-li jednou ze stran orgán veřejné moci, jsou pravidla o to přísnější. Při sběru osobních údajů, a především při výkonu většiny práv subjektů, je třeba volit způsob komunikace umožňující jednoznačnou identifikaci jednajících stran.

S výjimkou práva na informace musí být prakticky při veškeré komunikaci obsahující osobní údaje, nebo související s výkonem práv, zvolen takový komunikační kanál, který škole tuto jednoznačnou identifikaci umožní. Řešením je také zavedení dalšího podpůrného faktoru pro ověření identity stran jednajících prostřednictvím běžné komunikace.

4.3.1 Osobní jednání se subjektem údajů

Uplatňuje-li subjekt práva vůči škole osobně, nebo poskytuje-li tímto způsobem osobní údaje a zároveň existuje nejistota o identitě subjektu, je přiměřenou reakcí školy ztotožnění proti předloženému dokladu totožnosti.

Jedná-li škola s domnělými zákonnými zástupci žáka, přičemž existuje určitá pochybnost o skutečném výkonu rodičovské povinnosti těchto osob, je přiměřené využít údaje ze základních registrů pro ověření subjektem deklarovaných informací.

Jedná-li statutární zástupce, jím pověřená osoba nebo pověřenec jménem školy se subjekty údajů při uplatňování jejich práv (ve smyslu obecného nařízení), musí být jednání dokumentováno. Kromě dodržení povinností evidence ve spisové službě jsou důvodem právní následky takového jednání a až na výjimky je důkazní břemeno legislativně souladného postupu při zpracování osobních údajů na správci, tedy škole.

4.3.2 Komunikace se subjektem údajů v listinné podobě

Pří písemném jednání v analogové podobě, tedy za pomoci hmotného substrátu, obvykle papíru, odpadá komplikace se zadokumentováním jednání, avšak přibývá jeden nový problém, a tím je autentizace jednajících. Ověření identity subjektu s vysokou úrovní důvěry téměř vylučuje prosté použití obyčejného podpisu, není-li využit další ověřovací faktor. Nelze předpokládat, že škola bude ověřovat grafologickým rozborem pravost vlastnoručních podpisů, proto musí být tento úředně ověřen. Jako případný další faktor ověření, není-li vlastnoruční podpis úředně ověřen, může škola pro verifikaci původce listinného dokumentu přistoupit ke kontaktování subjektu telefonicky, přičemž je k tomu využito telefonní číslo uložené v interní školní databázi, například v systému Bakaláři.

4.3.3 E-mailová komunikace se subjektem údajů

Běžná e-mailová komunikace, tedy zasílání elektronických zpráv prostřednictvím internetu, není bez dalšího zabezpečení obecně příliš důvěryhodným způsobem komunikace. Je to z důvodu relativně snadného podvržení totožnosti a chybí i potřebné záruky doručení, resp. bez kooperace příjemce není možné dovodit doručení zprávy.

Problém má dvě roviny. Tou první je schopnost školy prokázat, že e-mail odeslaný subjektu, vyžádal-li si takový způsob komunikace, mu byl skutečně doručen. Druhou komplikací je ověření identity odesílatele u e-mailů, které škola obdrží.

Předpokladem dále uvedeného je pochopitelně evidence ve spisové službě, tato otázka zde nebude vzhledem k cílům práce příliš detailizována, nicméně je vhodné se spisovou službou speciálně ve vztahu ke komunikaci zabývat podrobně.

Občanský zákoník připouští platnost právního jednání učiněného v elektronické formě nahrazením jinak vyžadovaného podpisu osoby na listinném dokumentu podpisem elektronickým.[172] Klíčové je tedy vymezení správného použití elektronického podpisu, aby zamýšlené právní jednání vyvolávalo očekávané účinky. Pokud tedy není v souladu s nařízením eIDAS[173] a zákonem o službách vytvářejících důvěru pro elektronické transakce[174] zásilka opatřena ze strany školy uznávaným podpisem, který je pro OVM zmíněným zákonem definován jako zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis a umístěný na kvalifikovaném prostředku, nelze uplatnit pro tuto písemnost nevyvratitelnou domněnku pravosti.

Soukromoprávní subjekty mohou díky zákonné výjimce[175] ukládat své certifikáty mimo kvalifikované prostředky a vůči OVM činit podání použitím elektronického podpisu, který je uložen např. v úložišti operačního systému (nemusí si zajišťovat čipovou kartu nebo USB token). To činí jejich použití pro soukromé osoby jednodušším a není tedy nepřiměřené je po subjektech vyžadovat v situacích, kdy by díky nedůvěryhodné e-mailové komunikaci hrozil zásah do práv a svobod subjektů, jejichž identita může být potenciálně zneužita.

[172] Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2012, částka 33, číslo 89, § 561, 562.
[173] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014. In: *EUR-Lex*. Brusel, 2014, Úř. věst. L 257/73, číslo 910.
[174] Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2016, částka 115, číslo 297.
[175] Ibid., § 6.

Praktickým příkladem budiž situace, kdy škola obdrží e-mailem žádost o přístup k osobním údajům z e-mailové adresy *josef.novak.75@email.cz,* které se rozhodne vyhovět. V žádosti subjekt uvede, že je Josef Novák, ročník 1975, a že je zákonným zástupcem žáka, Jana Nováka, ročník 2010, navštěvujícího předmětnou školu. E-mail, ve kterém požaduje přístup k osobním údajům svého syna, však není opatřen elektronickým podpisem.

Škola má několik možností, jak situaci vyřešit, tedy jak přiměřeným způsobem ověřit identitu žadatele a tím oprávněnost nároku.

a) Vyhledá si ve vlastní databází kontaktních údajů na rodiče telefonní číslo na zákonné zástupe žáka Jana Nováka, pokud tyto údaje existují, panu Josefu Novákovi zavolá a požádá ho o potvrzení, že je autorem žádosti.
b) Disponuje-li e-mailovým kontaktem (databáze viz bod „a"), odpoví panu Josefu Novákovi na adresu, která je prokazatelně spojena se zákonnými zástupci subjektu, tedy žáka Jana Nováka. V případě, že se budou e-mailové adresy lišit, tedy adresa, ze které přišlá žádost nebude korespondovat s adresou uloženou ve školním informačním systému, použije škola tu z vlastní databáze. V nejhorším případě bude osloven skutečný pan Novák, rodič žáka, který nebude o své žádosti tušit, neboť byla jeho identita zneužita. Je však oprávněným příjemcem a nebude se jednat o porušení zabezpečení.
c) Škola kontaktuje pana Nováka odpovědí na jeho e-mail, který použil pro žádost (nebude ověřovat pravost e-mailové adresy) a instruuje ho, aby použil jiný způsob komunikace. Tedy aby se dostavil do školy s dokladem totožnosti, aby svůj e-mail podepsal elektronickým podpisem, aby využil datovou schránku nebo zaslal listinnou žádost opatřenou vlastnoručním úředně ověřeným podpisem.
d) Zašle panu Novákovi požadované informace datovou schránkou, ověří-li škola úspěšně v seznamu datových schránek[176], že ji má zpřístupněnu.
e) Odešle panu Novákovi listinný dokument s požadovanými údaji na adresu bydliště, kterou má škola v databázi, případně si ji ověří prostřednictvím informačního systému základních registrů (ISZR)[177].

Ve vztahu k e-mailové komunikaci je vhodné podtrhnout ještě jedno riziko nesouvisející s výkonem práv subjektů. Je jím hromadná e-mailová korespondence.

[176] *Seznam držitelů datových schránek (https://www.mojedatovaschranka.cz/sds/)* [online]. [cit. 2021-03-09].
[177] *Správa základních registrů : Informační systém základních registrů (ISZR)* [online]. [cit. 2021-01-03].

V naprosté většině případů je hromadný e-mail zaslaný školou s otevřenou hlavičkou zprávy (všichni adresáti zprávy uvidí celý seznam příjemců) na adresy zákonných zástupců žáků porušením nařízení GDPR. Tento výklad se s příchodem obecného nařízení nezměnil. Takové praktiky byly porušením ZZOÚ dlouho před příchodem GDPR.

4.3.4 Komunikace se subjektem údajů prostřednictvím datové schránky

Povinností každého orgánu veřejné moci, školy nevyjímaje, je před odesláním jakékoliv písemnosti libovolnému subjektu ověřit, zda má tento zřízenu a zpřístupněnu datovou schránku a využít ji jako jediný komunikační prostředek. Výjimka se použije, neumožnuje-li přenos datové zprávy povaha písemnosti, tedy nevylučuje-li to velikost zprávy, nestandardní formát nebo zvláštní okolnost.[178] Kontrolu existence DS provádějí obvykle sofistikované informační systémy zajišťující provoz spisové služby zcela automatizovaně. Není-li tomu tak, musí škola, kromě případu, kdy vystupuje jako subjekt soukromého práva (jednajíce např. v rámci dodavatelsko-odběratelských vztahů), důsledně kontrolovat, zda má subjekt zpřístupněnu datovou schránku. Právní důsledky nedodržení této povinnosti v rámci výkonu působnosti mohou být například důvodem pro nevykonatelnost rozhodnutí nebo nenabytí právní moci.

Pokud škola jednající při výkonu veřejné moci odešle fyzické osobě, která má zpřístupněnu datovou schránku, dokument jiným způsobem, dojde kromě porušení zákona k absenci fikce doručení. Příkladem budiž situace, kdy je subjektu odeslána písemnost v analogové formě, tedy jako listinný dokument prostřednictvím doporučené poštovní zásilky. Pokud si subjekt takovou zásilku nepřevezme, nastává standardně podle povahy zásilky domněnka dojití či fikce doručení. Dle okolností je subjekt vyzván oznámením o uložení zásilky a případné rozhodnutí může být, opět podle okolností, pro nabytí první moci například doručeno veřejnou vyhláškou. Blíže toto upravuje např. správní řád v § 23. Použije-li však OVM zmíněný způsob doručení i přesto, že má subjekt zpřístupněnu datovou schránku, nenastává právní fikce doručení, ale vyvratitelná domněnka doručení, tedy subjekt může napadnout tento postup u soudu a je velmi pravděpodobné, že díky porušení zákona ze strany OVM zvrátí případný nepříznivý dopad nepřevzetí listinné zásilky.

Je diskutabilní, zda se má při komunikaci se subjekty týkající se výkonu práv ve smyslu obecného nařízení uplatnit toto ustanovení, protože fakticky nejde o výkon veřejné

[178] Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2008, částka 98, číslo 300, § 17.

moci. Škola se však nenachází ani v roli soukromoprávního subjektu. **Pokud se komunikace se subjekty týká zpracování prováděného v rámci organizace vzdělávání a všech s tím souvisejících činností, je důrazně doporučeno postupovat v souladu s výše uvedenými pravidly.**

Komunikace datovou schránkou je velmi důvěryhodná, doručování datových zpráv je garantováno a o identitě jednajících stran není pochyb.

4.3.5 Telefonická komunikace se subjektem údajů

Telefonickou komunikaci lze z pohledu důvěryhodnosti antagonisticky rozdělit na dva typy. Pokud škola využije kontakt na subjekty, obvykle zákonné zástupce dětí, které má v databázi ještě z doby podání žádosti o přijetí dítěte, případně má toto číslo uloženo v mobilním telefonu, je komunikace důvěryhodná. Stejné důvěryhodnosti dosahuje, volá-li subjekt do školy na mobilní telefon, případně pevnou linku, umožňující zobrazení čísla volajícího. Má-li škola toto číslo uloženo, může tím přiměřeně ověřit identitu.

Na opačné straně stojí telefonní hovor z neznámého čísla nebo na pevnou linku, která nepodporuje identifikaci volajícího. Byť se subjekt představí, není možné takovou komunikaci považovat za důvěryhodnou a jde o velké riziko, které na sebe škola bere, pokud si v rámci takové komunikace vyměňuje zneužitelné informace nebo poskytuje osobní údaje.

V praxi bylo ve školských zařízeních zaznamenáno ještě jedno velmi primitivní, avšak účinné, řešení. Byl zaveden mechanismus vícefaktorového ověření pomocí předem domluveného jedinečného hesla, které měla škola uloženo ve školní matrice u každého žáka.

4.4 Bezpečnostní incidenty a ohlašování porušení zabezpečení

Důsledky porušení zabezpečení, tedy vzniku bezpečnostních incidentů, jsou teoreticky charakterizovány v kapitole 3.7. Potenciál pro vznik bezpečnostních incidentů je v prostředí škol tak obrovský, že se nelze ilustrativním výčtem ani přiblížit jeho rozsahu. Pro naplnění cílů práce je však důležité vysvětlit alespoň několik příkladů spolu s postupem řešeni, který lze aplikovat analogicky na obdobné situace.

Mezi nejčastější porušení zabezpečení patří:

- ztráta přenosného paměťového úložiště, obvykle USB flash disku, obsahujícího nezabezpečená data zahrnující i osobní údaje
- zavirování osobního počítače s hrozící kompromitací uložených dat

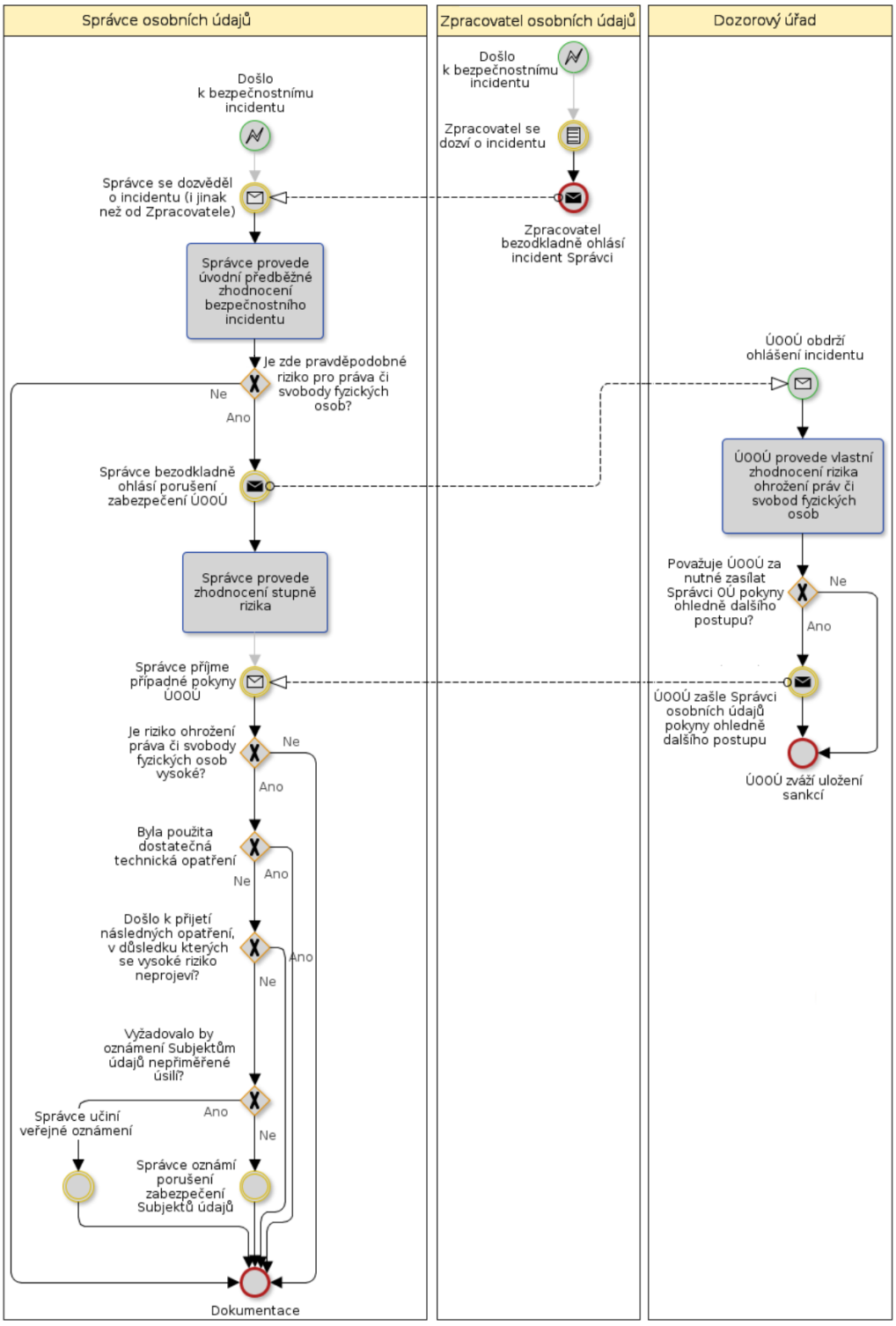
- napadení počítačové sítě přes nezabezpečená zařízení (často jde o IP kamery nebo záznamová zařízení, případně zastaralé aktivní síťové prvky s neaktualizovaným firmwarem)
- ztráta listinných dokumentů obsahujících osobní údaje
- zasílání hromadných e-mailů (zveřejnění adres více příjemců)
- špatná anonymizace dokumentů vkládaných do registru smluv (je-li škola povinným subjektem – závislost na kategorii zřizovatele)
- chybná anonymizace vyřízeních žádostí podle informačního zákona
- zveřejnění identity žadatele podle informačního zákona
- nepřiměřené zveřejňování údajů o žácích prostřednictvím sociálních sítí
- invazivní přístup k zakládání účtů žákům bez informování zákonných zástupců nebo bez souhlasu subjektu (např. zakládání uživatelských účtů ve školních systémech *jmeno.prijmeni@domenaskoly.cz*)
- nevyhovující zabezpečení systémů, zejména těch dálkově přístupných (nedostatečná délka nebo komplexita hesla vedoucí k prolomení hesla, případně snadno uhodnutelné či omylem zveřejněné heslo)

Dojde-li k podobným situacím, vznikne podezření na bezpečnostní incident. Dokud není tento potvrzen, je situace hodnocena jako bezpečnostní událost. Teprve po prokázání, že k porušení zabezpečení skutečně došlo, je situace kvalifikována jako bezpečnostní incident se všemi důsledky.

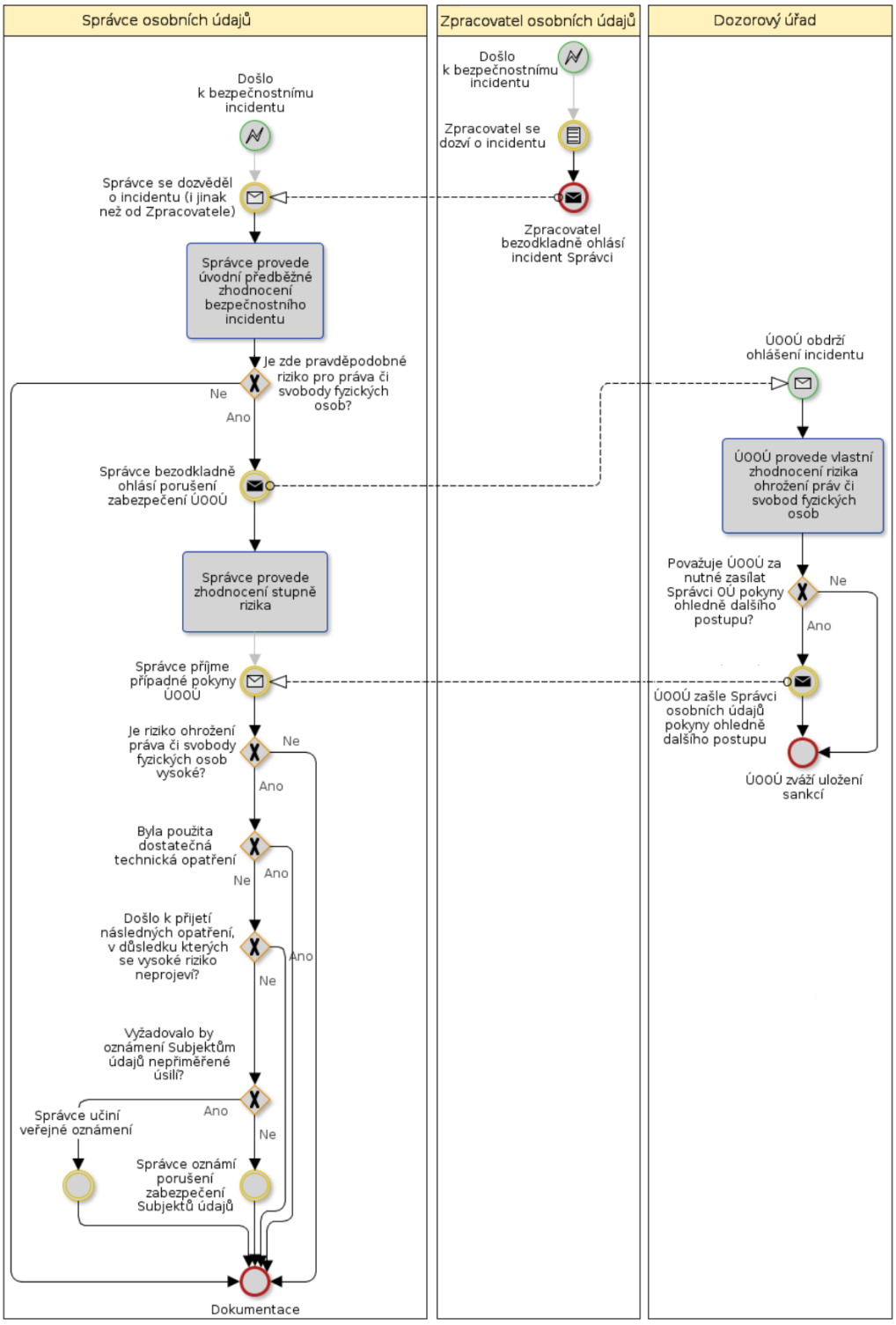
Škola musí přijmout taková pravidla, aby byla schopna koordinovat činnost pověřence, obvykle i externích IT firem nebo interních IT pracovníků (správců sítě) a klíčových vedoucích pracovníků, aby eliminovala eskalaci problémů a zabránila konsekventním škodám. Zároveň je třeba postupovat dostatečně rychle pro splnění lhůty 72 hodin na oznámení porušení ÚOOÚ. Případy porušení zabezpečení s vysokým rizikem zásahu do práv a svobod subjektů je třeba hlásit přímo subjektům.

Prioritou však je nastavit svoje systémy a pravidla zpracování tak, aby k incidentům vůbec nedocházelo. Je tedy třeba zavést přiměřená pravidla fyzické bezpečnosti.

Úlohou školy je také motivace vlastních zaměstnanců k nezatajování, ale naopak k co nejrychlejšímu oznamování bezpečnostních událostí. Rychlou reakcí je možné například snížit důsledky úniku dat.



Obrázek 10) sice nezdůrazňuje úlohu pověřence, školy by však jeho služeb měly v podobných situacích využívat. Pověřenec by měl v nejlepším případě na celý postup řešení incidentu dohlížet.



Obrázek 10: Oznamování porušení zabezpečení[179]

[179] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

4.5 Pověřenec pro ochranu osobních údajů v praxi škol

Kapitola 3.4.4 v teoretické části vymezila problematiku pověřence relativně detailně. Z praktického hlediska je vhodné připomenout zejména povinnost oznámení pověřence, resp. provedení revize, zda k tomuto oznámení došlo a zda byl správný kontakt na aktuálně jmenovaného pověřence sdělen dozorovému úřadu. Vzor oznámení je přílohou této práce (viz „Příloha 4 - Oznámení o jmenování pověřence“ na straně 185).

Oznámení o jmenování provádí výhradně škola, a to ideálně prostřednictvím datové schránky. Pověřenec nikdy nemůže oznamovat sám sebe. Údaje na pověřence je třeba zveřejnit na webových stránkách školy nejlépe v sekci kontaktů a zároveň v zásadách zpracování či v poučení o zpracování. [180]

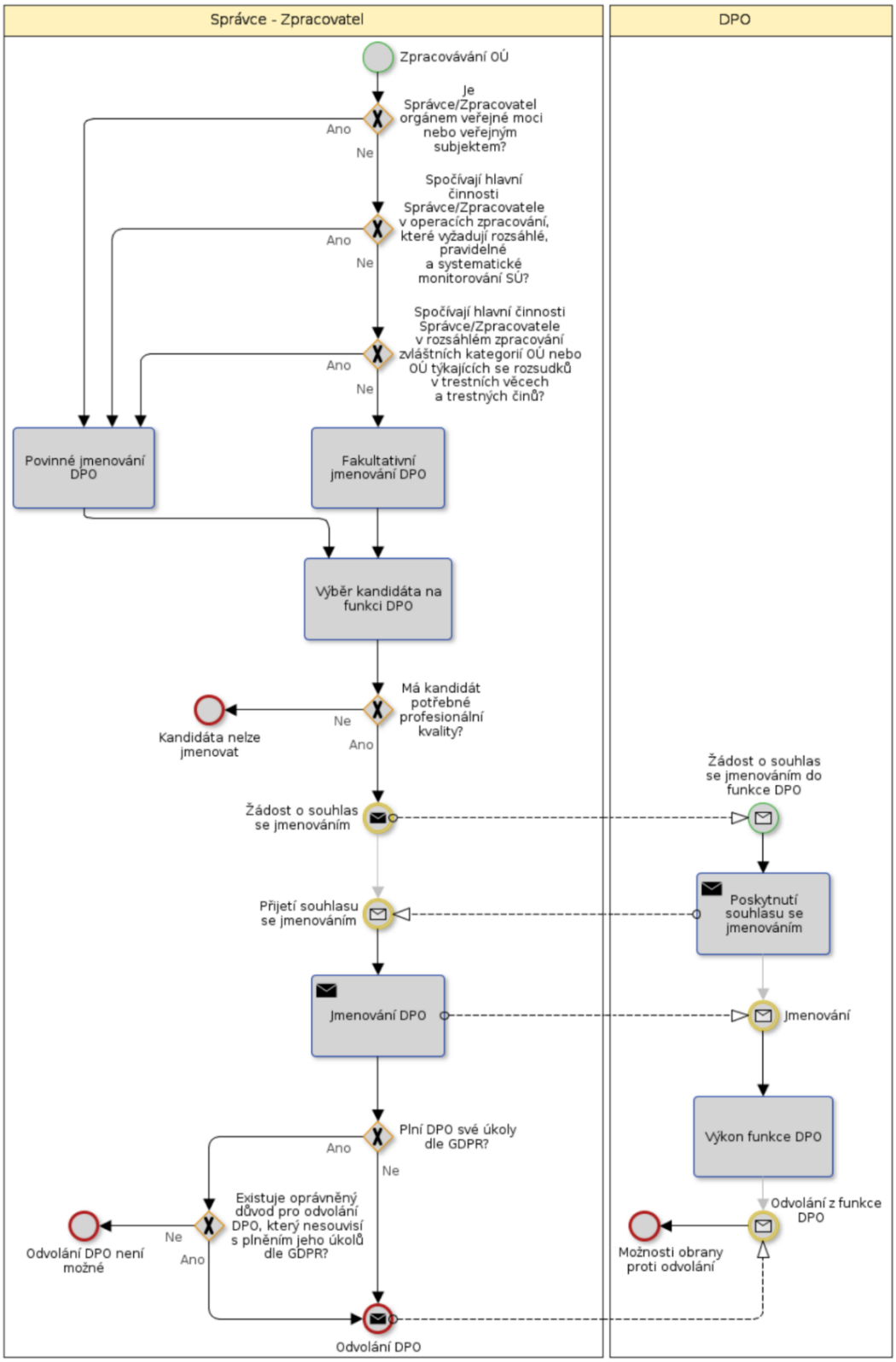
Z bezpečnostních důvodů (pro případnou jednoduchost výměny pověřence a pro udržení informovanosti statutárního zástupce) by měl být e-mail na pověřence založen neutrálně, tedy nikoliv na konkrétní jméno osoby a zároveň by mě být vytvořen na doméně školy – typicky *poverenec@domenaskoly.cz*. Není vyloučena anglická zkratka *dpo@...*, dozorový úřad se však k používání nečeských pojmů z obecného nařízení (kromě zažitého „GDPR“) vyjadřuje negativně.[181] Má-li v českém překladu obecného nařízení zkratka ekvivalent, měla by být využívána.

Praktický pohled je třeba zaměřit na náklady na pověřence a na způsob jeho zasmluvnění. Přes počáteční vysoké ceny za služby pověřenců se cena pro školy ustaluje na jednotách stokorun měsíčně. Asi nejlepší forma spolupráce s pověřencem je na bázi pracovněprávního vztahu, obvykle formou dohod konaných mimo pracovní poměr.

Pro funkci pověřence není doporučováno využívání vlastních zaměstnanců. Podílejí-li se totiž na zpracování, dostávají se do střetu zájmu. Navíc vzniká komplikovaný vztah nadřízenosti vedení školy a nezávislosti pověřence kontrolujícího v opodstatněných případech i operace zpracování prováděných svými nadřízenými. Pověřenec má při své práci navíc téměř neomezený přístup k osobním údajů svých kolegů (např. v personální agendě), což v reálném provozu školy skýtá prostor ke vniku konfliktům v kolektivu.

Následující obrázek znázorňuje rozhodování o jmenování a odvolávání pověřence.

[180] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 37, odst. 7.
[181] MATOUŠOVÁ, M. *Konzultace pro pověřence pro ochranu osobních údajů, Praha 9. října 2018*. Praha: Úřad pro ochranu osobních údajů, 2018.



Obrázek 11: Jmenování a odvolávání pověřence[182]

[182] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

Chce-li škola minimalizovat náklady na pověřence, je vhodné se domluvit s podobnou organizací a křížově si vyměnit pracovníky z vlastních řad.

Velmi často bývá k vidění model, kdy zřizovatelé, tedy krajské, městské i obecní úřady, poskytují hromadně bezplatně pověřence všem svým příspěvkovým organizacím. Jedná-li se o kvalifikovanou osobu, lze tento postup jen doporučit.

Protipólem zde uvedeného jsou smlouvy uzavírané krátce před účinností obecného nařízení, na základě kterých byly školám poskytovány služby pověřenců za mnohatisícové měsíční částky.

V rámci revize implementace GDPR by škola měla hledat vyvážené řešení kvality pověřence a nákladů na jeho služby. **Vzhledem k tomu, že pověřenec na rozdíl od ředitele školy za dodržování nařízení neodpovídá, je vhodné důkladně prověřit jeho kvality. Jedním z doporučených způsobů je zapojit ho do inventury procesů zpracování, postoupit mu tvorbu zásad a poučení a přenechat mu za úkol proškolení všech zaměstnanců školy. Kombinace těchto tří úkolů obvykle prověří jeho erudovanost.**

4.6 Fotografie, video a kamerové systémy ve škole

Materie fotografování je velmi obsáhlá a komplikovaná. Téma zachycení podobizny člověka je však v prostředí škol natolik nepochopené, že je nutností se alespoň pokusit o narovnání některých pochybení a o vyvrácení šířících se fám.

Kapitolu je proto vhodné uvést narušením jednoho školního postulátu, že fotografování je zpracováním osobních údajů a je vhodné žádat zákonné zástupce dětí o souhlas se zpracováním osobních údajů pro účely pořizování fotografií při různých školních aktivitách.

V následujících podkapitolách bude postupně vysvětlena problematika fotografování a natáčení dětí ve škole i na školních akcích, zveřejňování fotografií či záznamů, fotografování zaměstnanců školy a záznamů z kamerových systémů.

Legislativně jsou pravidla zachycování podobizny člověka zakotvena v občanském zákoníku, konkrétně v § 84–90. Vztahu tohoto kodexu práva a GDPR se stručně věnuje v teoretické rovině kapitola 3.1.2, následující podkapitoly budou zaměřeny více prakticky.

V prostředí školy se obvykle setkáváme se čtyřmi režimy, čtyřmi obecnými účely, pořizování fotografií nebo videa. Detailněji jsou popsány níže. Kromě čtvrtého uvedeného, popisujícího kamerové systémy, jde vždy o fotografie nebo časově omezené audiovizuální záznamy. Tím je myšleno pořizování standardních fotografií a běžné natáčení videa pomocí

mobilních telefonů, přenosných fotoaparátů a příručních kamer. Do této kategorie nespadají kontinuálně pořizované záznamy z kamerových systémů.

4.6.1 Fotografování a natáčení na soukromých akcích

Fotografováním a natáčením na soukromých akcích, byť konaných v prostředí školy, jsou myšlena soukromá setkání učitelů v rámci různých oslav, ale i běžně konaná soukromá setkání pedagogů s rodiči a jejich dětmi v rámci akcí neorganizovaných oficiálně školou (pouštění draků, opékání vuřtů, majálesy apod.). Pedagogové se jich obvykle účastní ve svém volnu. V těchto případech se na nakládání s fotografiemi a záznamy uplatňují čistě pravidla občanského zákoníku, a to i na případné následné zveřejňování pořízených fotografií doprovázené ztotožňováním osob. Škola zde není v postavení správce. Fotografování probíhá bez výslovného souhlasu osob, ale není skryté. Každý, kdo je takové akce účasten, může důvodně předpokládat, že bude soukromými osobami pro soukromé účely dění dokumentováno. Přeneseně můžeme hovořit o konkludentní formě souhlasu, nevyhýbají-li se subjekty fotografování. Pokud si někdo fotografování nebo natáčení své osoby nepřeje a svůj nesouhlas dá najevo, pravidla morálky standardně a zcela přirozeně postačí na regulaci takového počínání. Škola není v nakládání s fotografiemi, ani s jejich pořizováním, nijak spojena. Účastnící obdobných setkání tak činí pouze pro vlastní osobní účely. Pravidla z nařízení GDPR se tak neaplikují.

4.6.2 Fotografování a natáčení zaměstnanců na oficiálních školních akcích

Děje se tak například za účelem dokumentování postupů na různých školeních, poradách apod. a jde o zcela přirozené, v drtivé většině případů také účelu přiměřené jednání. Občanský zákoník toto připouští bez souhlasu osob. Fakt, že tak činí zaměstnavatel ve vztahu ke svým zaměstnancům, nepředstavuje problém, jsou-li zaměstnanci na toto upozornění a mají-li prostor se k takové činnosti vyjádřit, aniž by to na ně mělo negativní dopad. Případné následné použití fotografií spolu s identifikací osob, tedy při doplnění podobizny jménem osoby, je sice zpracováním osobních údajů v duchu nařízení GDPR, ale jsou-li takové materiály využívány pro interní potřebu školy nebo jako součást přiměřeného neinvazivního zveřejňování v rámci reportážní činnosti, je zcela legitimní.

Příkladem může být uveřejnění fotografií účastníků pedagogické rady ve školním časopisu nebo na webových stránkách školy spolu s článkem o účasti, o řešených tématech a výstupech. Jde o jednoznačný oprávněný zájem školy (viz kapitola 4.1.6). Ve vybraných

případech, jde-li například o akce řešící veřejně diskutované problémy nebo dotýkající se vzdělávání, může být takové použití fotodokumentace v rámci informování v médiích prováděno pod právním titulem „veřejný zájem“ (viz kapitola 4.1.5).

V naprosté většině případů se tedy takové zpracování neprovádí na základě souhlasu se zpracováním osobních údajů. Právními důvody jsou dle okolností oprávněné zájmy školy nebo veřejný zájem.

Důležité je ovšem správné informování zaměstnanců, že k takovýmto zpracováním dochází (viz kapitola 3.6.1 věnující se právu na informace), v rámci kterého jsou seznámeni se svými právy, především pak právem podat námitku proti zpracování prováděném v oprávněném nebo veřejném zájmu.

Pokud zaměstnanec svého práva na námitku využije a bude školu žádat o nezveřejňování a další nezpracovávání jeho fotografií nebo záznamů, je nejen povinností školy tuto žádost odpovědně posoudit, ale i projevem slušného transparentního přístupu jí vyhovět, neohrozí-li to nepřiměřeně činnost školy. Právo na ochranu soukromí osob je obvykle nadřazeno uvedeným zájmům školy. Vyhodnocení je však spíše subjektivní.

4.6.3 Fotografování a natáčení dětí při školních aktivitách

Na školou organizovaných akcích, nebo těch, kterých se škola účastní v přímé souvislosti s organizací vzdělávání, případně při dokumentování pedagogických postupů, které nelze efektivně zachytit jiným způsobem, je fotografování prováděno v souladu s občanským zákoníkem, a to bez souhlasu osob. Následné zpracování fotodokumentace zachycující podobizny subjektů, byť jde o děti, je legitimní, i když jsou ve vybraných případech snímky doplněny o další identifikátory (typicky jméno, věk, název školy apod.). Legitimita je dána ustanovením § 89 občanského zákoníku *„Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.“*[183]

Je třeba zdůraznit, že takto pořízené fotografie z probíhající výuky, školních výletů, škol v přírodě, uměleckých vystoupení, soutěží, olympiád a dalších podobných akcí nesmí být využívány pro komerční účely, nesmí být zpracovávány nepřiměřeně

[183] Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2012, částka 33, číslo 89, § 89.

a k jiným účelům a nesmí zachycovat osoby v nedůstojných, nevhodných nebo jakkoliv ponižujících situacích.

V této kategorii pořizování fotografií dělají školy nejvíce chyb. Přes laxní přístup a neřešení této problematiky, tedy ponechání ji bez pravidel, se objevuje spíše protipól, tedy přehnaně opatrný postup, který škodí zamýšleným účelům.

Pokud školy nesprávně vyžadují po zákonných zástupcích žáků souhlas se zpracováním osobních údajů pro účely fotografování, což je v podstatě oxymóron, dopouštějí se porušování obecného nařízení. Má-li být fotografování z nějakého důvodu postaveno na souhlasu, musí se jednat o „souhlas se zachycením podobizny člověka" ve smyslu § 84 občanského zákoníku. Teprve následné použití fotografií pro účely jednoznačné identifikace osoby nebo spolu s dalšími osobními údaji identifikujícími subjekt lze označit za zpracování osobních údajů. Vyžadují-li to okolnosti, je postaveno na souhlasu se zpracováním dle GDPR, v prostředí škol je však obvykle prováděno pod právním důvodem „veřejný zájem" (viz kapitola 4.1.5).

Hranice mezi zpracováním prováděném bez a se souhlasem je sice tenká, je však třeba ji rozlišovat a neuvádět rodiče dětí v omyl vyžadováním souhlasů v rozporu s obecným nařízením.

Škola by pochopitelně měla respektovat případná přání zákonných zástupců dětí na nezveřejňování fotografií svých dětí, tedy vyjádření opt-out principu, je-li k tomu opodstatněný důvod. V praxi byly zaznamenány situace, kdy byla rodina v programu na ochranu svědků a bylo nutné eliminovat veřejnou publicitu jakýchkoliv členů dotčené rodiny. Je to však spíše vzácností a s rodiči je třeba o důsledcích takového rozhodnutí diskutovat. Deklarovaný veřejný zájem u následného zpracovávání/zveřejňování fotografií dává osobám vykonávajícím rodičovskou povinnost dostatečný prostor pro podání námitky proti zpracovávání fotografií jejich dětí. Opět je důležité všechny zainteresované správně informovat, tedy pravidla fotografování dětí přehledně popsat v informacích o zpracování osobních údajů.

Vycházíme-li z premisy, že škola fotografie používá opravdu s rozumem a zejména je **nikdy neprezentuje na sociálních sítích nebo prostřednictvím obdobných nekontrolovatelných kanálů,** je v zájmu všech, ten úsek dětského života stráveného ve školách dokumentovat. **Hodnota takových fotografií je nevyčíslitelná a je velkou škodou**

o ně děti připravit jen díky nesmyslně přísnému vykládání právních norem nebo chybné komunikaci školy s rodiči.

Pořizování fotografií dětí by ve školách nemělo být dotčeno vyjádřením námitky, resp. škola by měla děti i v takových případech fotografovat dál, avšak jejich fotografie smí poskytnout pouze zákonným zástupcům. Sama by je neměla dále zpracovávat.

Pro pochopení celé šíře problematiky je třeba uvažovat o vážných důsledcích na psychiku dětí, které jsou vyloučeny z kolektivu, vyjádří-li rodiče nesouhlas s jejich fotografováním. Prostor pro takový nesouhlas je dán právě zcela nadbytečným dotazováním. V situaci, kdy je ve třídě třiceti dětí jedno dítě vyřazeno z možnosti fotografování, dochází ke zcela patologickým situacím. Typicky v případě, kdy je dítě umístěno stranou fotografovaného dění, aby fotografující osoby dostály vyjádřenému nesouhlasu. Jde o zjevnou diskriminaci dítěte vyloučením ze skupiny děti narušující vzájemné sociální vztahy.

Bez výslovného souhlasu zákonných zástupců by se však nikdy neměly objevit fotografie a videozáznamy na sociálních sítích (typicky Facebook, YouTube, Instagram, Pinterest, TikTok, Twitter aj.), nebo na webových stránkách, které nemá z hlediska obsahu škola pod vlastní kontrolou. Vzhledem k licenčním ujednáním většiny sociálních sítí (obsah se stává jejich vlastnictvím nebo k němu získávají neomezené právo použití) a vzhledem k téměř trvalé stopě, kterou zanechává obsah na nich umístěný, je důrazně doporučeno, je zcela vyřadit z používání pro účely distribuce fotografií dětí. Souhlas rodičů sice tzv. „přikryje“ nakládání s předmětným obsahem, ale ten se dostává mimo kontrolu a dětem může v budoucnu značně zkomplikovat snahy o ochranu jejich soukromí. Roztomilá fotografie z dětství může být v jejich vyšším věku zneužita ke kyberšikaně apod.

Děti obvykle nedostávají prostor se k této otázce vyjádřit. Rodiče poskytující souhlas pro plnění školního účtu na Facebooku fotkami jejich ratolestí často nechápou zrádnosti online prostředí, které se dlouhodobě nedaří zkrotit ani evropskými nařízeními, jakými je například GDPR nebo chystané nařízení ePrivacy[184]

V závěru práce jsou obdobné situace zhodnoceny v kontextu dalších povinností vyplývajících z nařízení GDPR. Zdůrazněna je i úloha pověřence při posuzování správnosti

[184] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) COM/2017/010 final - 2017/03 (COD) [NÁVRH - NAŘÍZENÍ NENÍ ZATÍM SCHVÁLENO]. In: *EUR-Lex*. Brussels, 2017, .

nakládání s osobními údaji dětí. Právě pověřenec by měl hledat cesty k efektivnímu fungování školy v souladu s GDPR, nikoliv argumenty, proč některé činnosti zastavit s odůvodněním „pro jistotu“ nebo naopak opatřovat rozporuplná počínání právně „neprůstřelnými“ souhlasy.

4.6.4 Kamerové systémy

Pravidla pro provoz kamerového systému se záznamem se odvíjí od účelu, pro který je provozován. Ve škole se vyskytují obvykle dva důvody, tedy dva účely. Je možné se však setkat i s třetím typem použití popsaným níže.

Prvním je zajištění bezpečnosti školy, primárně ochrana dětí. V takovém případě je právním důvodem zpracování „veřejný zájem“.

Druhým případem může být pořizování záznamu z kamer za účelem ochrany majetku, tedy případné zachycení pachatelů pro účely dokazování. Pokud je v úmyslu poskytovat záznamy výhradně OČTŘ a kamerový systém chrání primárně majetek veřejné školy, je možné zpracování provádět opět na základě „veřejného zájmu“.

Třetí situací je pořizování nebo následné používání záznamu v oprávněném zájmu například pro kontrolu dodržování pracovní doby zaměstnanců nebo obecně pro kontrolu pohybu osob. V takovém případě je právní základ velmi slabý a je důležité testem proporcionality prokázat oprávněnost takového zpracování.

Bez ohledu na účel, pro který je systém provozován, je třeba respektovat práva osob na ochranu soukromí a pečlivě zvažovat použití kamer vně školy. Umístění kamer na plášti budovy, zachycují-li veřejné prostranství, musí být adekvátně zdůvodněno a musí být zajištěno, aby kamery nesledovaly například okna vedlejších budov.

Určitá pravidla platí i pro vnitřní kamery, ty nesmějí být umístěny v místech, kde by docházelo k narušení soukromí (kabinety pedagogů, prostory k převlékání apod.). Problematické a komplikovaně obhajitelné je také umísťování kamer do tříd, proto se důrazně nedoporučuje.

O přítomnosti kamerového systému musí být osoby upozorněny při vstupu do střežených prostor a informace o účelech a právních důvodech je třeba zapracovat do veřejně přístupných informací o zpracování. V této souvislosti je důležité připomenout zásadu účelového omezení. Pokud je záznam pořizován ve veřejném zájmu za účelem zajištění bezpečnosti dětí a subjektům je takto deklarován, je nepřípustné jej následně používat

v oprávněném zájmu například pro kontrolu docházky zaměstnanců nebo kontrole špatného parkování na dvoře školy.

Poskytování záznamů policii v případě podezření na trestnou činnost tím samozřejmě není dotčeno a posuzování slučitelnosti účelů zpracování se v takových situacích neprovádí.

Zvláštní situace může nastat při pokusu subjektu o výkon práva na přístup k osobním údajům. Vyžádá-li si část záznamu z kamerového systému, který je provozován ve veřejném zájmu, bude takové poskytnutí obvykle zamítnuto. Je-li záznam z kamer prováděn pod oprávněným zájmem školy, bude subjektu obvykle vyhověno, avšak nastává povinnost školy důsledně anonymizovat další osoby na záznamu, což přináší zvýšené náklady na výkon práva a v takovém případě je přiměřené požadovat po žadateli jejich úhradu.

4.7 Zpracovatelé v prostředí škol

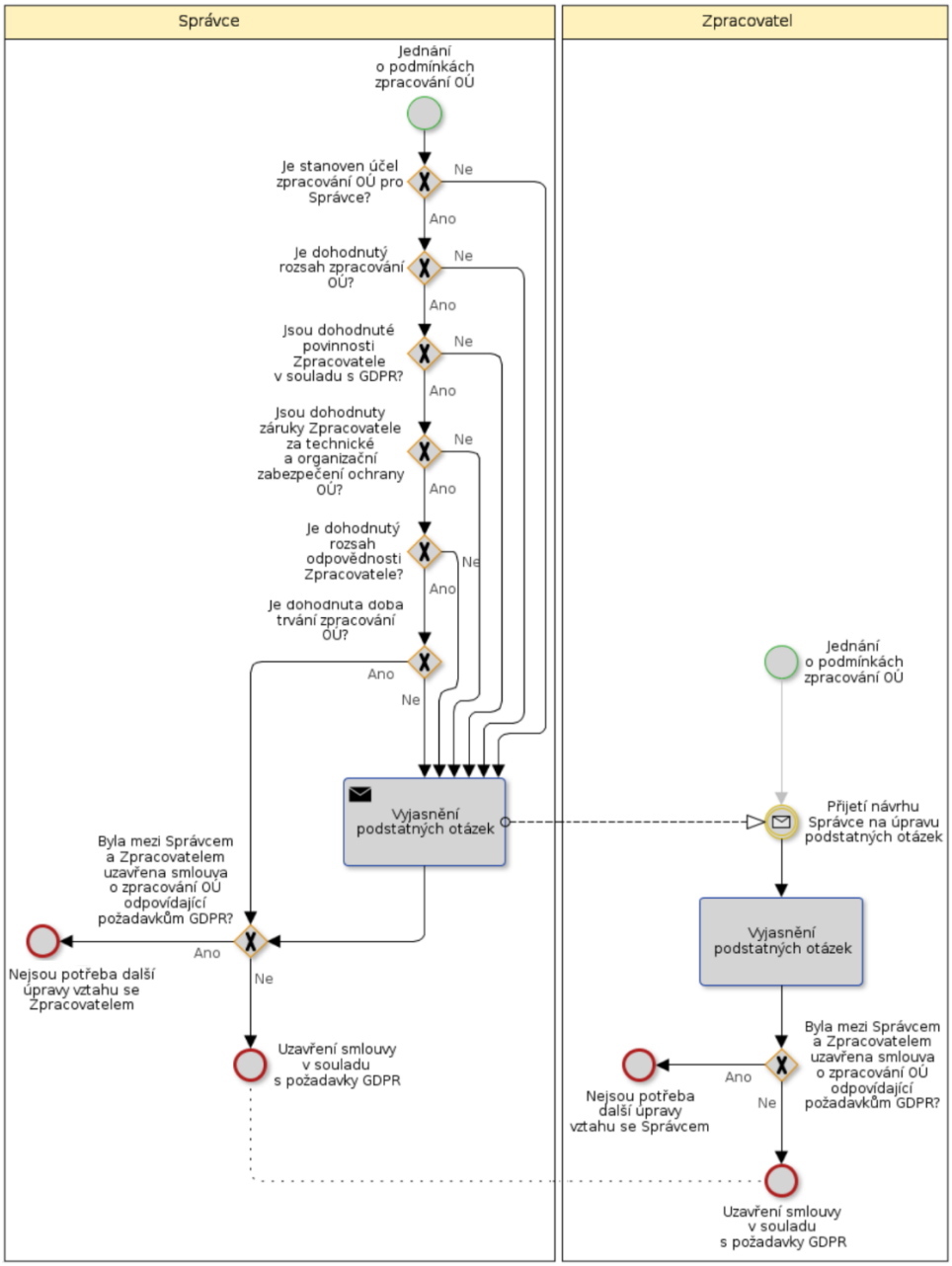
Určit v praxi, které spolupracující osoby, organizace, společnosti, dodavatelé či poskytovatelé služeb atd. jsou v roli zpracovatelů osobních údajů nebo pouze v roli případných příjemců, stojí primárně na pochopení, co je a co není zpracováním osobních údajů. Teoreticky je tato otázka řešena v kapitole 3.4.2.

V praxi škol je možné se setkat s reálnou potřebou uzavírání zpracovatelských smluv:

- s poskytovateli cloudových či hostingových služeb obvykle při provozu e-mailových a webových služeb, a především školních informačních systémů na serverech poskytovatelů (např. systém Bakaláři[185] nebo iZUŠ[186]),
- s externími účetními (nemá-li škola zajištěno vedení účetnictví osobami v pracovně-právním vztahu).

Jen zřídka je v pozici přímého zpracovatele externí IT firma. Správa výpočetní techniky a informačních systémů, tedy obvyklý servis výpočetní techniky, neprobíhá za účelem zpracovávání osobních údajů školy. Není vyloučeno, že by škole IT firma takové služby poskytovala, tedy že se by se dostala do role zpracovatele, obvykle je však se správou IT a ICT spojen pouhý přístup k osobním údajům, který je vhodné řešit pomocí NDA[187], tedy dohodou o mlčenlivosti.

[185] www.bakalari.cz
[186] www.izus.cz
[187] Non-disclosure agreement – dohoda o mlčenlivosti



Obrázek 12: Uzavírání zpracovatelských smluv[188]

Obrázek 12 zobrazuje postup najímání zpracovatele. Je doporučeno, aby na celý postup a na obsah smluv dohlížel pověřenec.

4.8 Pseudonymizace a anonymizace ve školách

Pseudonymizace a anonymizace se v praxi provádí velmi podobně, ovšem se zcela odlišnými výsledky, jak teoreticky vysvětluje kapitola 3.4.3.

[188] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

PSEUDONYMIZACE

Konkrétním příkladem pseudonymizování osobních údajů v prostředí škol je zabezpečení jmen účastníků přijímacích řízení, zkoušek, testů či olympiád. Při znalosti speciálního identifikátoru, kterým je jméno po celý průběh vyhodnocování nahrazeno, je následně žák nebo zákonný zástupce schopen vyhledat výsledky v seznamu, který je jako pseudonymizovaný kompletně zveřejněn. Zneužití údajů je minimalizováno, protože jen škola a konkrétní subjekt znají příslušný identifikátor, tedy určitý kód, kterým je nahrazeno skutečné jméno žáka.

Dalším příkladem je zabezpečení souboru šifrováním či heslem. Takové soubory sice mohou obsahovat osobní údaje, ale bez příslušeného hesla nebo dešifrovacího klíče jsou pro ostatní zcela nečitelné.

Takto lze zabezpečit nejen soubory ukládané na přenosné flashdisky či zasílané e-mailem, lze šifrovat celé disky, přenosné i pevně instalované v osobních počítačích. Bezplatný šifrovací nástroj BitLocker je součástí operačního systému Microsoft Windows 10 Professional. K dispozici jsou však i jiné bezplatné programy nebo jiná technická řešení, například přenosné šifrované USB flashdisky, které lze otevřít až po zadání příslušného hesla.

Obrázek 13: Pseudonymizace v pojetí kreslíře a učitele Milana Kocmánka

Pseudonymizace nesmí být pochopitelně nadužívána, její použití musí být přiměřené účelu a případnému riziku zneužití konkrétních osobních údajů. Na níže uvedeném obrázku kreslíře a dlouholetého učitele z Masarykovy základní školy v Lanžhotu, Mgr. Milana Kocmánka, je vidět možné nepochopení smyslu pseudonymizace (viz Obrázek 13).

Byť se jedná o vtip, přesně takový přístup byl v praxi mateřských a základních škol zaznamenán dozorovým úřadem. V rámci setkání pověřenců popsala doktorka Matoušová, vrchní rada pro vládní agendy, praxi nahrazování jmen dětí čísly, které se zákonní zástupci musí naučit, aby například věděli, která skřínka v šatně patří jejím dětem.[189]

ANONYMIZACE

Správně provedená anonymizace musí, pokud možno, vyloučit následné deanonymizování osobních údajů. V praxi provádějí anonymizaci školy například při vyřizování žádostí o informace podle informačního zákona. Anonymizují se vždy a velmi důsledně osobní údaje žadatelů o informace[190]. Opomenutí tohoto kroku je porušením obecného nařízení a rozhodovací praxe soudů toto potvrzuje.

Anonymizace je nutná rovněž při zveřejňování v registru smluv[191], je-li škola povinným subjektem. V menších školách bývá technicky správné provedení anonymizace při absenci programů určených pro editování skenovaných PDF souborů obvykle komplikované. Pro tyto účely Ministerstvo vnitra vypracovalo metodiku[192], a především poskytlo pro všechny orgány veřejné moci, tedy i školy, bezplatný anonymizační nástroj[193].

4.9 Metodická pomůcka MŠMT

Několik předchozích kapitol nastínilo určitou specifickou úlohu dokumentu „Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR)“[194]. Mělo jít o nástroj, který pomůže školám s praktickou implementací GDPR. MŠMT jej vydalo

[189] MATOUŠOVÁ, M. *Konzultace pro pověřence pro ochranu osobních údajů, Praha 9. října 2018*. Praha: Úřad pro ochranu osobních údajů, 2018.
[190] Zákon č. 106/1999 Sb. , o svobodném přístupu k informacím. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 1999, částka 39, číslo 106.
[191] Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2015, částka 144, číslo 340.
[192] *Metodický návod k aplikaci zákona o registru smluv*. In: . Praha: Ministerstvo vnitra, 2021, 1.11.
[193] *Ministerstvo vnitra: Nástroj pro anonymizaci dokumentů* [online]. [cit. 2021-01-10].
[194] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) (aktuální web)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021].

6. listopadu 2017[195] a ve velmi krátké době měl tisíce stažení. Týden před účinností obecného nařízení, konkrétně 17. května 2018, činil počet jeho stažení ze stránek MŠMT 29 096[196], krátce po účinností GDPR, 11. června 2018 (bližší snímek WAYBACK MACHINE na serveru „The Internet archive“ není bohužel k dispozici) byl stažen již 34 209x[197] a do vydání nové verze (v srpnu 2019) překročil 42 tisíc stažení[198]. Na dokument bylo okazováno při různých seminářích a školeních – stal se primárním zdrojem informací pro implementaci GDPR ve školství.

Pro srovnání, nová verze metodiky[199] obsahující opravu níže uvedených závažných nedostatků byla za poslední rok a půl (od vydání v září 2019 do března 2021) stažena 3 190x.

Z uvedených čísel je zjevné, že opravené metodické pomůcce je, pravděpodobně díky malé mediální publicitě a vlažnému zájmu o problematiku ochrany osobních údajů, věnována minimální pozornost.

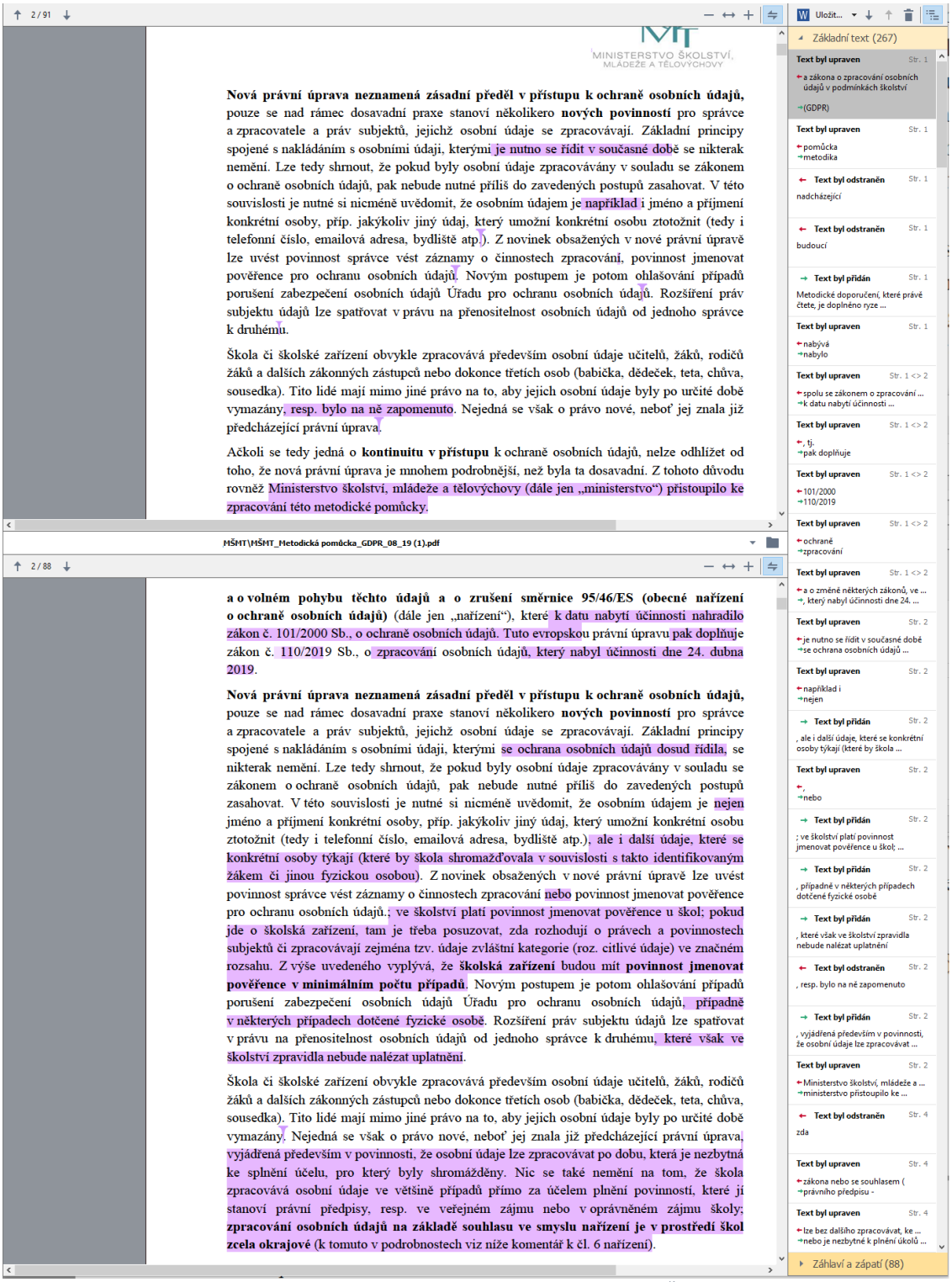
4.9.1 Komparace dvou verzí metodiky

Pro přesné porovnání starší a nové verze metodiky byl použit program ABBYY FineReader PDF 15 Corporate obsahující komparační modul pro identifikaci rozdílu v PDF souborech (viz Obrázek 14). Sktruktura i délka obou verzí je podobná, obsahem a významem pro aplikaci GDPR jsou však dokumenty diametrálně odlišné. Bylo nalezeno 355 změn, pro naplnění cílů práce však budou dále zkoumány pouze změny, které měly přímý dopad na posuzování zpracování osobních údajů ve školách a určování právních důvodů zpracování.

Obě verze metodiky svorně a správně deklarují, že *„Nová právní úprava neznamená zásadní předěl v přístupu k ochraně osobních údajů, pouze se nad rámec dosavadní praxe stanoví několikero nových povinností pro správce a zpracovatele a práv subjektů, jejichž*

[195] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství - 2017 (stránka s informacemi o soboru www.msmt.cz/file/44592)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2017 [cit. 01.03.2021].
[196] *The Internet Archive [MAY 17 2018]: http://web.archive.org/web/20180517095207/http:/www.msmt.cz/file/44592* [online]. [cit. 2021-03-03].
[197] *The Internet Archive [JUN 11 2018]: http://web.archive.org/web/20180611091356/http://www.msmt.cz/file/44592/* [online]. [cit. 2021-03-03].
[198] *The Internet Archive [SEP 22 2019]: http://web.archive.org/web/20190922122703/http:/www.msmt.cz/file/44592* [online]. [cit. 2021-03-03].
[199] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021].

osobní údaje se zpracovávají. Základní principy spojené s nakládáním s osobními údaji, kterými se ochrana osobních údajů dosud řídila, se nikterak nemění.“[200]



Obrázek 14: Ukázka z procesu komparace metodik MŠMT[201]

[200] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství - 2017 (stránka s informacemi o soboru www.msmt.cz/file/44592)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2017, s. 2 [cit. 01.03.2021].
[201] Vlastní zpracování v programu ABBYY FineReader PDF 15 Corporate

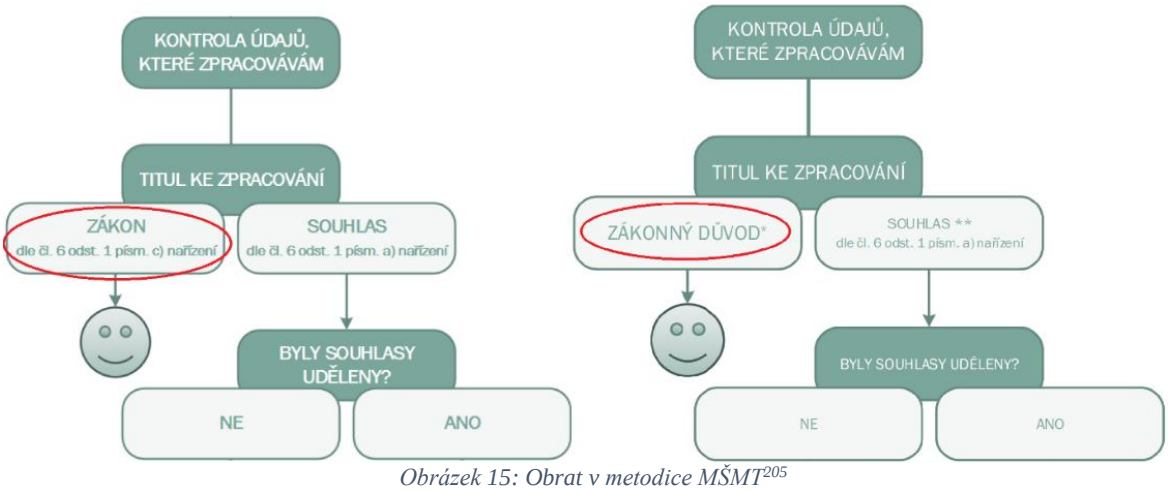
4.9.2 Obrat v metodice stanovování právních důvodů zpracování

Velký obrat nové metodiky v postoji k právním důvodům zpracování lze spatřit už na druhé straně doplněním odstavce, který v první verzi zcela chyběl:

„Nic se také nemění na tom, že škola zpracovává osobní údaje ve většině případů přímo za účelem plnění povinností, které jí stanoví právní předpisy, resp. ve veřejném zájmu nebo v oprávněném zájmu školy; zpracování osobních údajů na základě souhlasu ve smyslu nařízení je v prostředí škol zcela okrajové“[202]

Největší vypovídací hodnotu o východiscích obou metodik má Obrázek 16 a Obrázek 17. Obrázek 15 pro přehlednost nejprve rozhodující změnu zvýrazňuje. Starší verze metodiky téměř dva roky své existence nabádala její adresáty ke generování souhlasů se zpracováním vždy, není-li zpracování prováděno dle čl. 6, odst. 1., písm. c), tedy *„zpracování nezbytné pro splnění právní povinnosti, která se na správce vztahuje“*[203]

Další čtyři právní důvody jsou metodikou v jejich klíčových částech ignorovány, přičemž například zákonný důvod zpracování prováděného *„pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci“*[204] je pro školy stěžejní a jeho aplikací by se s blížící se účinností GDPR v květnu 2018 neodstartoval předem prohraný závod v uzavírání vysokého množství souhlasů.



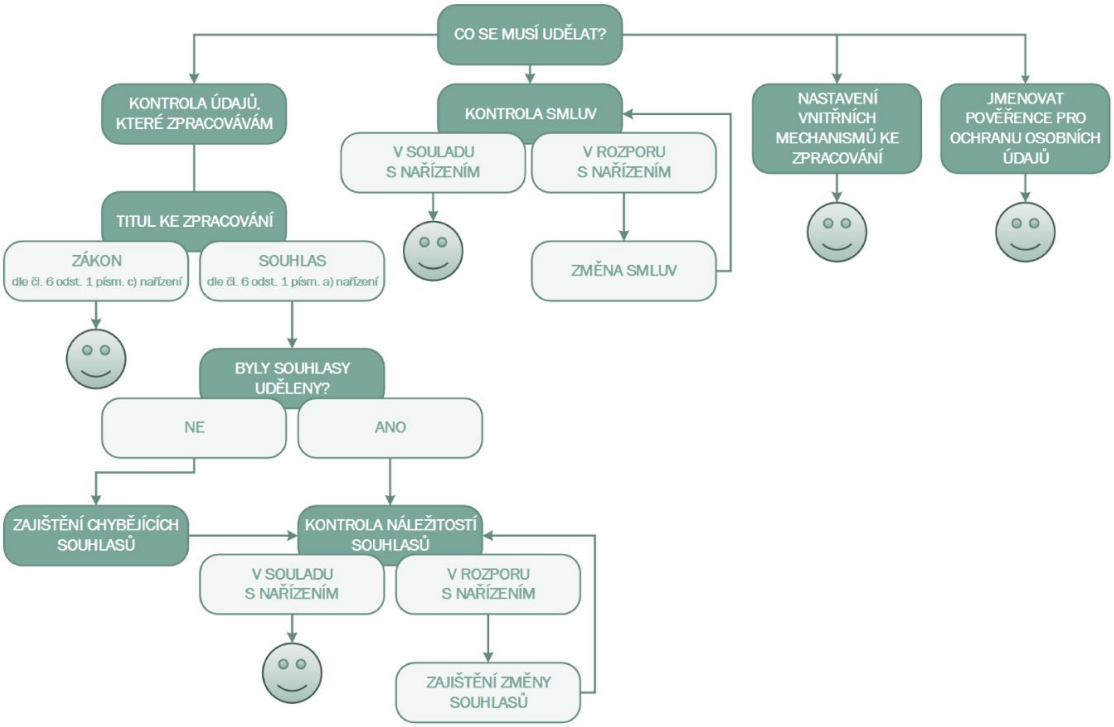
Obrázek 15: Obrat v metodice MŠMT[205]

[202] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019, s. 2 [cit. 01.03.2021].

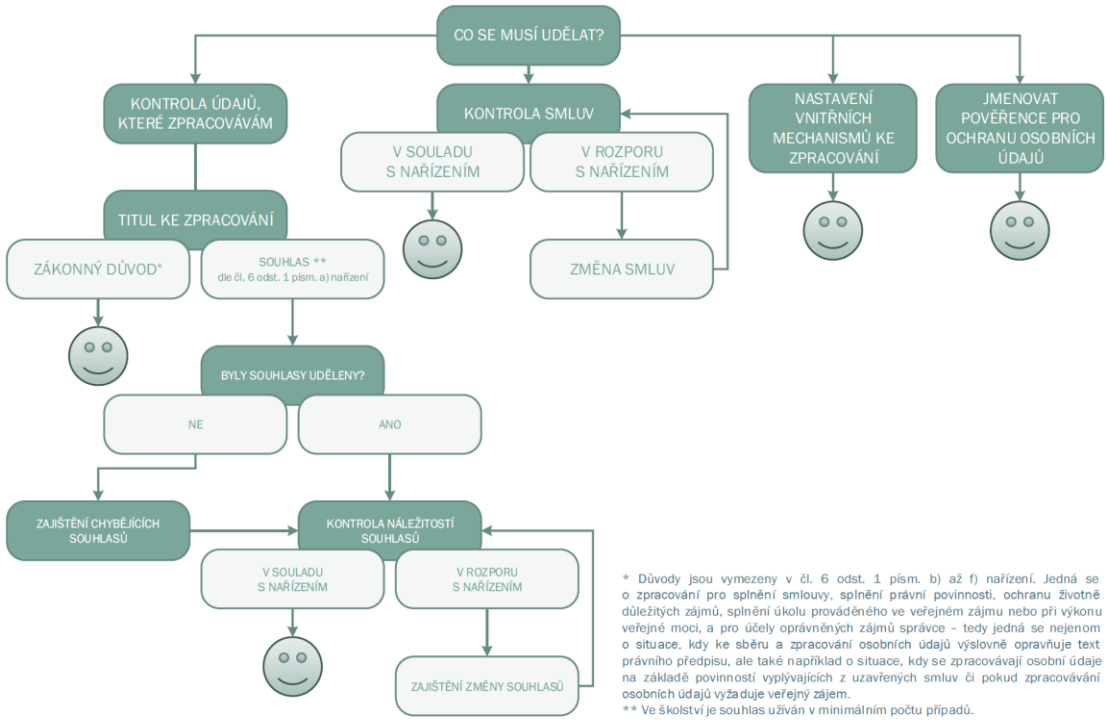
[203] *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. 2016, čl. 6, odst. 1., písm. c).

[204] *Ibid.*, čl. 6, odst. 1., písm. e).

[205] Vlastní zpracování – výřez z obrázků „*Co se musí udělat do dne nabytí účinnosti nařízení (tedy do dne 25. 5. 2018)?“* (Metodika MŠMT z listopadu 2017) a *„Postup před nabytím účinnosti nařízení (tedy do dne 25. 5. 2018) – co se musí udělat“*? (Metodika MŠMT ze září 2019)



Obrázek 16: Co se musí udělat do dne nabytí účinnosti nařízení? (starší metodika)[206]



Obrázek 17: Postup před nabytím účinnosti nařízení – co se musí udělat? (nová metodika)[207]

[206] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství - 2017 (stránka s informacemi o soboru www.msmt.cz/file/44592)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2017 [cit. 01.03.2021].

[207] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021].

Vzhledem k tomu, že je tato metodika dle MŠMT určena všem, kdo přijdou ve školství do styku s problematikou osobních údajů, například pro[208]:

- *ředitele škol a školských zařízení,*
- *rektory vysokých škol a další akademické pracovníky,*
- *učitele,*
- *hospodáře a účetní škol,*
- *zaměstnance krajských a obecních úřadů,*
- *správce sítě, jiné pracovníky IT a další,*

je potenciál jejího dopadu na soulad obecným nařízením obrovský.

Starší metodika nabádala ke kontrole zpracovávaných údajů a prověření, *„zda je tak činěno na základě zákona nebo se souhlasem (osobní údaje, jejichž zpracování vyplývá ze zákona lze bez dalšího zpracovávat, ke zpracování ostatních údajů je třeba souhlas)“.*[209]

Novější metodika ve stejném odstavci správně uvádí, že má být ověřeno, zda je zpracování *„činěno na základě právního předpisu - osobní údaje, jejichž zpracování vyplývá ze zákona nebo je nezbytné k plnění úkolů prováděných ve veřejném zájmu či při výkonu veřejné moci, resp. v oprávněném zájmu školy, lze zpracovávat, aniž by bylo nezbytné zajišťovat souhlas subjektů údajů [jde o jakékoli jiné důvody než je zpracování na základě souhlasu dle čl. 6 odst. 1 písm. a) nařízení]; zpracování pro plnění smlouvy je bez souhlasu; nebo v okrajových případech se souhlasem subjektu údajů“.*[210]

V tomto duchu pokračuje celý dokument a odpovídajícím způsobem narovnává předchozí nedostatky.

V kapitole věnované rozlišování zpracování osobních údajů na základě zákona dokonce nová metodika ostře kritizuje aplikaci souhlasů, když uvádí, že *„V případě zákonného zpracování souhlas subjektu údajů není potřebný ani relevantní; vyžadování souhlasu v takových případech by naopak mohlo být nezákonné“.*[211]

---

[208] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství - 2017 (stránka s informacemi o soboru www.msmt.cz/file/44592)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2017, s. 1 [cit. 01.03.2021].
[209] *Ibid.*, s. 4 [cit. 01.03.2021].
[210] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019, s. 4 [cit. 01.03.2021].
[211] *Ibid.,* s. 11 [cit. 01.03.2021].

Mezi další přínosy novější metodiky patří kvalitnější vysvětlení způsobilosti k poskytnutí souhlasu ve vztahu ke specifickým službám informační společnosti.

V kapitole věnované souhlasu se zpracováním osobních údajů nová metodika při hodnocení tzv. „přesouhlasování" otevřeně kritizuje postupy doporučované předchozí verzí.

„Zpracování osobních údajů na základě souhlasu je obecně ve školství ojedinělé. Příkladem špatné praxe, kdy škola nadbytečně vyžaduje souhlas se zpracováním osobních údajů, je např. situace, kdy je vyžadován souhlas pro zveřejnění jména a příjmení žáků účastnících se za školu soutěží a olympiád, či pro zveřejnění výtvarných děl žáků v prostorách školy. Konečně, je třeba nezaměňovat udělení souhlasu ke zpracování osobních údajů pro konkrétní účely s plněním informační povinnosti správce údajů. V praxi škol se totiž ukázalo, že příčinou vyžadování nadbytečných až nesmyslných souhlasů je často absence informací pro rodiče, kdy souhlas de facto plní roli informační povinnosti."[212]

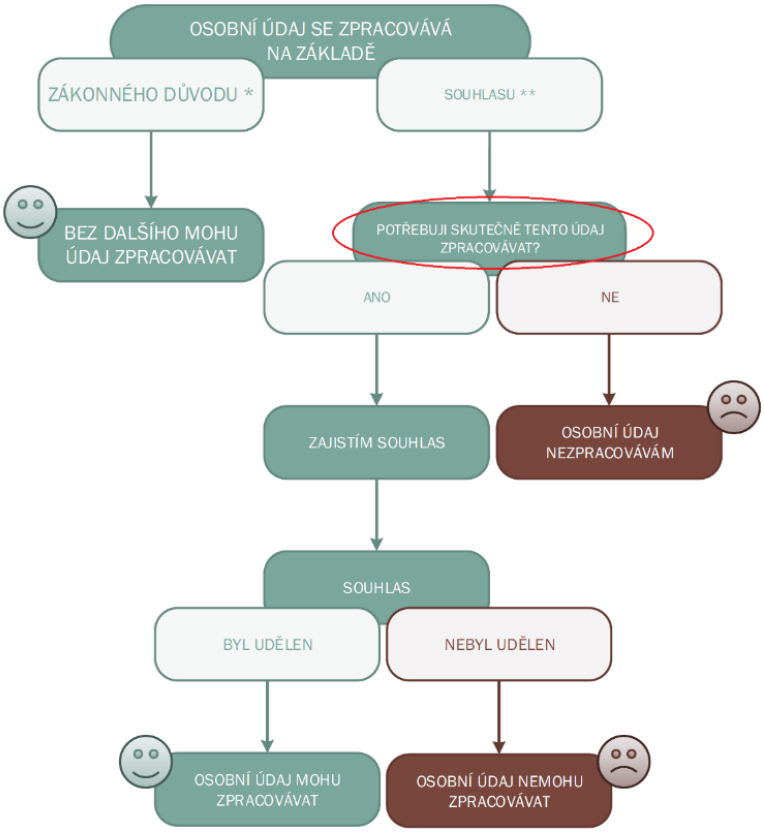
Postupoval-li ředitel školy nebo pověřenec při implementaci GDPR dle pomůcky MŠMT, *„příčinou vyžadování nadbytečných až nesmyslných souhlasů"* nebyla absence informací pro rodiče, ale kvalita metodické pomoci ministerstva školství.

Jakkoliv byla situace před účinností nařízení GDPR nepřehledná, existovalo v té době mnoho literatury vykládající obecné nařízení správně. Cílem této práce není hledat viníka, resp. autora chyb v metodickém doporučení MŠMT. Cílem je upozornit na závažné nedostatky materiálu, podle kterého v České republice postupovaly při implementaci tisíce škol. **Úkolem komparace metodik je upozornit na existenci nové verze, verifikovat její relevantnost a použitelnost a připravit ředitele škol na nezbytnost revize implementace GDPR, byla-li tato v jejich škole motivována starší verzí návodu od MŠMT.**

Závěrem komparace je třeba upozornit, že i přes katarzi, kterou nová metodika prošla, stále zůstala problematika souhlasů nepochopena z pohledu rozhodování školy o aplikaci souhlasu a **„potřebou"** nebo **„chtěním"** jejich zpracování. Mezi tím je propastný rozdíl, protože potřebuje-li škola nějaké údaje a onou potřebou je jakákoliv smysluplná činnost související s organizací vzdělávání, efektivním fungováním školy, naplňováním poslání školy apod., potom **je souhlas se zpracováním evidentně nesprávným titulem zpracování**. Nepotřebuje-li předmětné údaje škola vůbec (pouze je tzv. chce), dávalo by použití souhlasu

[212] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019, s. 13 [cit. 01.03.2021].

smysl. Nesprávně se k tomu staví původní i aktuální metodika (viz Obrázek 18) a před takovým počínáním je nutno varovat nejen školy, ale veškeré správce.



Obrázek 18: Rozhodování o potřebě zpracovávat (nová metodika)[213]

4.10 Postup revize implementace GDPR v prostředí škol

Pro potřeby této práce je prakticky doporučovaný postup vedení projektu implementace GDPR, jak již bylo vysvětleno v kapitole 3.9.3, na základě empirických poznání při vzorových implementacích GDPR v komparaci s projektovým řízením IPMA, zjednodušen. Pro naplnění cílů práce není po odborné stránce detailizován procesní management, návrh se orientuje na podstatu a účel jednotlivých činností, nikoliv na způsoby provedení a principy jejich řízení. Není řešena otázka reportingu ani kontroly jednotlivých fází ze strany manažera projektu. Samotná revize implementace GDPR je v prostředí školy relativně snadná a příliš komplikované a precizní procesní řízení by mohlo způsobit větší alokaci času než revize implementace samotná.

Postup je rovněž více optimalizován s ohledem na očekávaný praktický přínos práce, kterým je zejména podpora ředitelů škol při první revizi dříve uskutečněného zavádění

[213] *Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137)* [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019, s. 5 [cit. 01.03.2021].

GDPR, tedy s předpokladem, že od aplikace GDPR provedenou ještě před jeho účinností v květnu 2018 neproběhla komplexní kontrola souladu. Následná opakovaná revize obvykle nepředstavuje velkou zátěž, dodržuje-li se od poslední provedené revize nastavený standard. Zde doporučený komplexní postup lze přesto bez obav aplikovat.

Naopak provádění zcela nové implementace GDPR ve školském zařízení není příliš pravděpodobné, leda by se jednalo o nově zřízenou organizaci. Níže navržený postup je však univerzální, na drobné odlišnosti je v příslušných subprocesech při deskripci upozorněno, a je možné jej aplikovat i na nově zřízené školy nebo na školy, ve kterých k implementaci GDPR v minulosti vůbec nedošlo, což je zhusta nepravděpodobné, ne-li nemožné.

Předpokladem úspěšného zvládnutí celého procesu je angažovanost všech zaměstnanců na projektu, zejména pak osobní účast ředitele školy na všech jeho fázích. Pro schopnost následného dodržování standardu ochrany osobních údajů je porozumění celé problematice klíčové. Nejlepší cestou k uvedení činností do souladu s nařízením GDPR je provedení implementace svépomocí za přispění pověřence, případně za částečného přispění specialistů. Ti by však neměli provádět jednotlivé kroky formou externě poskytované služby, ale vést a vzdělávat aktéry ke svépomocné aplikaci obecného nařízení. Zaměstnanci školy tak lépe pochopí význam a podstatu obecného nařízení a budou schopni reagovat pružněji na případné legislativní změny, zejména pak na výkon práv subjektů údajů.

FÁZE PROJEKTU REVIZE IMPLEMENTACE GDPR

1) **Příprava na implementaci, resp. revizi implementace (podkapitola 4.10.1)**
    a. Prvotní zaškolení vedení školy specialistou na danou problematiku
    b. Sestavení a zaškolení projektového mini týmu
    c. Jmenování pověřence / ověření oznámení o jmenování pověřence a jeho zapojení do procesu
    d. Konzultace se zřizovatelem
    e. Sestavení rozpočtu
    f. Stanovení osoby odpovědné za analýzu zpracování
    g. Rozdělení úkolů a nastavení termínů
2) **Analýza zpracování osobních údajů (podkapitola 4.10.2)**
    a. Analýza vzorových materiálů
    b. Informování zaměstnanců o vstupní analýze zpracování
    c. Identifikace agend zpracování (definice účelů)

d. Sběr informací o zpracování osobních údajů
e. Kompletace informací do organizované datové struktury
f. Doplnění atributů zpracování (právní důvody)
g. Identifikace zpracovatelů a příjemců

3) GAP analýza (podkapitola 4.10.3)

a. Kontrola zákonnosti zpracování
b. Inventura a kontrola souhlasů se zpracováním
c. Inventura a kontrola balančních testů
d. Analýza vztahů se zpracovateli a příjemci
e. Kontrola elektronických i fyzických úložišť dat
f. Kontrola informačních systémů
g. Kontrola odpovědnosti a rolí ve zpracování
h. Revize dokumentace
i. Rozbor získaných informací, posouzení legislativního souladu a tvorba výstupu GAP analýzy

4) Analýza rizik (podkapitola 4.10.4)

a. Posouzení jednotlivých agend z hlediska rizika zpracování
b. Vyhodnocení rizik a návrh opatření

5) Tvorba a úprava dokumentace (podkapitola 4.10.5)

a. Plnění informační povinnosti
b. Uzavření a revize zpracovatelských smluv, uzavření NDA
c. Uzavření chybějících souhlasů, rušení nadbytečných souhlasů
d. Tvorba aktuálních záznamů o činnostech zpracování
e. Aktualizace smluv v pracovněprávních vztazích

6) Zjednodušený audit a revize ICT (podkapitola 4.10.6)

a. Inventura HW a SW
b. Ověření možnosti kontroly přístupu k informacím
c. Inventura a evidence přístupů
d. Tvorba a ověření obálkových účtů
e. BYOD a využívání služebních počítačů pro soukromé účely
f. Tvorba dokumentace

7) Úprava procesů a přijetí opatření (podkapitola 4.10.7)

a. Kontrola a nastavení pravidel pro práci s informacemi

b. Kontrola a nastavení pravidel pro spisovou službu
c. Specifická úprava pravidel pro agendu informačního zákona a zákona o registru smluv
d. Kontrola a nastavení pravidel pro práci s ICT
e. Nastavení pravidel pro výkon práv subjektů
f. Nastavení přenesené odpovědnosti
g. Vydání vnitřního předpisu a přijetí opatření

8) Post-implementační fáze (4.10.8)

a. Kontrola plnění úkolů
b. Kontrola dokumentace a publikace povinných dokumentů
c. Úprava postupů pro budoucí revizi

Detailněji se jednotlivým fázím věnují následující podkapitoly 4.10.1 až 4.10.8 představující subprocesy celého procesu implementace GDPR, resp. revize implementace. Na základě své návaznosti jsou jednotlivé činnosti slučovány do těchto subprocesů při dodržení chronologické posloupnosti.

Protože tato práce přímo nezohledňuje velikost školy, ale poskytuje co nejvíce univerzální postupy, jsou od sebe odděleny a samostatně popsány činnosti, které mohou být v menších školách jednoduše sloučeny. Analogicky ovlivňuje velikost školy role osob v subprocesech. V popisech se mohou vyskytnout pozice, které na některých školách nemusí existovat. V takových případech jsou úkoly těchto osob standardně vykonávány osobou v jiné existující pozici. Není tedy obtížné přiřadit správně vybrané operace a kroky popisovaných subprocesů správným aktérům. S ohledem na velikost školy se může rovněž měnit čas potřebný pro dokončení subprocesu.

4.10.1 Příprava na implementaci, resp. revizi implementace

PRVOTNÍ ZAŠKOLENÍ VEDENÍ ŠKOLY

Úvodní edukace je pro nastavení správného směru a kvality subprocesů zásadní.

Vzhledem k břemenu přímé odpovědnosti za dodržování právních předpisů upravujících činnost školy ležícím na řediteli školy, musí být tento schopen celý projekt vést, nebo alespoň kontrolovat a vyhodnocovat jeho výstupy, svěří-li jeho vedení například svému zástupci. Musí znát principy fungování obecného nařízení, zejména pak veškeré povinnosti správce. V počáteční fázi (při přípravě na samotnou implementaci) musí dostatečně vzdělávat v předmětné problematice sebe, své zástupce i další vedoucí a klíčové pracovníky.

Toto prvotní zaškolení standardně provádí najatý externí pracovník nebo pověřenec pro ochranu osobních údajů, má-li odpovídající edukativní schopnosti bez ohledu na jeho profesní kvality. Samotná způsobilost k výkonu pověřence a precizní znalost problematiky ochrany a zpracování osobních údajů automaticky nepredikuje prezentační schopnosti a dovednosti v předávání informací.

SESTAVENÍ A ZAŠKOLENÍ PROJEKTOVÉHO MINI TÝMU

V rámci této činnosti je sestavován malý tým složený z osob, které budou koordinovat sběr informací v navazujícím subprocesu analýzy zpracování osobních údajů. Kromě vedení školy bývá jeho součástí správce výpočetní techniky, pověřenec, zástupce pedagogů, vybraný pracovník ekonomického úseku a v případě obav ze zvládnutí implementace také specialista na oblast ochrany osobních údajů (ovšem pouze v postavení konzultanta). Sestavováním mini týmu se odehraje většinou zcela přirozeně a v řádu minut, více času pochopitelně zabere jeho proškolení ohledně pravidel posuzování operací zpracování a analýzy dokumentů.

JMENOVÁNÍ POVĚŘENCE (OVĚŘENÍ OZNÁMENÍ O JMENOVÁNÍ POVĚŘENCE) A JEHO ZAPOJENÍ DO PROCESU

Postup v rámci této činnosti je závislý na faktu, zda je prováděna revize implementace GDPR v dříve existující organizaci nebo zda je organizace čerstvě zřízena.

Organizace v roli OVM, které svou činnost právě zahajují, musí pochopitelně jmenovat pověřence pro ochranu osobních údajů a toho oznámit ÚOOÚ. Vzor oznámení je přílohou této práce (viz „Příloha 4 - Oznámení o jmenování pověřence“ na straně 185).

Byl-li již v minulosti pověřenec jmenován, je důrazně doporučeno prověřit tuto skutečnost ve spisové službě. Jsou-li o oznámení pověřence dozorovému úřadu pochybnosti nebo byl-li jmenován jiný pověřenec, je třeba toto oznámení neprodleně odeslat.

Po uvedení pověřence do funkce je třeba jej zapojit do dalších subprocesů implementace GDPR a zajistit mu přístup ke všem důležitým informacím.

KONZULTACE SE ZŘIZOVATELEM

Je vhodné, aby zřizovatelé škol co nejvíce kooperovali se svými příspěvkovými organizacemi (dále také „PO“) **a přispěli tak k co nejjednodušší aplikaci obecného nařízení.** Není přímo žádoucí, aby nešetrně zasahovali do procesu implementace (odpovědnost a pravomoci jsou na straně ředitelů škol), nicméně poskytnutím pomoci formou konzultací, vypracováním vzorů potřebné dokumentace nebo zprostředkováním

společných konstruktivně vedených setkání ředitelů PO lze proces revize implementace GDPR zrychlit, zjednodušit a zkvalitnit. **V případě, že zřizovatel poskytuje svým PO bezplatně pověřence (viz doporučení v kapitole 0), je přímo žádoucí některá pravidla a postupy sjednocovat.**

Ředitelům je doporučeno v rámci možností se zřizovatelem spolupracovat a synchronizovat přístup k problematice ochrany a zpracování osobních údajů.

V praxi však byly zachyceny velmi patologické přístupy k nařízení GDPR, a to zejména při nabízení služeb pověřence pro ochranu osobních údajů. Byly zaznamenány případy vypisování netransparentních výběrových řízení ze strany zřizovatelů na analýzy zpracování osobních údajů v PO nebo na externí předražené zajišťování služeb pověřence. Dokonce byla pozorována situace, kdy magistrátní zaměstnanci uzavírali dohody o provedení práce či dohody o pracovní činnosti s PO, prostřednictvím kterých služby pověřence nabízeli a na PO následně vyvíjeli nátlak, aby těchto služeb využívaly. Z objektivních důvodů není žádoucí toto přinejmenším neetické, spíše však nezákonné počínání dále konkretizovat a není to ani v zájmu naplňování cílů práce.

Pokud je vztah mezi zřizovatelem a PO narušen podobně závadnými skutečnostmi, je vhodné od takové spolupráce upustit a vybírat pouze nezávislé specialisty na provádění školení a zcela nezávislé pověřence pro ochranu osobních údajů.

SESTAVENÍ ROZPOČTU

S ohledem na sledované cíle práce nebude uvažována alternativa implementace GDPR formou outsourcingu. Sestavení rozpočtu tedy bude zahrnovat obvykle mírně zvýšené náklady na externí dodavatelskou firmu nebo na osobu provádějící správu a údržbu výpočetní techniky a dále náklady na pověřence, nejsou-li sjednány fixně. Rovněž je třeba počítat s výdaji na specialistu provádějícího školení zástupců vedení školy a následně i jednotlivých zaměstnanců, případně poskytujícího konzultace. V neposlední řadě je třeba myslet na možné výdaje spojené s nově přijímanými technickoorganizačními opatřeními. Jejich určení a provedení odhadu souvisejících nákladů, byť jen hrubého, bude realizovatelné obvykle až v závěrečných fázích celého procesu. I ve středně velkých školách však náklady na celý projekt dosahují obvykle jednotek tisíc Kč, zcela výjimečně se pohybují v řádu desítek tisíc.

STANOVENÍ OSOBY ODPOVĚDNÉ ZA ANALÝZU ZPRACOVÁNÍ

Analýza zpracování osobních údajů představuje v celém procesu implementace velmi náročnou část. Obvykle při této činnosti dochází k rozsáhlému sběru a vyhodnocování informací. Zpracování těchto dat a jejich ukládání do snadno editovatelné datové struktury pak vyžaduje nejen základní orientaci v problematice ochrany osobních údajů, ale rovněž zkušenosti při práci s tabulkovými procesory (např. Microsoft Excel nebo LibreOffice Calc), případně s jinými aplikacemi, bude-li zvolen sofistikovanější způsob sběru a zpracování informací (např. specializované aplikace, jako je Xeelo GDPR[214] nebo upravené databázové prostředí Microsoft Access s grafickou nadstavbou). O zpracovávání analýzy v analogové (listinné) podobě se pro následnou neudržitelnost aktuálnosti údajů bez vynaložení nepřiměřeného úsilí neuvažuje.

ROZDĚLENÍ ÚKOLŮ A NASTAVENÍ TERMÍNŮ

S ohledem na sledované cíle práce není uvažována alternativa implementace GDPR formou nákupu externí služby. Protipólem by pak bylo provedení implementace zcela svépomocí, tedy bez přispění specialisty a bez aktivního zapojení pověřence. K této variantě docházelo často ještě před účinností obecného nařízení, v době, kdy školy neměly jmenované pověřence. Dnes tuto alternativu rovněž nelze doporučit.

V úvahu tedy připadají dvě možnosti provedení implementace (revize implementace):

a) ve spolupráci s externím specialistou na problematiku ochrany osobních údajů

b) pod vedením pověřence

Optimální je vyvážená kombinace obou variant.

Ředitel školy musí v tomto kroku určit osoby odpovědné za jednotlivé fáze, tedy definovat osoby odpovědné za řízení a dokončení subprocesů, nebude-li vykonávat tyto úlohy sám. Jakkoliv se zdá být tento krok složitý, vzhledem ke schopnostem, kterými obvykle ředitelé škol disponují, neboť jsou pro jejich funkci nezbytné, se tato fáze odehraje v několika minutách.

Stanovení přísných termínů je nezbytné pro eliminaci zbytečného odkládání dokončování jednotlivých fází a k zamezení potenciálního zvyšování nákladů na externí konzultanty, jsou-li do procesu zapojeni. I v poměrně velké škole se dá při znalosti

[214] *Xeelo GDPR (http://www.xeelo.com/gdpr/)* [online]. [cit. 2021-01-11].

problematiky dokončit celý proces implementace za 2-3 týdny, proto by měly být lhůty na splnění dílčích úkolů co nejkratší.

4.10.2 Analýza zpracování osobních údajů

Tento subproces představuje časově nejnáročnější část v celém projektu. Skládá se ze sedmi vzájemně navazujících činností, bez kterých nelze následně provést posouzení souladu s obecným nařízením. Analytická tabulka sestavená v průběhu tohoto subprocesu bude později využita kromě GAP analýzy při sestavování záznamů o činnostech zpracování a při analýze rizik.

ANALÝZA VZOROVÝCH MATERIÁLŮ

Vzhledem k dostupnosti materiálů věnujících se analýze zpracování v prostředí škol (viz kapitola 3.9.2) je vhodné vlastní analýzu začít přípravou tabulky agend vycházející ze vzorových podkladů. Následně budou pouze vyřazeny agendy zpracování, které konkrétní škola neprovádí, nebo naopak doplněny agendy chybějící.

INFORMOVÁNÍ ZAMĚSTNANCŮ O VSTUPNÍ ANALÝZE ZPRACOVÁNÍ

Před sběrem informací pro analýzu zpracování je třeba všem zaměstnancům školy důkladně vysvětlit, jak zásadní roli budou při tomto sběru hrát, co tato činnost představuje a jaká data se při ní budou sbírat. Kvalitní komunikace vedení školy se všemi pedagogickými i nepedagogickými pracovníky je pro relevantnost získávaných údajů zcela zásadní. Je vhodné, aby byli zaměstnanci spraveni o základních náležitostech zpracování osobních údajů, což jim následně pomůže při popisu jimi prováděných zpracování.

IDENTIFIKACE AGEND ZPRACOVÁNÍ (DEFINICE ÚČELŮ)

Tato činnost se skládá z několika provázaných operací:

- příprava aktuálního seznamu všech zaměstnanců
- analýza pracovních náplní a organizačních či pracovních řádů
- výpis agend zpracování přidělených konkrétním pracovníkům (u nepedagogických pracovníků jde typicky o vedení spisové služby, vedení účetnictví, personalistiku, dodavatelsko-odběratelské vztahy; u pedagogických o vedení školní matriky, vedení školní družiny, agendy výchovného poradce apod.)
- výpis nezbytných přístupů k datům v jednotlivých agendách ze strany zaměstnanců

- sepsání účelů zpracování (účely představují obvykle operace zpracování v rámci větších agend – blíže se této problematice věnují podkapitoly s právními důvody zpracování v kapitole 4.1)
- příprava analytické tabulky nebo příslušné databáze pro sběr údajů

SBĚR INFORMACÍ O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

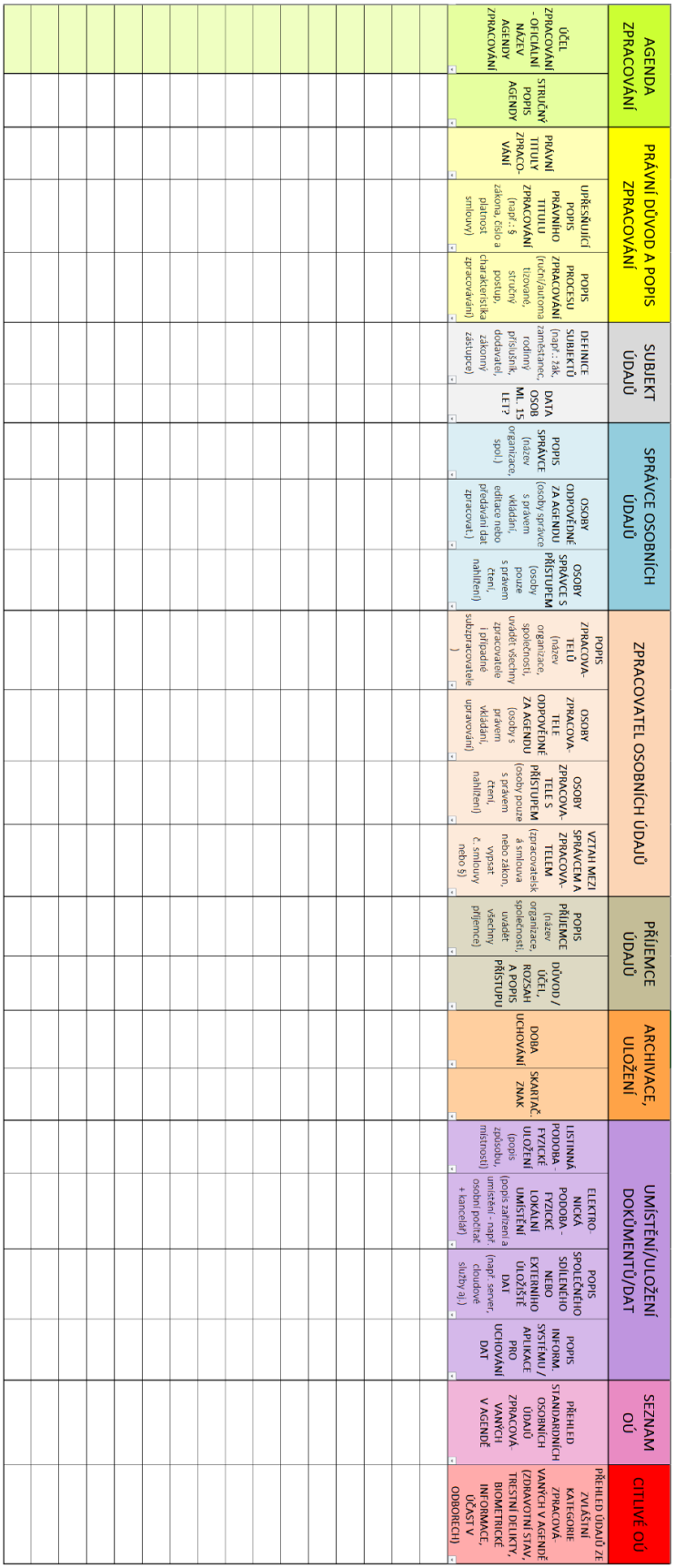
Tato dílčí fáze představuje jednu z nejdůležitějších činností nejen v tomto subprocesu, ale v celém projektu. Sebelepší příprava bude znehodnocena, pokud nebude sběr informací o zpracování proveden zodpovědně. Rovněž budou devalvovány téměř všechny navazující subprocesy, protože jsou většinou přímo závislé na kvalitě a úplnosti sběru informací o zpracování. Nelze posuzovat soulad s nařízením GDPR, pokud správce nemá odpovídající přehled o rozsahu jím zpracovávaných osobních údajů a způsobech, jakým jsou tyto zpracovávány.

V praxi bývá aplikována velmi efektivní a účinná metoda sběru dat a na základě empirického ověření z prakticky prováděných aplikací GDPR ji lze jen doporučit. Spočívá v umístění papírového sešitu na pracoviště každého zaměstnance školy, který při své práci provádí sběr osobních údajů nebo zasahuje do jejich zpracovávání. V prostředí školy tak činí přímo téměř každý zaměstnanec. Velmi okrajově do procesů zpracování zasahují obvykle školníci, uklízečky a kuchařky ve školních jídelnách. Ani tyto pracovníky však nelze při sběru informací opomenout. **Do tohoto sešitu pracovníci každý den zapisují, jaké operace zpracování provádějí, jaké typy údajů při něm využívají a jakých subjektů se týká.**

Důležitou roli při sběru informací o zpracování hraje případná existence odloučených pracovišť a specificky do analýzy zpracování zasahuje i doplňková činnost školy, která bývá běžně komerčního charakteru. Všechny tyto skutečnosti je třeba pečlivě zaznamenat, aby mohly být jednotlivé agendy zpracování správně popsány a posouzeny z pohledu legislativního souladu.

Je velmi nepravděpodobné, že by jednotliví pracovníci dokázali ve velmi krátkém čase popsat veškerá zpracování. K efektivnímu zachycení operací zpracování dochází právě v situacích, kdy takové zpracování reálně probíhá, a proto je doporučeno alokovat na tuto činnost 1-2 týdny při plném provozu školy a neprovádět sběr například v období prázdnin.

KOMPLETACE INFORMACÍ DO ORGANIZOVANÉ DATOVÉ STRUKTURY



Obrázek 19: Tabulka pro analýzu zpracování (bez části pro hodnocení rizik) (vlastní zpracování r. 2017)

Informace získané v předchozích krocích je třeba zkompletovat a uložit do přehledné strukturované podoby. Bez ohledu na způsob sběru, tedy zda probíhal elektronicky nebo v analogové podobě, je třeba informace setřídit podle účelů zpracování do připravené analytické tabulky (vzor viz Obrázek 19 a „Příloha 2 - Vzor tabulky pro analýzu zpracování osobních údajů“ na straně 182) nebo do speciálního SW.

Před dalším nakládáním s analytickou tabulkou je důrazně doporučeno konzultovat získané informace a postup finalizace analýzy zpracování se specialistou na problematiku ochrany osobních údajů nebo přímo zapojit pověřence.

DOPLNĚNÍ ATRIBUTŮ ZPRACOVÁNÍ (PRÁVNÍ DŮVODY)

Po zkompletování získaných dat je nezbytné do analytické tabulky doplnit k jednotlivým účelům a agendám zpracování také zákonný důvod zpracování. V případě jeho absence je konkrétní zpracování protiprávní. Přidělení právních titulů musí následně zkontrolovat pověřenec nebo najatý specialista. V rámci upřesnění právního základu pro zpracování je důrazně doporučeno uvádět příslušné právní předpisy ukládající danou povinnost, případně odkazovat na související smlouvy, souhlasy či balanční testy (vše v závislosti na použitém právním důvodu, blíže vysvětleno v kapitole 4.1).

Identifikované agendy je vhodné viditelně rozdělit na:

a) agendy provozní (typicky zpracování prováděná pří zajišťování provozu školy, při správě budov, majetku, při vedení spisové služby a v rámci pracovněprávních vztahů),

b) agendy přímo související s organizací vzdělávání (např. vedení školní matriky, správy dat žáků a agendy rozhodování ředitele školy)

c) agendy doplňkové činnosti školy

Jednotlivé záznamy musí být ještě doplněny o popis technických prostředků využitých na konkrétní zpracování, o odpovědné osoby, osoby s přístupem, o lokalitu a technické prostředky pro uložení dat a v neposlední řadě také doplněny o dobu uložení a skartační znak, jsou-li tyto informace k dispozici (viz položky v přiložené tabulce pro analýzu - „Příloha 2 - Vzor tabulky pro analýzu zpracování osobních údajů“ na straně 182).

IDENTIFIKACE ZPRACOVATELŮ A PŘÍJEMCŮ

Dalším nezbytným krokem je doplnění údajů o případných zpracovatelích zapojených do zpracování a příjemcích osobních údajů. U jednotlivých agend je třeba vyznačit, k jakým

osobním údajům mají přístup externí subjekty (příjemci osobních údajů), a tyto identifikovat. Analogicky musí být uvedeny identifikační údaje zpracovatelů propojené s konkrétní agendou nebo s procesem zpracování. Tyto informace budou mj. využity při revizi zpracovatelských smluv a dohod o mlčenlivosti.

4.10.3 GAP analýza

GAP analýza, tzv. analýza mezer, představuje subproces složený z velkého množství činností, při kterých se analyzuje diskrepance mezi aktuálním stavem a mezi očekávaným cílovým stavem. I když to není vyloučeno, je značně nepravděpodobné, že by nebyly nalezeny žádné nedostatky, tedy že by nebyla zaznamenána žádná „mezera“. Ony mezery zjištěné při kontrole veškerých prováděných zpracování i v existující dokumentaci vyjadřují odchýlení se od souladu s GDPR – od očekávaného stavu. Výstupem musí být kromě přehledu zjištěných nedostatků rovněž doporučení na jejich odstranění. Je důležité, aby GAP analýzu po celou dobu monitoroval ředitel, a to v úzké spolupráci s pověřencem, případně se specialistou na tuto problematiku. Pokud jsou výstupy z předchozího subprocesu sběru informací kvalitní, je možné celou GAP analýzu ve středně velké škole dokončit za 2-3 dny.

KONTROLA ZÁKONNOSTI ZPRACOVÁNÍ

V rámci této činnosti je třeba prověřit správnost přidělení právních důvodů k jednotlivým identifikovaným zpracováním, prověřit adekvátnost rozsahu zpracovávaných údajů a zkontrolovat dodržování veškerých povinností vyplývajících z platné legislativy, obzvláště pak těchto zásad obecného nařízení:

- „Zásada zákonnosti, korektnosti a transparentnosti“ (viz kapitola 3.5.1),
- „Zásada účelového omezení“ (viz kapitola 3.5.2),
- „Zásada minimalizace údajů“ (viz kapitola 3.5.3),
- „Zásada omezení uložení“ (viz kapitola 3.5.5).

INVENTURA SOUHLASŮ SE ZPRACOVÁNÍM

U všech zpracování, která byla při analýze navázána na právní důvod „souhlas se zpracováním osobních údajů“, je třeba zkontrolovat legitimitu jeho použití, zejména pak, neexistuje-li jiný aplikovatelný právní titul. Následně musí dojít k inventuře stávajících souhlasů a kontrole jejich náležitostí (blíže viz kapitola 4.1.1), na což naváže mj. subproces „Tvorba a úprava dokumentace“ (viz podkapitola 4.10.5).

INVENTURA BALANČNÍCH TESTŮ

Obdobně jako u souhlasů (předchozí činnost) je nezbytné prověřit zpracování prováděná na základě oprávněného zájmu správce, především pak existenci a náležitosti balančních testů (blíže k balančnímu testu a oprávněnému zájmu viz kapitoly 3.6.7 a 4.1.6).

ANALÝZA VZTAHŮ SE ZPRACOVATELI A PŘÍJEMCI

Tato činnost se zaměřuje na ověření vztahů s najatými zpracovateli a příjemci. Zahrnuje potvrzení existence a náležitostí zpracovatelských smluv se zpracovateli, dohod o mlčenlivosti či obdobných ujednání s příjemci informací (blíže se problematice věnuje kapitola 4.7), dále pak správnému zařazení některých příjemců mezi zpracovatele a v neposlední řadě také posouzení záruk, kteří tito zpracovatelé a příjemci poskytují. Příjemci, kteří nejsou v postavení zpracovatelů, musí být rovněž zavázáni k dodržování pravidel pro ochranu osobních údajů, k čemuž se v praxi používají různé smluvní doložky nebo samostatné NDA (dohody o mlčenlivosti).

KONTROLA ELEKTRONICKÝCH I FYZICKÝCH ÚLOŽIŠŤ DAT

Do této činnosti nespadá posuzování technické úrovně ICT prostředí, tomu se věnuje samostatný subproces v rámci auditu ICT. Kontrola úložišť se zaměřuje na obecné principy zabezpečení, na schopnost monitorování přístupu k osobním údajům a na nastavení pravidel pro dobu ukládání. Škola musí zajistit přiměřenou úroveň bezpečnosti elektronických úložišť, typicky serverů nebo datových síťových úložišť NAS (Network Attached Storage), musí být schopna evidovat, kdo má k těmto úložištím přístup, a musí mít přehled, jaká data se na nich nacházejí. Jakkoliv zní toto zcela logicky a analogii lze spatřovat ve fyzických spisovnách, kde je evidence uložených listin přirozená a obvykle dobře zpracovaná, je ve školách i obdobných organizacích zcela běžné, že ani zástupci vedení neznají rozsah a způsob ukládání elektronických dat, natož pak mechanismy jejich zálohování. Mnohdy těmito informacemi nedisponují ani žádní kmenoví zaměstnanci školy a zcela nezdokumentované postupy jsou pouze v hlavách externích správců výpočetní techniky (blíže tuto problematiku rozvádí subproces „Zjednodušený audit ICT“).

Ve vztahu k prostorám s uloženými listinnými dokumenty je třeba prověřit přiměřenost fyzického zabezpečení a úroveň organizačních opatření nastavujících pravidla pro vstup do těchto prostor, a to včetně odpovídající evidence vstupujících pro účely dodatečné identifikace osob při řešení bezpečnostních událostí a incidentů.

Problematika ukládání dat v elektronické i listinné podobě jsou dvě samostatné disciplíny, byť v mnoha ohledech úzce provázané. Jejich detailní deskripce by vydala na samostatnou práci. Pro účely navrhované GAP analýzy se doporučení omezují velmi obecně pouze na dvě výše uvedené oblasti. Je proto důrazně doporučeno svěřit kontrolu ukládání, zálohování, archivace a likvidace digitálních i analogových dat specialistům na danou oblast. Je žádoucí nastavit pro neviditelný svět „jedniček a nul“ a pro trochu hmatatelný ekosystém školní výpočetní techniky, který je však pro mnohé ředitele neprůhledným světem „black boxů“[215], jasná a kontrolovatelná pravidla.

KONTROLA INFORMAČNÍCH SYSTÉMŮ

Ani tato činnost se v rámci subprocesu „GAP analýza“ nesnaží konkurovat „ICT auditu“ popisovanému dále. Informačním systémem (IS) je pro zjednodušení v rámci GAP analýzy myšlen počítačový software či soubor programového vybavení tvořící určitý celek. Kontrolou IS se pro účely této činnosti rozumí ověření náležitostí nutných pro soulad s obecným nařízením, především pak vlastností nezbytných pro výkon práv subjektů. Není výjimkou, že starší IS nepodporují obecně potřebnou evidenci přístupu k datům, tedy že nelze zpětně ověřit, kdo a k jakým datům prostřednictvím příslušné aplikace přistupoval. Velmi často také absentuje funkcionalita omezení zpracování (blíže je právo na omezení zpracování vysvětleno v kapitole 3.6.5), tedy zablokování určitých údajů před další změnou nebo před výmazem. Dokonce byly v praxi zaznamenány velmi závažné nedostatky systémů, jako např. nemožnost provádět výmaz určitých informací (blíže k právu na výmaz viz kapitola 3.6.4).

KONTROLA ODPOVĚDNOSTI A ROLÍ VE ZPRACOVÁNÍ

Podstata této činnosti spočívá v kontrole rolí osob uvedených v analýze zpracování u jednotlivých agend, především pak v revizi role odpovědnostní. Pro každou agendu zpracování osobních údajů musí být znám okruh osob s přístupem k datům a osob s právem zpracování dat v dané agendě. Zcela zásadní je pak určení osoby odpovědné za agendu, přičemž její určení musí vyplývat z pracovního řádu, z pracovní náplně nebo pracovní smlouvy příslušného zaměstnance. Určení odpovědné osoby je podmínkou aplikovatelnosti některých technickoorganizačních opatření (viz subproces „Úprava procesů a přijetí opatření“ v podkapitole 4.10.7).

[215] ve smyslu elektronického zařízení se vstupy a výstupy, o kterém nikdo neví, jak funguje, z čeho se skládá a mnohdy není znám ani důvod, proč je v organizaci umístěno

REVIZE DOKUMENTACE

Ve škole existuje celá řada dokumentů souvisejících s problematikou ochrany a zpracování osobních údajů. Velká část byla prověřována při předchozích činnostech subprocesu „GAP analýza“, doposud však nebyla řešena kontrola plnění informační povinnosti vůči žákům, jejich zákonným zástupcům a rodinným příslušníkům a ani směrem k zaměstnancům školy. Kromě těchto písemností je třeba při revizi dokumentace zkontrolovat případné dodatky k pracovním smlouvám, protokoly o absolvování zaměstnaneckého školení v oblasti ochrany a zpracování osobních údajů, smlouvu s pověřencem pro ochranu osobních údajů a v neposlední řadě vnitřní předpis upravující specificky pravidla pro nakládání s osobními údaji.

ROZBOR ZÍSKANÝCH INFORMACÍ, POSOUZENÍ LEGISLATIVNÍHO SOULADU A TVORBA VÝSTUPU GAP ANALÝZY

V závěru GAP analýzy je třeba vypracovat přehled nedostatků a soubor doporučení na jejich odstranění. Nesmí chybět návrh nápravných opatření a revidovaná podoba kontrolovaných dokumentů s vyznačením doporučených změn. V případě zjištění závažnějších nedostatků nebo dokonce porušování právních předpisů je nutné ponechat subproces „GAP analýza“ otevřený, přistoupit k realizaci nápravných opatření, odstranit zjištěné nedostatky a opakovat některé činnosti GAP analýzy pro verifikaci nápravy.

4.10.4 Analýza rizik

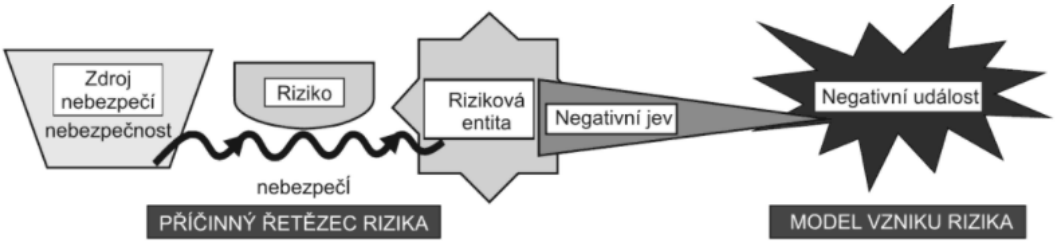
POSOUZENÍ AGEND Z HLEDISKA RIZIKA ZPRACOVÁNÍ

Analýza rizik je velmi komplexní disciplína vědního oboru rizikologie. Je nad akceptovatelný rozsah práce věnovat se analýze rizik detailněji, avšak vzhledem k již několikrát skloňovanému principu nařízení GDPR, tedy „přístupu založenému na odpovědnosti správce a **riziku** zpracování“, je nezbytné si z nauky o riziku vypůjčit alespoň definici pojmu „riziko“ a teoreticky stručně přiblížit postup jeho hodnocení.

Existuje velké množství pojmových vymezení, pro účely analýzy rizik zpracování osobních údajů se jako příhodné jeví znění *„Riziko je pravděpodobnost vzniku nestandardního stavu konkrétní entity v daném čase a prostoru“*.[216] Onou entitou je zdroj nebezpečí, který s určitou pravděpodobností představuje nositele rizika.

[216] Janíček, P., Marek, J. *Expertní inženýrství v systémovém pojetí*. Praha: Grada, 2013, s. 306. Expert (Grada).

Negativním událostem je nutné předcházet opatřeními nejen pro snížení následků rizika, ale především eliminací pravděpodobnosti vzniku nepříznivých stavů potlačením zdroje nebezpečí a redukcí cest přenosu nebezpečí řetězcem rizika. Model vniku rizika znázorňuje Obrázek 20.



Obrázek 20: Model vzniku rizika[217]

Posuzování rizik je velmi subjektivní záležitost. Proto je analytická tabulka („Příloha 2 - Vzor tabulky pro analýzu zpracování osobních údajů“ na straně 182) opatřena nejen částí pro výpočet rizika zpracování (viz Obrázek 21), ale v samostatném listu je připraven i vzorový číselník rizik (viz Obrázek 22), který osobám hodnotícím zpracování pomůže stanovit rizikovost agendy zpracování z pohledu dopadu na subjekt údajů.

VÝPOČET RIZIKA ZPRACOVÁNÍ				
ZPRACOVÁ-VANÉ OSOBNÍ ÚDAJE (dle listu "číselník")	DOPAD NA SUBJEKT ÚDAJŮ (dle listu "číselník")	POČET ZÁZNAMŮ S OSOBNÍMI ÚDAJI V AKTUÁLNÍ EVIDENCI (dle listu "číselník")	RIZIKO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	VYHODNO-CENÍ RIZIK, PŘIJATÁ OPATŘENÍ atp.
1	2	3	6	
3	2	1	6	
1	1	1	1	
2	2	2	8	
3	3	3	27	
4	4	4	64	
5	5	5	125	

Obrázek 21: Výpočet rizika zpracování (dopadu na subjekt) v analytické tabulce[218]

[217] Janíček, P., Marek, J. *Expertní inženýrství v systémovém pojetí*. Praha: Grada, 2013, s. 305. Expert (Grada).
[218] Vlastní zpracování (r. 2017, revize 2018 a 2021)

Zpracovávané osobní údaje

Body	Popis
1	základní kontaktní osobní údaje (zejména veřejně dostupné)
2	standarní osobní údaje, jejichž zvěřejnění nepředstavuje rizika pro subjekty
3	běžné osobní údaje s vyšším rizikem zneužití
4	agenda obsahuje rodné číslo nebo jeden údaj ze zvláštní kategorie
5	agenda obsahuje více údajů ze zvláštní kategorie

Dopad na subjekt údajů

Body	Popis
1	zpracování údajů včetně předání dat externímu zpracovateli neidentifikuje konkrétní subjekt údajů
2	zpracování údajů včetně předání dat externímu zpracovateli nemá vliv na subjekt údajů
3	zpracování údajů včetně předání dat externímu zpracovateli může mít za následek malá rizika pro subjekt údajů (zneužití pro marketingové účely, spam)
4	zpracování údajů včetně předání dat externímu zpracovateli může mít za následek střední rizika pro subjekt údajů (možnost zneužití údajů a zjištění informací o chování subjektu, jeho preferencích a denních činnostech)
5	zpracování údajů včetně předání dat externímu zpracovateli může mít za následek značná rizika pro subjekt údajů (zneužití údajů ze zvláštní kategorie pro vydírání nebo manipulaci se subjektem údajů, krádež identity)

Počet záznamů s osobními údaji v a Riziko zpracování osobních údajů

Body	Popis
1	do 100 údajů
2	101 - 1 000 údajů
3	1 001 - 5 000 údajů
4	5 001 - 10 000 údajů
5	více než 10 000 údajů

Rozmezí bodů	Riziko
1 - 2	zanedbatelné
3 - 12	nízké
13 - 36	střední - nutné přijmout organizační opatření
37 - 64	vysoké - nutné přijmout organizační a technická opatření
65 - 125	kritické - nutné přijmout organizační a technická opatření, zvážit konzultaci s ÚOOÚ a provedení DPIA, v případě kritické hodnoty 125 nutné provést DPIA

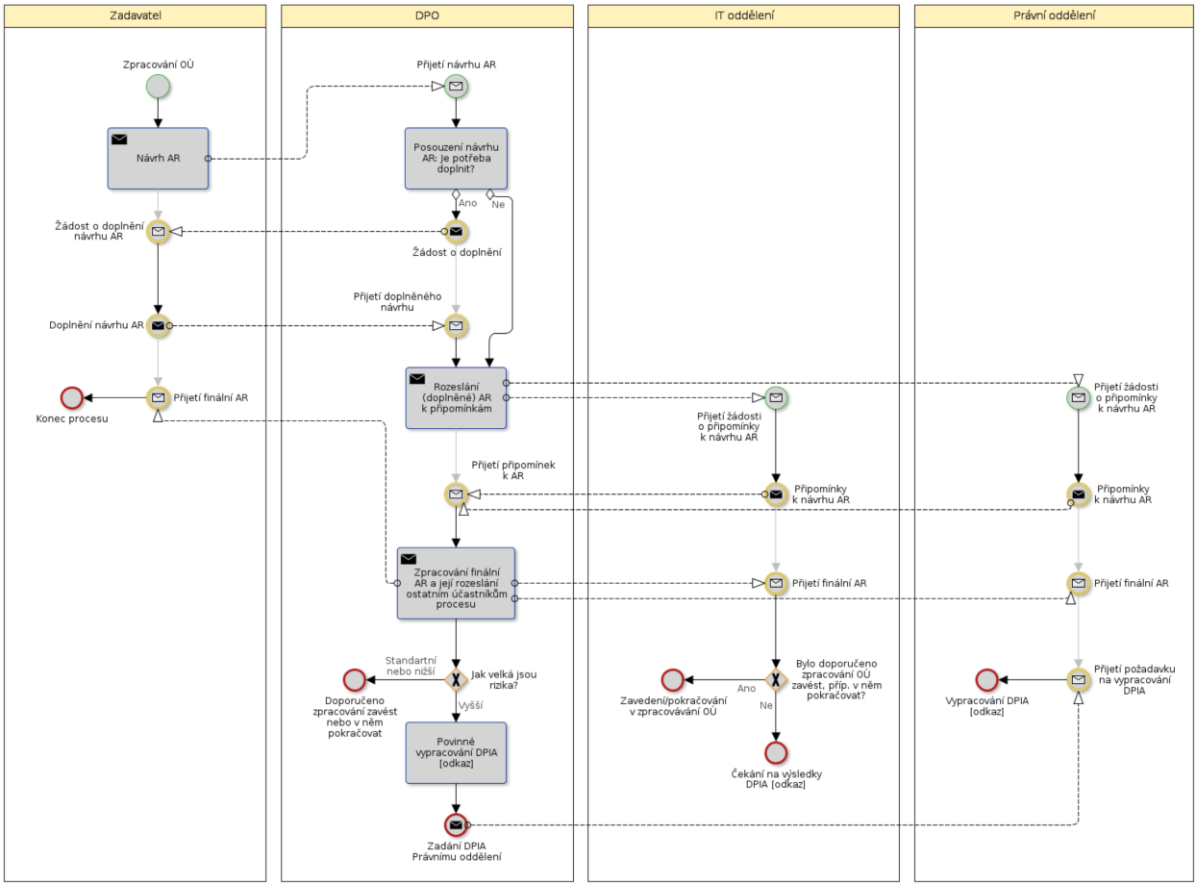
Obrázek 22: Číselník rizik zpracování v analytické tabulce[219]

VYHODNOCENÍ RIZIK A NÁVRH OPATŘENÍ

[219] Vlastní zpracování (r. 2017, revize 2018 a 2021)

Pro návrh nezbytných opatření je nutné výsledné hodnoty analýzy rizik zpracování (viz předchozí činnost „POSOUZENÍ JEDNOTLIVÝCH AGEND Z HLEDISKA RIZIKA ZPRACOVÁNÍ“ kombinovat ještě s rizikem prostředí, ve kterém zpracování probíhá, s úrovní fyzického zabezpečení a s přihlédnutím ke stavu techniky, která je na zpracování využita. Kombinací těchto aspektů je možné stanovit nejen riziko dopadu porušení zabezpečení na subjekt, které je předmětem výše popisované analýzy rizik, ale je možné odhadnout pravděpodobnost vzniku takového rizika.

Na následujícím obrázku (Obrázek 23) je procesní mapa analýzy rizik sestavená advokátní kanceláří PRK Partners, která zohledňuje i případnou nutnost provedení DPIA, tedy posouzení vlivu na ochranu osobních údajů (blíže k DPIA viz kapitola 3.7), která se v prostředí škol provádí ojediněle (zcela vyloučit ji nelze). Na návrhu AK PRK Partners je vidět zásadní zapojení pověřence do analýzy rizik, se kterým lze jen souhlasit.



Obrázek 23: Analýza rizik dle AK P/R/K Partners[220]

[220] Škubal, J., Loebl, Z. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

Na závěrečném vyhodnocení rizik se musí podílet vedení školy. Detailní znalost prostředí je klíčová a externí pracovníci touto znalostí obvykle nedisponují. Najatý specialista nebo externí pověřenec mají pouze poradní roli, teprve ve spolupráci s mini týmem provádějícím implementaci GDPR mohou s vedením školy identifikovaná rizika vyhodnotit a navrhnout opatření k jejich potlačení.

Navržená opatření lze kategorizovat na opatření *technická* (například nákup nové techniky, zvýšení fyzického zabezpečení, pořízení nového programového vybavení) a *organizační* (proškolení osob, úprava procesů zpracování, přijetí vnitřních předpisů, nastavení kontrolních mechanismů apod.). Vzájemnou kombinací jsou potom *technickoorganizační opatření* představující základní instrument v rukou ředitele školy k řízení rizik zpracování a k udržení trvalého souladu s obecným nařízením.

4.10.5 Tvorba a úprava dokumentace

Tento subproces přímo reaguje na výstup GAP analýzy.

PLNĚNÍ INFORMAČNÍ POVINNOSTI

Úlohu dokumentů sloužících pro naplnění práva subjektů na informace vyzdvihly již kapitoly 3.6.1 a 4.2.1. Jedná se o nejviditelnější písemnosti, kterými prezentuje správce osobních údajů svůj přístup k nakládání s osobními údaji. V rámci této činnosti musí být odstraněny nedostatky existujících informačních memorand odhalené GAP analýzou a zapracovány nové požadavky či vytvořena úplně nová poučení o zpracování pro kategorii subjektů, která nebyla původní dokumentací pokryta (např. specifické zásady zpracování uchazečů o zaměstnání nebo osob spolupracujících v rámci doplňkové činnosti).

V době pandemie Coronaviru SARS-Cov-2 je často třeba dopracovat velmi specifické informace o zpracování prováděném v souvislosti s testováním na onemocnění COVID-19, tedy pro účely „vytváření bezpečného a zdraví neohrožujícího pracovního prostředí“.

Při dobré znalosti agend zpracování, tedy v případě kvalitně provedené analýzy zpracování (subproces v kapitole 4.10.2), je finalizace informačního memoranda otázkou několika minut (vzor viz „Příloha 1 - Vzor informací pro subjekty“ na straně 180).

UZAVŘENÍ A REVIZE ZPRACOVATELSKÝCH SMLUV, UZAVŘENÍ NDA

Tato činnost reaguje na chybějící zpracovatelské smlouvy se zpracovateli vykonávajícími pro správce činnost klasifikovanou jako „zpracování osobních údajů“,

přičemž tato není aktuálně regulována smluvním ujednáním v souladu s obecným nařízením. Analogicky se řeší zpracovatelské smlouvy, které nemají požadované náležitosti.

Rovněž jsou činěny kroky pro rušení nadbytečně uzavřených zpracovatelských smluv s příjemci, kterým je nesprávně přisuzována role zpracovatelů, přestože fakticky pro správce žádná zpracování neprovádějí. S takovými příjemci musí být uzavřena dohoda o mlčenlivosti nebo musí být existující smluvní závazek doplněn o podobně fungující ujednání. Obdobně je třeba postupovat u nově identifikovaných příjemců, se kterými doposud žádné smluvní ujednání uzavřeno není.

Je-li škola v existujícím vztahu „společné správcovství“, nebo chystá-li se do takového režimu vstoupit, je nutné revidovat smluvní dokumenty, případně iniciovat jejich vznik, a v rámci této činnosti zajistit uzavření smlouvy o společném správcovství.

Případná nemožnost nebo neochota jedné ze stran uzavřít zpracovatelskou smlouvu, smlouvu o společném správcovství nebo NDA dohodu povede k ukončení spolupráce.

UZAVŘENÍ CHYBĚJÍCÍCH A RUŠENÍ NADBYTEČNÝCH SOUHLASŮ

Otázce souhlasů se zpracováním osobních údajů v prostředí škol se detailně věnovala kapitola 4.1.1, a není pochyb o jejich nadbytečném užívání. Zejména v prvních dvou letech po účinnosti obecného nařízení bylo často skloňováno tzv. „přesouhlasování“, což vysvětluje mj. i kapitola 4.9 komparujíc dvě verze metodických pomůcek od MŠMT.

V rámci této činnosti musí být odstraněny všechny nadbytečné souhlasy. U opodstatněných souhlasů musí být zkontrolovány potřebné náležitosti. Souhlasy, jejichž použití jako právního základu pro zpracování je legitimní, nicméně nesplňují povinné náležitosti, musí být revidovány a opětovně předloženy subjektům k posouzení s žádostí o potvrzení. Na subjekty nesmí být vyvíjen žádný nátlak k podpisu a škola musí apriori předpokládat, že souhlas neobdrží, tedy nezakládat na něm zpracování, které není svým významem pro školu marginální (blíže viz kapitola 4.1.1 a 4.9.2). Osobní údaje, jejichž zpracování bylo chybně prováděno pod právním důvodem „souhlas“, budou nyní zpracovávány na základě jiného legitimního právního důvodu nebo musí dojít k jejich výmazu. O tomto kroku je třeba subjekty transparentně informovat prostřednictvím zásad zpracování nebo poučení o zpracování.

Jak již však bylo vysvětleno v části práce věnující se zákonnosti zpracování, užití souhlasů ve školním prostředí je spíše okrajové. Administrativní náročnost s uzavíráním chybějících souhlasů se tudíž nepředpokládá.

TVORBA AKTUÁLNÍCH ZÁZNAMŮ O ČINNOSTECH ZPRACOVÁNÍ

O roli a důležitosti záznamů o činnostech zpracování hovořila zejména kapitola 3.5.7. Jako o důležitém zdroji informací pro tyto záznamy a o dvojí úloze analytické tabulky se pak zmiňovala kapitola 4.10.2.

Správně vyplněná analýza zpracování, tvořená dle přiloženého vzoru v (viz „Příloha 2 - Vzor tabulky pro analýzu zpracování osobních údajů“ na straně 182), je ideálním zdrojem podkladů pro záznamy o činnostech zpracování. Dokonce se těmito záznamy může po nepatrné úpravě přímo stát.

Vzhledem k tomu, že jsou záznamy o činnostech zpracování neveřejné, přestože je některé školy nevhodně publikují, je jejich struktura velmi volná. Obecné nařízení se věnuje pouze náležitostem. Jejich absence nepředstavuje pro školu bezprostřední riziko, je ovšem v zájmu pověřence, aby záznamy byly vyhotoveny kvalitně a aby jemu i vedení školy byly vždy přístupny.

AKTUALIZACE SMLUV V PRACOVNĚPRÁVNÍCH VZTAZÍCH

Český zákoník práce explicitně nestanovuje zaměstnancům běžných zaměstnavatelů podmínky mlčenlivosti aplikovatelné na problematiku obecného nařízení. V § 303 stanovuje speciální podmínky pouze ve vztahu k vybraným taxativně uvedeným veřejnoprávním zaměstnavatelům, resp. jejich zaměstnancům nastavuje přísnější podmínky.[221] Pro vyšší ochranu statutárního zástupce – ředitele školy, a pro zvýšení odpovědnosti zaměstnanců, se doporučuje alespoň s těmi zaměstnanci školy, kteří se na zpracování osobních údajů podílí, uzavřít dodatek k pracovní smlouvě. Tento zaváže pracovníky k dodržování přísnějších pravidel zejména ve vztahu ke zpracování osobních údajů a vyřeší tak značnou nedostatečnost a komplikovanou uplatnitelnost § 301, písm. d) zákoníku práce, který hovoří pouze obecně o povinnosti zaměstnance *„nejednat v rozporu s oprávněnými zájmy zaměstnavatele“*[222]. Vzor dodatku k pracovní smlouvě, který se snaží situaci řešit, je přílohou této práce (viz „Příloha 5 - Dodatek k pracovní smlouvě“ na straně 186).

4.10.6 Zjednodušený audit a revize ICT

Rychlost a úroveň elektronizace v prostředí škol se zvyšuje již mnoho let. Tlak na používání moderních technologií se zavedením distanční výuky jako jednoho z opatření

[221] Zákon č. 262/2006 Sb., zákoník práce. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2006, částka 84, číslo 262. § 303.
[222] *Ibid.,* § 301, písm. d).

v boji s COVID-19 působí jako akcelerant. Masivní rozvoj výpočetní techniky se tak dotkl i škol, které byly zvyklé využívat spíše zastaralejší technologie a tradiční způsoby komunikace či nakládání s informacemi. Obecně tak směřovaly zpracování informací do analogových forem. Praxe ovšem ukazuje, že ani inovátorský přístup k ICT vybavení nepredikuje automaticky, že bude mít škola tyto moderní technologie pod kontrolou.

Jelikož je přístup k této problematice velmi individuální a disproporce mezi schopnostmi a znalostmi kmenových zaměstnanců škol jsou značné, je školám důrazně doporučeno provedení základního auditu školou používaných informačních a komunikačních technologií, zjednodušeně inventuru a kontrolu veškerého hardwaru (HW) a softwaru (SW).

Obecným a empiricky ověřeným pravidlem je, že by tento mini audit neměli provádět sami stávající správci výpočetní techniky, a to bez ohledu na fakt, zda jsou interními zaměstnanci nebo externími subjekty. Ředitel školy by měl požadovat zcela nezávislé informace o stavu IT infrastruktury nezkreslené případnou snahou o maskování nedostatků ze strany osob aktuálně zajišťujících její správu.

INVENTURA HW A SW

Tato činnost nepředstavuje nic jiného než prostý soupis veškerého aktivně používaného nebo záložního HW(s potenciálem využití) a soupis veškerého aktuálně instalovaného nebo zakoupeného (s možností budoucího využití) programového vybavení, a to včetně hostovaných aplikací nebo pronajatého IT vybavení (vč. služeb Cloud computingu). HW vybavením se v této souvislosti rozumí i veškeré aktivní síťové prvky, IP kamery, záznamová zařízení, tiskárny, ale i trvale nezapojená zařízení, jako jsou externí harddisky nebo přenosné flashdisky, datové projektory, skenery apod. Při analýze používaného programového vybavení je třeba zahrnout i bezplatný software, který standardně v majetku organizace není, nelze tedy jeho existenci dovodit jinak než přímou znalostí prostředí.

Inventuru ICT nelze v tomto případě slučovat s postupy obvyklými při evidenci majetku, nicméně výpis z inventarizace pomůže při kontrole úplnosti sběru informací.

Smyslem inventury HW a SW je získání uceleného přehledu o prostředcích, které jsou využívány nebo jsou využitelné pro zpracovávání informací, a mohou být i potenciálním rizikem vedoucím až k porušení zabezpečení údajů.

Podklady získané při této činnosti jsou velmi cenným materiálem pro pověřence při šetření bezpečnostních událostí a incidentů, slouží řediteli školy při orientaci ve využívaných technologiích a pomáhají i při sestavování plánů obnovy výpočetní techniky (z hlediska

morálního zastarávání HW a SW), plánu obnovy v případě havárie (tzv. IT Disaster Recovery Plan) a v neposlední řadě při detailizování popisu procesů zpracování osobních údajů (zejména pro účely analýzy rizik).

Obrovským přínosem je tato dokumentace při nenadálé potřebě změny, nahrazení či dočasného zastoupení správce výpočetní techniky (např. při dlouhodobém onemocnění). Podklady slouží k rychlé orientaci v IT infrastruktuře a pomáhají eliminovat i tzv. vendor lock-in, tedy situace, kdy je prostředí vytvořeno natolik neprůhledně nebo kdy jsou použity natolik specifické komponenty či technologie, že je výměna dodavatele IT služeb prakticky znemožněna, případně je vykoupena vynaložením velkého úsilí a finančních nákladů. Na tuto problematiku navazují další činnosti v subprocesu „Zjednodušený audit ICT“, zejména pak ty zaměřující se na dokumentaci a obálkové účty.

OVĚŘENÍ MOŽNOSTI KONTROLY PŘÍSTUPU K INFORMACÍM

Obecné nařízení vyžaduje po správcích plnění celé řady povinností. Některým však nelze dostát, není-li správce schopen efektivně sledovat, kdo ke zpracovávaným údajům přistupuje. Obvykle není složité evidovat přístup k fyzicky uloženým informacím. Typicky se zavádí správa klíčů od prostor s uloženými listinnými dokumenty, instalují se EZS (elektronické zabezpečovací systémy) nebo je provozován kamerový systém se záznamem sledující vstup do spisoven, na sekretariát, do ředitelen apod.

Ekosystém elektronické komunikace je pro mnohé ředitele velkou neznámou, je proto vhodné konzultovat s IT specialisty zavedení přiměřeného monitoringu sítě a sledování provozu serverů a IS, minimálně pak systémů pro výkon spisové služby a vedení školní matriky. Získávané údaje nesmí být nešetrně preventivně vyhodnocovány, a využívány smí být právě v případě řešení bezpečnostních událostí a incidentů. Zaměstnanci musí být o existenci sledování informováni (blíže toto upřesňuje např. § 316 zákoníku práce[223]).

V rámci této činnosti je třeba ověřit, že je zavedené sledování provozu sítě a evidence přístupu k datům funkční, je v adekvátním rozsahu a je využitelné pro zamýšlené účely.

INVENTURA A EVIDENCE PŘÍSTUPŮ

Tato fáze představuje kontrolu uživatelských účtů určených pro vstup do prostředí operačních systémů služebně využívaných osobních počítačů (včetně notebooků) s cílem redukovat nepoužívané účty, nastavit omezená (jen nezbytně nutná) oprávnění pro využívání

[223] Zákon č. 262/2006 Sb., zákoník práce. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2006, částka 84, číslo 262, § 316, ost (2) a (3).

školou určených aplikací. Obdobně musí být provedena kontrola a evidence přístupů do IS, serverů, do cloudového prostředí apod. Evidence musí postihnout i přístupy na školní WiFi.

Specificky je třeba evidovat a kontrolovat tzv. privilegované účty, tedy uživatelské přístupy s vyšším oprávněním určené pro správce sítě, administrátory, ICT koordinátory a vybrané pokročilé uživatele s právy provádět údržbu, změny v nastavení, instalovat nové aplikace atp. Tyto účty by nikdy neměly být využívány při běžné práci, tedy ani správci výpočetní techniky či ICT koordinátoři, kteří administrátorské účty objektivně potřebují, by je neměli využívat při běžných uživatelských činnostech.

TVORBA A OVĚŘENÍ OBÁLKOVÝCH ÚČTŮ

Při správě ICT je nezbytná existence tzv. privilegovaných účtů, jak je upřesněno v předchozí činnosti, které jsou také předmětem evidence. Tyto účty jsou však přiděleny pouze vybraným osobám a slouží pro velmi specifické účely. V praxi byly velmi často zaznamenány zcela nesystémové přístupy k problematice privilegovaných účtů, kdy nikdo z vedení školy nedisponoval záložním administrátorským účtem s právy měnit ostatním interním i najatým externím správcům výpočetní techniky hesla k jejich účtům, tyto účty zakládat nebo rušit. To může způsobit velmi závažné komplikace v kritických situacích a zcela paralyzovat některé činnosti prováděné školou. Pokud zhavaruje server nebo informační systém a příslušný IT správce je z jakéhokoliv důvodu nedostupný nebo je nutné z jakýchkoliv důvodů provést nezávislou kontrolu systémů, kterou nesmí administrátoři ovlivnit, má škola bez odpovídajících přístupů zásadně limitované možnosti.

Pro tyto účely musí být zřízeny a pravidelně ověřovány tzv. obálkové účty, které jsou bezpečně uloženy buď v elektronické podobě ve specializovaných aplikacích umístěných mimo spravovanou techniku (např. KeePass s databází uloženou na flashdisku ředitele školy) nebo v listinné podobě v zapečetěné obálce ve školním trezoru (odtud pochází obecně používaný termín „obálkové účty“). Tyto účty musí disponovat nejvyššími možnými oprávněními a jejich použití musí být přísně regulováno a protokolováno. Až na naprosté výjimky řídí a kontroluje jejich využití ředitel školy.

BYOD A VYUŽÍVÁNÍ SLUŽEBNÍCH POČÍTAČŮ PRO SOUKROMÉ ÚČELY

Byť je tento bod vnořen hluboko do procesu implementace GDPR, je třeba mu věnovat velkou pozornost. Výpočetní technika může být v prostředí škol využívána zaměstnanci v těchto třech nejběžnějších režimech:

1) **Využívání svěřené výpočetní techniky (osobních nebo přenosných počítačů) výhradně pro pracovní účely** – jedná se o nejméně rizikový způsob využití. Pokud je počítač správně zabezpečen a je zajištěn rovněž dostatečný přehled o informacích na něm uložených, nepředstavuje to při řešení bezpečnostních událostí velké komplikace a jejich vzniku je navíc snazší předcházet. Nastavení pravidel pro legislativní soulad i kontrola jejich dodržování nevyžaduje zvýšené úsilí a v případě, že je na počítači instalován kvalitní antivirový program, pevný či polovodičový disk je šifrován (bezplatné šifrování je např. součástí operačního systému Microsoft Windows 10 Professional), uživatel je proškolen a jsou dodržována pravidla pro bezpečnou práci v online prostředí, je možné poměrně bez obav využívat tyto počítače i v domácích sítích například při práci na homeoffice nebo při organizaci distančního vzdělávání.
2) **Používání svěřené výpočetní techniky dle předchozího režimu rozšířeného o využívání pro soukromé účely** – takové použití je bez předchozího schválení zaměstnavatelem v rozporu s ustanovením §316 zákoníku práce[224]. Pokud takový způsob využívání pracovní výpočetní techniky zaměstnavatel umožní, zvyšuje riziko vzniku bezpečnostních událostí, nedodržuje-li zaměstnanec důsledně nastavená pravidla. Soukromé aktivity prováděné na služebních počítačích nikdy nesmí ohrozit uložená data, která zahrnují obvykle i osobní údaje žáků. Soubor podmínek pro takové použití musí být sestaven po konzultaci se specialistou na IT a zaměstnanec s nimi musí být prokazatelně seznámen.
3) **BYOD[225]** – v tomto režimu zaměstnavatel dovoluje zaměstnancům využívat pro pracovní účely vlastní soukromá zařízení. Jakkoliv se může zdát pro školu toto řešení výhodné, je zdrojem obrovského rizika pro zpracovávání osobních údajů a informací obecně. Kromě nezbytného povolení zaměstnavatele pro zpracovávání a ukládání školních dat na soukromých zařízeních a např. pro jejich zapojení do školní sítě je zcela klíčové vytvoření seznamu přísných pravidel a podmínek pro tento specifický režim. Zaměstnanec musí respektovat, že jeho zařízení nesmí být následně svěřeno předem neschválenému servisu výpočetní techniky, jsou-li na něm uložena školní data a tato nejdou například kvůli poruše bezpečně smazat před předáním k servisu. Využití servisu není akceptovatelné dokonce ani

[224] Zákon č. 262/2006 Sb., zákoník práce. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2006, částka 84, číslo 262, § 316, odst. (1).
[225] Bring Your Own Device = přines si vlastní zařízení

v případě, že je zařízení v záruce, což může představovat pro zaměstnance velkou komplikaci a zvýšené náklady při uplatňování výrobcem poskytované garance. Výjimkou je případ, kdy jsou data bezpečně zašifrována a riziko jejich kompromitace je eliminováno i při opravách zařízení v externím servisu. Zaměstnanec musí rovněž respektovat určitá omezení v používání neschválených aplikací na svém vlastním zařízení, pokud jej používá souběžně pro pracovní účely.

TVORBA DOKUMENTACE

V závěru tohoto subprocesu je třeba vypracovat souhrnnou dokumentaci k celému IT ekosystému. Tato musí obsahovat popis všech systémů, význam a konfiguraci jednotlivých zařízení, informace o uložených datech a provozovaných systémech, přehled přístupů a rovněž mapu sítě s výpisem síťových zařízení. Součástí musí být záložní dešifrovací klíče pro odemčení pevných a polovodičových disků z osobních počítačů pro případ nutnosti nouzové obnovy. Přiloženy musí být i informace o zálohování s popisem procesu obnovy.

Dokumentace musí být bezpečně uložena mimo výpočetní techniku, aby byla přístupná v listinné podobě i v případě nefunkčnosti všech systémů.

4.10.7 Úprava procesů a přijetí opatření

KONTROLA A NASTAVENÍ PRAVIDEL PRO PRÁCI S INFORMACEMI

V návaznosti na výstup subprocesu analýzy rizik a s ohledem na zjištění získaná auditem ICT musí být přijata opatření technického rázu pro odstranění všech nedostatků, případně, není-li to bez vynaložení nepřiměřeného usilí nebo bez vynaložení neadekvátních finančních prostředků možné, musí být přijata opatření pro eliminaci následků potenciálních rizik.

Typicky se může jednat o používání zastaralého programového vybavení, které vykonává ve škole nezastupitelnou funkci a nejsou k němu vydávány bezpečnostní aktualizace, přičemž jeho nahrazení by bylo velmi komplikované. Takový SW se dá pro snížení rizika zpracovávaných informací relativně snadno izolovat od dalších zařízení v síti.

Technická opatření jsou dále doplněna opatřeními organizačními, kterými ředitel školy nastavuje všechny procesy s cílem nenarušit efektivní chod školy, avšak nastavit akceptovatelnou hranici rizik zpracování informací. Příkladem budiž přiměřená pravidla pro zacházení s dokumenty, která nejsou postavena na nepodložených a nadužívaných pravidlech typu „politika čistého stolu“ nebo „kvalitní zámky na skříních v kabinetech“.

Pokud se někdo bude chtít k informacím dostat a překoná zámek na dveřích od kabinetu (ten musí být zcela logicky zabezpečen v případě nepřítomnosti zaměstnance školy), pravděpodobně ho nezastaví ani uzamčená skříň.

KONTROLA A NASTAVENÍ PRAVIDEL PRO SPISOVOU SLUŽBU

Téma spisová služba představuje materii přesahující zaměření a rozsah této práce. Detailní popis spisové služby by nebyl ani v zájmu naplnění cílů, proto se deskripce fáze „nastavení pravidel pro spisovou službu" v procesu implementace GDPR omezuje na obecná doporučení. Spisová služba však představuje prostředek pro zpracovávání velkého objemu dat ve školách a pravidla pro její povinné vedení jsou z pohledu legislativy, především pak zákona č. 499/2004 Sb., o archivnictví a spisové službě[226], velmi přísná. Rizika vyplývající z nedodržování povinností při výkonu spisové služby jsou nezanedbatelná. Přesto jde často o téma velmi podceňované.

Nastavení spisové služby by mělo zahrnovat mj. kroky:

- proškolení osob vedoucích spisovou službu (se zaměřením na specifika komunikace se subjekty při výkonu práv ve smyslu obecného nařízení),
- revizi spisového řádu (pravidla pro nakládání s písemnostmi v souladu s legislativou),
- revizi skartačního řádu (zejména z pohledu správného přidělování skartačních znaků a dodržování doby uložení písemností),
- kontrolu elektronické spisové služby na soulad se standardem NSESSS[227, 228] (tento standard mj. poskytuje garance legislativního souladu konkrétního programového vybavení určeného pro výkon spisové služby).
- kontrola přístupů jednotlivých uživatelů (ověření, zda přístupy ke spisům korespondují s pracovní náplní či organizačním nebo pracovním řádem; zamezení přístupu uživatelům, kteří jej při své práci nepotřebují),
- revize metodiky k vedení spisové služby (zejména se zaměřením na principy označování spisů a používání osobních údajů v poli „věc" – to by nemělo obsahovat zneužitelné informace nebo osobní údaje, není-li to vzhledem

[226] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2004, částka 173, číslo 499.
[227] Národní standard pro elektronické systémy spisové služby
[228] *Oznámení Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby VMV čá. 57/2017. Znění účinné od 4. července 2017*. In: . Praha: Ministerstvo vnitra, 2017, číslo 57.

k povaze spisu nezbytné; kontrola pravidel prioritizace komunikace – viz správné způsoby komunikace se subjekty v kapitole 4.3),

- kontrola zálohování a obnovitelnosti databází (vč. pravidel pro ukládání a likvidaci záloh dat spisové služby),
- kontrola používání certifikátů a časových razítek při vypravování elektronických písemností,
- kontrola formátu ukládaných písemností ve formátu PDF/A pomocí validátoru národního archivu (dostupný na adrese https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravni-puvodci/nastroje-narodniho-digitalniho-archivu[229]),
- kontrola napojení na základní registry (např. ověření pravidel pro ztotožňování subjektů dle evidence obyvatel),
- kontrola nastavených pravidel pro ukládání dokumentů při zachování právní váhy a domněnky pravosti (například instrukce k provádění autorizované konverze dokumentů z moci úřední v prostředí CzechPOINT@Office[230]),
- ověření funkcionalit „omezení zpracování“, „výmaz“ a vyhledávání informací o osobách přistupujících k informacím uloženým ve spisové službě,
- kontrola a nastavení pravidel pro nakládání s analogovými spisy (vynášení písemností ze spisovny, zejména pak odnášení mimo školu).

Zde uvedený seznam rozhodně není taxativním výčtem, jde o návodný soubor oblastí, kterými je třeba se při revizi výkonu spisové služby zabývat s ohledem na přesnost a bezpečnost zpracování.

SPECIFICKÁ ÚPRAVA PRAVIDEL PRO AGENDU INFORMAČNÍHO ZÁKONA A ZÁKONA O REGISTRU SMLUV

Je velkou chybou opomenout zdánlivě nesouvisející téma v podobě těchto dvou agend s GDPR. Obě zmíněné agendy jsou prostorem pro velmi častá pochybení. Škola musí nastavit jasná pravidla pro provádění anonymizace vyřizovaných žádostí subjektů o informace a musí postupovat analogicky při anonymizaci dokumentů zveřejňovaných v registru smluv (je-li škola povinným subjektem ve smyslu zákona o registru smluv).

[229] *Národní archiv: Nástroje národního digitálního archivu* [online]. [cit. 2021-02-13].
[230] *Czech POINT: Konverze z moci úřední* [online]. [cit. 2021-02-11].

Blíže se této problematice věnuje kapitola 4.8, která zmiňuje i metodiku MVČR a bezplatný anonymizační nástroj.

KONTROLA A NASTAVENÍ PRAVIDEL PRO PRÁCI S ICT

V rámci této činnosti musí dojít k vydání či úpravě vnitřního předpisu zejména v reakci na subproces „Zjednodušený audit a revize ICT“ (viz podkapitola 4.10.6).

Stručný a přehledný soupis nejdůležitějších pravidel by měl být zaměstnancům poskytnut samostatně. Jeho vzorový návrh je v kapitole 4.11.

Se zněním vnitřního předpisu musí být zaměstnanci nejen prokazatelně seznámeni, ale je vhodné mu věnovat podstatnou část školení. Čtenost směrnic a předpisů nebývá vysoká a k jejich vytváření nedochází pro účely jejich „existence“, ale pro účely jejich praktického dodržování. S tím souvisí i následné získávání zpětné vazby od zaměstnanců a určitá reflexe zaměstnavatele v případě námitek k nepřiměřeným nebo špatně argumentovaným ustanovením vnitřních předpisů. Jejich nedodržování může mít v reakci na direktivní přístup školy podobu pasivní rezistence. Předpis, který nelze v praxi dodržovat nebo v jeho dodržování nevidí zaměstnanci smysl, riziko zpracování objektivně nesníží.

NASTAVENÍ PRAVIDEL PRO VÝKON PRÁV SUBJEKTŮ

Jak bylo objasněno kapitolou 4.2 „Praktický výkon práv subjektů v prostředí veřejných škol“, je nutné vytvořit metodiku pro příjem žádostí subjektů a pro realizaci jejich požadavků. Kromě práva na informace, které bude a může naplňovat prakticky každý zaměstnanec školy, musí ředitel spolu s pověřencem vytvořit soubor instrukcí a návod, jakým způsobem bude se subjekty komunikováno, a to spolu se seznamem osob odpovědných za přijímání a vyřizování žádostí subjektů. S těmito pravidly je třeba zaměstnance seznámit, aby mohli subjekty odkazovat na publikované zásady zpracování a na konkrétní odpovědné osoby. Není výjimkou, že je pro účely výkonu práv subjektů a pro komunikaci se subjekty určen pouze pověřenec.

NASTAVENÍ PŘENESENÉ ODPOVĚDNOSTI

V rámci této činnosti jsou z dat získaných při analýze zpracování, a to v kontextu s povinnostmi zaměstnanců plynoucích z pracovních náplní, pracovních či organizačních řádů a pracovních smluv, vytvářeny **odpovědnostní role**. Každá agenda zpracování musí být přidělena osobě, která za ni bude v předem definovaných mezích odpovědná. Tímto krokem přenáší statutární zástupce – ředitel školy, odpovědnost na své podřízené. V případě, že by

tyto odpovědnosti nebyly definovány a nešly by nesporně dovodit z výše uvedených zdrojů, zůstala by odpovědnost na statutárním zástupci. Pro potřeby této práce je zde popisovaná problematika pracovního práva zjednodušena. Ředitelům škol je doporučeno tuto problematiku nepodceňovat a kombinací vnitřních předpisů, kvalitně sestavených pracovních náplní či obdobných závazných dokumentů a za podpory dodatků k pracovním smlouvám (viz „AKTUALIZACE SMLUVNÍCH DOKUMENTŮ V PRACOVNĚPRÁVNÍCH VZTAZÍCH“ v subprocesu „Tvorba a úprava dokumentace“ v podkapitole 4.10.5) prokazatelně zajistit odpovídající přesun odpovědnosti za agendy zpracování na pracovníky, kteří mají předmětnou oblast fakticky na starosti.

VYDÁNÍ VNITŘNÍHO PŘEDPISU A PŘIJETÍ OPATŘENÍ

Finální fází subprocesu „Úprava procesů a přijetí opatření“ je přijetí nápravných a technickoorganizačních opatření pokrývajících výše uvedené oblasti, tedy řešící buď zjištěné nedostatky nebo nastavující preventivní opatření. Následně musí dojít k oficiálnímu vydání vnitřních předpisů (synonymicky vnímáme pojmy „interní směrnice“, „interní předpis“, „vnitřní směrnice“ či „interní normativní akt“) upravujících povinnosti zaměstnanců i zaměstnavatele v souvislosti s regulací a kontrolou zpracování osobních údajů, výpočetní technikou a listinnými materiály. Po prokazatelném seznámení zaměstnanců s těmito předpisy dojde s nabytím jejich účinnosti v podstatě k dokončení revize implementace obecného nařízení, případně k jeho první aplikaci.

4.10.8 Post-implementační fáze

Název této podkapitoly napovídá, že je ve své podstatě počátkem samostatného procesu udržitelnosti souladu s obecným nařízením a nespadá již do procesu implementace. Post-implementační fáze vychází z premisy, že implementace, resp. její revize, byla zakončena subprocesem „Úprava procesů a přijetí opatření“ (viz předchozí podkapitola 4.10.7). Pokud nebude nastavena relativně jednoduchá zásada periodické kontroly vybraných oblastí, kontroly, které se může zhostit po dohodě pověřenec, hrozí do několika let opakování revize souladu s GDPR v obdobném rozsahu, jak jej popisuje kapitola 4.10. Budou-li však dodržována níže uvedená doporučení, dá se složitější a časově náročnější budoucí revizi aplikace obecného nařízení předejít.

KONTROLA SPLNĚNÍ ÚKOLŮ

Post-implementační fáze by měla být zahájena kontrolou splnění úkolů vyplývajících z předchozích činností implementačního procesu, především pak ověřením „zaplnění mezer“ odhalených GAP analýzou a narovnáním nedostatků v ICT prostředí a ve vedení spisové služby. Odstranění chyb a nedostatků je v prostředí škol mnohdy velmi banální a nevyžaduje obvykle ani nepřiměřené náklady.

Největším nedostatkem bývá špatná vzájemná komunikace. Celá řada chyb vzniká jen z nevědomosti, proto by součástí tohoto post-implementačního subprocesu mělo být zařazení problematiky ochrany osobních údajů na program pravidelných porad.

KONTROLA DOKUMENTACE A PUBLIKACE POVINNÝCH DOKUMENTŮ

Byť zní zcela logicky, že schválené finalizované povinné dokumenty, jmenovitě informace o zpracování, jsou zároveň odpovídajícím způsobem publikovány, praxe ukazuje, že je tato oblast velmi podceňována.

Při vzorových kontrolách webových stránek škol i listinných poučení určených pro osobní kontakt se subjektem byly zaznamenány závažné nedostatky. Fakticky existující aktuální dokumenty nebyly dány do oběhu nebo byly umístěny nepřehledně vedle původních verzí a subjekt na první pohled nerozezná, kterými se může a má řídit. Mnohdy nebyly zveřejněny aktuální kontakty na pověřence.

Kontrola nezbytných dokumentů a informací pro subjekty musí probíhat periodicky alespoň dvakrát ročně a ad hoc v případě zásahů do webových stránek školy.

Nelze zapomínat ani na distribuci aktuálních zásad zpracování vlastním zaměstnancům, které se standardně nezveřejňují a distribuují se výhradně interní cestou.

ÚPRAVA POSTUPŮ PRO BUDOUCÍ REVIZI

Sebelépe připravené projekty obvykle neprobíhají na 100 % dle představ jejich manažerů a autorů. Komplikace, chybné předpoklady a nedostatky jednotlivých subprocesů je důležité zaznamenat a promítnout je do procesní mapy, která bude využita při budoucím opakování procesu. Je nutné zachytit zpětnou vazbu od všech aktérů, tedy od pedagogických i nepedagogických zaměstnanců školy, od pověřence i případných externích specialistů, a to jakkoliv by byla tato zpětná vazba kritická. Jen tak se lze vyhnout opakování stejných chyb.

4.11 Nastavení povinností a proškolení zaměstnanců

Důležitost následně uvedených činností a kroků nesmí být snižována pro jejich nezařazení do samotné implementace. O níže popisovaném školení zaměstnanců zaměřeném na problematiku ochrany osobních údajů a kybernetickou bezpečnost se dá dokonce hovořit jako o nejdůležitějším organizačním opatření vůbec. Absence kvalitního školení zaměstnanců a absence jednoduchého a přehledného seznamu jejich povinností vede k patologickým přístupům v podobě extrémně nedostatečných nebo naopak zbytečně přehnaných reakcí na různé situace spojené se zpracováním či ochranou osobních údajů. Neméně závažné je přehlížení kybernetické bezpečnosti. Naprosto nevyhovující povědomí uživatelů o rizicích spojených s ICT technologiemi, především pak s online světem, se stávají příčinou bezpečnostních incidentů.

V rámci naplňování cílů této práce není prováděn výzkum příčin neuspokojivých znalostí uživatelů a nedodržování elementárních principů bezpečné práce s výpočetní technikou. Následující doporučení vycházejí čistě z empirických zjištění při provádění auditů ICT ve školských zařízeních a ze zpětné vazby od účastníků školení.

ŠKOLENÍ ZAMĚSTNANCŮ

Školení zaměstnanců školy musí být kvalitní, dobře strukturované, pravidelné a přiměřeně interaktivní. Je vhodné do něj zahrnout i externí spolupracující subjekty, například externí správce výpočetní techniky či externí účetní.

Po obsahové stránce musí v teoretické rovině přiblížit smysl a principy obecného nařízení, vysvětlit reálné dopady na fungování školy a na zcela praktických příkladech vysvětlit aplikaci GDPR při každodenně prováděných činnostech.

Problematika GDPR nesmí být při vzdělávání zaměstnanců bagatelizována, ale ani přeceňována na úkor jiných zcela nepokrytých témat, typicky kybernetické bezpečnosti, sociálních sítí a obecně internetu. Jmenovitě těmto třem příkladům by měla být věnována značná část školení. Na edukaci zaměstnanců školy ve správném nakládání s pracovní výpočetní technikou a v používání programového vybavení by měla navazovat samostatná část zaměřená na rizika číhající v online prostředí na děti. Ty jsou i za běžného fungování školy vedeny k využívání ICT, v obdobích nařízené distanční výuky jsou však k tomuto přímo nuceny. Velká část žáků bohužel nedisponuje potřebnými znalostmi o nástrahách internetu, a ne každý má doma rodiče erudované

v této problematice. Úloha školy je tedy neoddiskutovatelná a prvním krokem ke správnému vedení dětí zapojených do online výuky je ovládnutí kyberprostoru ze strany pedagogů.

TVORBA JEDNODUCHÉHO PŘEHLEDU POVINNOSTÍ A PRAVIDEL PRO ZAMĚSTNANCE

Při zpracování osobních údajů a obecně při práci s dokumenty a s výpočetní technikou by měli být zaměstnanci po nezbytném důkladném proškolení vybaveni stručným přehledem zásad práce s informacemi a s technikou. Ten by měl kromě specifických pravidel vyplývajících z konkrétní pracovní pozice obsahovat alespoň tyto body:

Zaměstnanec musí:

- pracovat pouze pod vlastní přidělenou uživatelskou identitou (nepoužívat společné účty nebo účty kolegů při vstupu do informačních systémů a dalších školních aplikací),
- udržovat svá hesla v tajnosti a dodržovat pravidla pro jejich tvoření a změnu,
- zabezpečit svůj uživatelský účet před použitím jinou osobou (v případě opuštění pracoviště, byť na velmi krátkou dobu, zajistit uzamčení prostředí operačního systému na osobním počítači nebo zabezpečit místnost před vstupem dalších osob),
- hlásit nadřízenému nebo pověřenému pracovníkovi neprodleně jakékoliv zjištění neoprávněného přístupu k údajům či podezření na narušení bezpečnosti,
- zajistit, aby k systému či údajům (v elektronické i listinné podobě) nemohla získat přístup neoprávněná osoba,
- odebírat výtisky se zneužitelnými informacemi nebo osobními údaji ze sdílených tiskáren ihned po vytištění nebo využívat funkci „bezpečný tisk“ (vytištění po zadání hesla),
- hlásit neprodleně svým nadřízeným pracovníkům, IT pracovníkům nebo pověřeným osobám veškeré chybové stavy, podezření na bezpečnostní události a incidenty (např. zneužití přístupových údajů, svěřených zdrojů a podezření na narušení bezpečnosti, ztrátu kontroly nad daty v listinné i elektronické podobě, poruchy systémů a techniky).

Zaměstnanec nesmí:

- připojovat neschválená zařízení do počítačů, související techniky ani do počítačové sítě (např. soukromé flashdisky, externí pevné disky, mobilní telefony),
- instalovat samostatně bez povolení nadřízeného aplikace nebo měnit nastavení již nainstalovaných aplikací,
- obcházet či vypínat bezpečnostní mechanismy, technická a administrativní opatření,
- spouštět aplikace, které zaměstnanci nebyly nainstalovány pro výkon jeho pracovní činnosti,
- používat pro pracovní účely nebo na výpočetní technice zaměstnavatele jinou než e-mailovou schránku přidělenou zaměstnavatelem (zejména soukromý e-mail),
- otevírat podezřelé přílohy elektronické pošty a podezřelé odkazy, a to i ve zprávách pocházejících z důvěryhodných adres,
- přistupovat na pracovním počítači na internetové zdroje nesouvisející s jeho pracovní náplní,
- sdělovat informace jiným než oprávněným příjemcům.

5 Závěr

O GDPR se v roce 2017 a v první polovině roku 2018 hovořilo doslova jako o revoluci v ochraně osobních údajů. I když se s blížící účinností GDPR začal používat vhodnější termín „evoluce“, celkový veřejně vnímaný obraz obecného nařízení se měnil pomalu. Úlohu sehrála média a zištné počínání některých „poradců“, kteří využili příležitosti a připravovali správce na příchod GDPR způsobem, který není při znalosti jeho principů, zásad a dopadu odůvodnitelný. Výsledkem byly nákladné a chybné implementace GDPR.

Toto zjištění, podpořené zdroji v teoretické části práce, naplňuje spolu s výstupem analýzy „Metodické pomůcky k aplikaci obecného nařízení o ochraně osobních údajů (GDPR)“ vydané v roce 2017 MŠMT dílčí cíl práce – hledání vysvětlení pro rozsáhlé chybné zavádění GDPR ve školství.

Komparací starší verze metodiky MŠMT s její opravenou verzí (z druhé poloviny roku 2019), byla potvrzena její významná úloha v defektním přístupu škol k implementaci GDPR. Nesprávná doporučení k aplikaci právních důvodů zpracování osobních údajů v prostředí škol akcelerovala generování enormního množství souhlasů, kterými školy zaplavily zákonné zástupce dětí. Návod od MŠMT byl díky autoritě ministerstva považován školami za důvěryhodný zdroj, což jeho škodlivost umocnilo, a nevalidní postupy nebyly řediteli škol příliš rozporovány. O novou verzi napravující nedostatky není bohužel zájem, což oddaluje soulad s GDPR ve školství.

Důvodem volby sekundárního cíle bylo hledání argumentů nezbytnosti revize dříve prováděných implementací GDPR. To posiluje i význam primárního cíle práce, který na tuto evidentní potřebu revize odpovídá chronologicky sestaveným návodem na zavádění GDPR.

Navržený proces implementace, resp. revize implementace, ve velké míře odráží zkušenosti autora práce získané při desítkách osobně prováděných aplikací GDPR v letech 2017 a 2018 a při následných revizích, školeních a při výkonu práv subjektů. Návrhy a doporučení vznikaly za přispění zpětné vazby od ředitelů škol a dalších pedagogických i nepedagogických pracovníků. Velkou pomocí byly konzultace s pověřenci působícími ve školství i v dalších institucích veřejné správy. Reflektovány byly rovněž názory pracovníků dozorového úřadu, kteří ochotně poskytovali rady na odborných seminářích a při osobních konzultacích.

Záměrem bylo také vysvětlit podstatu obecného nařízení. Nebude-li po přečtení této práce slovo „GDPR“ pro ředitele škol abstraktním pojmem, cíl lze považovat za splněný.

Samotné téma *„GDPR a jeho implementace v právnické osobě“* je velmi široké, a to i když je zkoumáno „pouze“ optikou školského zařízení. Na školská zařízení cílil i ucelený přehled pojmů, zásad, pravidel a souvisejících oblastí doplněný o ryze praktické příklady právě z prostředí škol. Smyslem bylo nastínit střet s realitou, se světem přetížených ředitelek a ředitelů škol, jejichž hlavním posláním je vzdělávat a připravovat děti na život, nikoliv studovat evropská nařízení a desítky souvisejících zákonů, s jejichž aplikací si neumí poradit ani velká ministerstva, jak dokazuje kvalita jimi produkovaných doporučení.

Práce proto čerpá z prakticky prováděných implementací a univerzálnost konstrukce zde prezentovaného procesu je průsečíkem rozdílných požadavků různě velkých a odlišně specializovaných škol. Základní školy orientované na sport nebo školy umělecké řeší mnohem častěji zpracování osobních údajů mimo běžné školní vzdělávací procesy. Organizují celou řadu uměleckých vystoupení nebo sportovních událostí, při kterých se vzájemně předávají osobní údaje žáků z jiných škol, ve větším rozsahu dochází k fotografování nebo natáčení videozáznamů a také k častějšímu využití reportážní činnosti při informování veřejnosti o pořádaných aktivitách a o úspěších žáků. Jakkoliv se navržený postup snaží pokrýt potřeby všech základních a základních uměleckých škol, je nutné jej ve spolupráci s odborníky na předmětnou problematiku či pověřencem pro ochranu osobních údajů optimalizovat pro konkrétní školu.

Obecným pravidlem pro zde popisovaný projekt, bez ohledu na velikost a zaměření školy, je přiměřenost přístupu při snaze o trvalé udržení legislativního souladu v oblasti ochrany a zpracování osobních údajů. Bagatelizování dopadu GDPR na školu nebo naopak zavádění přehnaně přísných organizačních opatření adresovaných zaměstnancům ve snaze ušetřit na opatřeních technických (typicky kvalitním programovém vybavení, antivirových a jiných bezpečnostních systémech) posiluje vynalézavost pracovníků při obcházení vnitřních předpisů nebo liknavost při jejich dodržování. Vyvážené nastavení technickoorganizačních opatření a adekvátní kontrola jejich dodržování je cestou k efektivnímu a nenákladnému souladu s obecným nařízením i dalšími právními předpisy.

Chová-li se škola dle zde uvedených doporučení k subjektům (žákům, jejich zákonným zástupcům i vlastním zaměstnancům) transparentně, respektuje-li jejich práva, zejména pak obecné právo na ochranu osobnosti, je velkou přidanou hodnotou správně zvládnuté implementace GDPR kladně vnímaný obraz školy ze strany veřejnosti.

Praktický přínos této práce lze spatřit i v konstrukci implementačního procesu GDPR. Ten nebyl navržen jako jednorázový plán aplikace GDPR ukončený v čase nic neřešícím

výstupem v podobě „papírového nárazníku“ maskujícího nedostatky v procesech zpracování před subjekty. Každý správce osobních údajů, školy nevyjímaje, by měl usilovat o udržení nastaveného standardu představujícího efektivní chod organizace při dodržování právních předpisů. Morfuje-li problematika obecného nařízení v zaprášený šanon umístěný v nejnižší polici ve spisovně nebo v zapomenutou složku na síťovém disku, dojde dříve či později k porušení zabezpečení osobních údajů a zásahu do práv a svobod subjektů, v prostředí škol bohužel těch nejohroženějších – dětí.

Smyslem revize souladu s obecným nařízením není jen instantní odstranění nedostatků, ale nastavení trvale udržitelného standardu ochrany osobních údajů. Úroveň zapojení a edukace všech aktérů se odrazí nejen na finančních a časových nákladech projektu, ale především na kvalitě jeho výstupu. Zaměstnanci školy, kteří nebudou participovat, omezí v budoucnu svou schopnost posoudit legislativní souladnost jejich počínání. Pravděpodobně nebudou v rozhodujících situacích s to vyhodnotit, že se odchýlili od školou nastavených pravidel, a mohou tak zbytečně ohrozit celý školní ekosystém tvořený velkým množstvím činností zpracování osobních údajů dětí. Úkolem pedagogů je s jejich údaji nakládat nad rámec zákonných norem, a to citlivě s ohledem na jejich rozumovou a emoční vyspělost, na možné důsledky pro jejich osobnost, na postavení v kolektivu, na vztahy se spolužáky a na celou řadu dalších atributů jejich osobního života.

S ohledem na problematiku ochrany osobnosti musí na žáky celá škola působit rovněž edukativně. Nesmí být zlehčován smysl právního rámce ochrany osobních údajů, byť by tak někteří pedagogové činili nevědomě pouze svou lhostejností k dodržování nastaveného standardu ochrany osobních údajů nebo naopak přehnaným neodůvodněným odmítáním některých činností s odkazem na nařízení GDPR. Typickým příkladem je fotografování dětí, kterému se tato práce detailně věnovala.

Mezi závěrečná doporučení určená ředitelům škol lze zařadit absolvování školení na problematiku GDPR a kybernetické bezpečnosti, provedení revize GDPR ve zde představeném rozsahu a vzdělávání zaměstnanců školy v předmětné problematice. Výsledkem bude pochopení GDPR a způsobilost k jeho jednoduché svépomocné aplikovatelnosti zajišťující ve vzájemné kombinaci soulad s právními předpisy při zachování zdravého rozumu a bez zátěže pro školní rozpočet.

I přes nutnost přepracování původního konceptu práce v reakci na pandemii COVID-19, která vyloučila empirický výzkum s osobní účastí ve školách a s tím související nemožnost praktického ověření navržených postupů, lze považovat cíle práce za splněné.

6 Použité zdroje

Odborná literatura:

DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. 2., aktualiz. a dopl. vyd. Praha: Grada, 2012. Expert (Grada). ISBN 978-80-247-4275-5.

GOVERNANCE, IT. *EU General Data Protection Regulation (GDPR), third edition: An Implementation and Compliance Guide: An Implementation and Compliance Guide*. 3rd edition. 978-1-78778-193-1: IT GOVERNANCE Publishing, 2019. ISBN 978-1-78778-192-4. Dostupné také z: https://books.google.cz/books?id=NDu8DwAAQBAJ

JANEČKOVÁ, Eva. *GDPR: řešení problémů v praxi škol*. Praha: Grada Publishing, 2020, 352 s. Právo pro praxi. ISBN 978-80-271-2579-1.

JANÍČEK, Přemysl a Jiří MAREK. *Expertní inženýrství v systémovém pojetí*. 1. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4127-7.

KŘÍŽ, Josef. *Řízení administrativních a správních procesů*. Vyd. 1. V Praze: Česká zemědělská univerzita, Provozně ekonomická fakulta, 2012. ISBN isbn978-80-213-2315-5.

NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0920-3.

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer, 2014. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-665-5.

NULÍČEK, Michal, Josef DONÁT, Bohuslav LICHNOVSKÝ, František NONNEMANN, , HABARTA a Kateřina KAŠPÁRKOVÁ. *Zákon o zpracování osobních údajů* [E-KNIHA]. Vydání první. Praha: Wolters Kluwer, 2019. Praktický komentář. ISBN 978-80-7598-468-5.

NULÍČEK, Michal, Michal NONNEMANN, Bohuslav LICHNOVSKÝ a Jan TOMÍČEK. *Obecné nařízení o ochraně osobních údajů (GDPR): Praktický komentář* [Systém ASPI]. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISSN 2336-517X. Dostupné také z: ASPI_ID KO32016R0679CZ

PATTYNOVÁ, Jana, Lenka SUCHÁNKOVÁ, Jiří ČERNÝ a Miroslav RŮŽIČKA. *Obecné nařízení o ochraně osobních údajů (GDPR): Zákon o zpracování osobních údajů : komentář*. 2. aktualizované a doplněné vydání. Praha: Leges, 2019, 752 s. Komentátor. ISBN 978-80-7502-396-4.

POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, 656 s. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7598-045-8.

POSPÍŠIL, , LANGÁŠEK, ŠIMÍČEK a WAGNEROVÁ A KOL. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer Česká republika, 2012. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7357-750-6.

PUŠKINOVÁ, Monika a Filip RIGEL. *Správní řízení v praxi škol a školských zařízení* [PDF]. Vydání první. Praha: Wolters Kluwer, 2016. Řízení školy (Wolters Kluwer). ISBN 978-80-7552-123-1.

RYCHETSKÝ, Pavel, Tomáš LANGÁŠEK, Tomáš HERC a Petr MLSNA. *Ústava České republiky: Ústavní zákon o bezpečnosti České republiky : komentář*. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-809-3.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-720-7.

VOIGT, Paul a Axel BUSSCHE. *The EU General Data Protection Regulation (GDPR): A Practical Guide* [eBook]. Cham: Springer International Publishing AG, 2017. ISBN 978-3-319-57959-7.

Odborné články:

GELLERT, R. Why the GDPR risk-based approach is about compliance risk, and why it's not a bad thing. *Jusletter IT* [online]. Weblaw AG, 2017, (), 7 [cit. 2021-02-07]. ISSN 1664848X. Dostupné z: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85037661777&partnerID=40&md5=262d401b274f681e8d54122d583e62de

MOLE, Ariane, Debora STELLA a Ruth BOARDMAN. *DPO in Europe* [online]. Bird & Bird [cit. 2021-02-18]. Dostupné z: https://www.twobirds.com/en/news/articles/2005/dpo-in-europe

PATTYNOVÁ, Jana. Šest měsíců s GDPR: novinky a průběh kontrol dozorového orgánu. *PRÁVNÍ PROSTOR* [online]. ATLAS CONSULTING spol. s.r.o. [cit. 2021-02-26]. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/sest-mesicu-s-gdpr-novinky-a-prubeh-kontrol-dozoroveho-organu

Internetové zdroje:

Article 29 working party: Opinions and recommendations. *Directorate-General for Justice and Consumers European Commission* [online]. [cit. 29.12.2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

CORMACK, Andrew. Is the Subject Access Right Now Too Great a Threat to Privacy?. *European Data Protection Law Review* [online]. 2016, **2**(1) [cit. 2021-01-05]. Dostupné z: https://doi.org/10.21552/EDPL/2016/1/5

Czech POINT: Konverze z moci úřední [online]. [cit. 2021-02-11]. Dostupné z: Národní archiv: Nástroje národního digitálního archivu [online]. [cit. 2021-02-13]. Dostupné z: https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravni-puvodci/nastroje-narodniho-digitalniho-archivu

ČESKÁ TELEVIZE. *Největší mýty o GDPR. Kvůli špatné přípravě je nová ochrana dat zahalena nejasnostmi* [online]. [cit. 2021-03-06]. Dostupné z: https://ct24.ceskatelevize.cz/ekonomika/2489812-nejvetsi-myty-o-gdpr-kvuli-spatne-priprave-je-nova-ochrana-dat-zahalena

Evropský sbor pro ochranu osobních údajů. *The European Data Protection Board (EDPB)* [online]. [cit. 20. 02. 2021]. Dostupné z: https://edpb.europa.eu/

GESELLSCHAFT FÜR DATENSCHUTZ UND DATENSICHERHEIT. *35. DAFTA am 17. und 18. November 2011 in Köln: Einheitliches Datenschutzrecht in Europa durch Verordnung* [online]. [cit. 2020-11-18]. Dostupné z: https://www.gdd.de/seminare/dafta/vergangene-daftaen/35-dafta-und-30-rdv-forum

Google Workspace for Education (https://edu.google.com/products/workspace-for-education/education-fundamentals) [online]. [cit. 2021-03-07]. Dostupné z: https://edu.google.com/products/workspace-for-education/education-fundamentals/

Hospodářská komora České republiky: GDPR – REVOLUCE V OCHRANĚ OSOBNÍCH ÚDAJŮ [online]. [cit. 2.2.2021].

JEŽEK, Mojmír. *Nový český zákon o zpracování osobních údajů z roku 2019: Adaptační český zákon k evropskému nařízení GDPR č. 110/2019 Sb. účinný od 24.4.2019* [online]. [cit. 2021-01-09]. Dostupné z: http://www.ecovislegal.cz/gdpr-a-ochrana-osobnich-udaju/novy-cesky-zakon-o-zpracovani-osobnich-udaju-2/

K povinnosti jmenovat pověřence vybranými městskými a krajskými organizacemi: Úřad pro ochranu osobních údajů zveřejňuje podrobnější informace týkající se rozsahu povinnosti jmenovat pověřence některými městskými či krajskými organizacemi. [online]. [cit. 18. 02. 2021]. Dostupné z: https://www.uoou.cz/k-povinnosti-jmenovat-poverence-vybranymi-mestskymi-a-krajskymi-organizacemi/d-31980

Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) - 2019 (stránka s informacemi o souboru www.msmt.cz/file/51137) [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021]. Dostupné z: www.msmt.cz/file/51137

Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů (GDPR) (aktuální web) [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2019 [cit. 01.03.2021]. Dostupné z: https://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane?highlightWords=metodick%C3%A1+pom%C5%AFcka

Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství - 2017 (stránka s informacemi o soboru www.msmt.cz/file/44592) [online]. Praha: Ministerstvo školství, mládeže a tělovýchovy, 2017 [cit. 01.03.2021]. Dostupné z: www.msmt.cz/file/44592

Metodický návod k aplikaci zákona o registru smluv. In: . Praha: Ministerstvo vnitra, 2021, ročník 2021, 1.11. Dostupné také z: https://www.mvcr.cz/clanek/registr-smluv.aspx?q=Y2hudW09OQ%3d%3d

Microsoft: Office 365 Education (https://www.microsoft.com/cs-cz/education/products/office) [online]. [cit. 2021-03-07]. Dostupné z: https://www.microsoft.com/cs-cz/education/products/office

Ministerstvo vnitra: Registru smluv [online]. [cit. 2021-03-02]. Dostupné z: https://smlouvy.gov.cz/

Ministerstvo vnitra: Nástroj pro anonymizaci dokumentů [online]. [cit. 2021-01-10]. Dostupné z: https://anonymizace.gov.cz/crossroad/

Ministerstvo vnitra: Systémové analýzy [online]. [cit. 2020-12-28]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/web-systemove-analyzy-systemove-analyzy.aspx

Ministerstvo vnitra: Systémové analýzy - Příloha č. 6 Systémové analýzy působnosti obcí z hlediska obecného nařízení o ochraně osobních údajů [online]. [cit. 01.03.2021]. Dostupné z: https://www.mvcr.cz/gdpr/soubor/priloha-c-6-podrizene-organizace.aspx

Národní archiv: Nástroje národního digitálního archivu [online]. [cit. 2021-02-13]. Dostupné z: https://www.nacr.cz/verejnost/2-predarchivni-pece/verejnopravni-puvodci/nastroje-narodniho-digitalniho-archivu

Nejdůležitější pojmy: Definice pojmů jsou obsaženy v článku 4 odst. 1 obecného nařízení. *Úřad pro ochranu osobních údajů* [online]. [cit. 2021-01-30]. Dostupné z: https://www.uoou.cz/3-nejd-lezit-jsi-pojmy/d-27293

Pokyny evropského Sboru (EDPB). *Úřad pro ochranu osobních údajů* [online]. Dostupné také z: https://www.uoou.cz/pracovni-skupina-wp29-k-gdpr/ds-4728/archiv=0&p1=1020

Seznam držitelů datových schránek (https://www.mojedatovaschranka.cz/sds/) [online]. [cit. 2021-03-09].

Správa základních registrů : Informační systém základních registrů (ISZR) [online]. [cit. 2021-01-03]. Dostupné z: https://www.szrcr.cz/cs/informacni-system-zakladnich-registru

THE EUROPEAN COURT OF HUMAN RIGHTS. *JUDGMENT - CASE OF ROTARU v. ROMANIA: (Application no. 28341/95)* [online]. 2000. STRASBOURG [cit. 01.03.2021]. Dostupné z: https://hudoc.echr.coe.int/eng?i=001-61853#{%22fulltext%22:[%2228341/95%22],%22itemid%22:[%22001-58586%22]}

The Internet Archive [JUN 11 2018]: http://web.archive.org/web/20180611091356/http://www.msmt.cz/file/44592/ [online]. [cit. 2021-03-03]. Dostupné z: http://web.archive.org/web/20180611091356/http://www.msmt.cz/file/44592/

The Internet Archive [MAY 17 2018]: http://web.archive.org/web/20180517095207/http:/www.msmt.cz/file/44592 [online]. [cit. 2021-03-03]. Dostupné z: http://web.archive.org/web/20180517095207/http:/www.msmt.cz/file/44592

The Internet Archive [SEP 22 2019]: http://web.archive.org/web/20190922122703/http:/www.msmt.cz/file/44592 [online]. [cit. 2021-03-03]. Dostupné z: http://web.archive.org/web/20190922122703/http:/www.msmt.cz/file/44592

Úřad pro ochranu osobních údajů: GDPR (obecné nařízení) [online]. [cit. 2021-01-13]. Dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

Úřad pro ochranu osobních údajů: Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA): Úřad pro ochranu osobních údajů [online]. [cit. 06. 03. 2021]. Dostupné z: https://www.uoou.cz/navod-k-posouzeni-vlivu-na-ochranu-osobnich-udaju-u-navrhu-pravnich-predpisu-dpia/ds-5344

Úřad pro ochranu osobních údajů: Ukončené kontroly [online]. [cit. 2021-03-11]. Dostupné z: https://www.uoou.cz/ukoncene-kontroly/ds-5649/archiv=0&p1=1649

Úřad pro ochranu osobních údajů: Základní informace [online]. [cit. 2021-01-13]. Dostupné z: https://www.uoou.cz/zakladni-informace/ds-5855/p1=5855

Xeelo GDPR (http://www.xeelo.com/gdpr/) [online]. [cit. 2021-01-11]. Dostupné z: http://www.xeelo.com/gdpr/

Základní příručka k ochraně: Sankce, pokuty. *Úřad pro ochranu osobních údajů* [online]. [cit. 2021-01-21]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287/p1=4744

Legislativní dokumenty:

Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. In: *EUR-Lex*. Brussels: Official Journal of the European Union, ročník 2020, L 114/7, číslo 518. Dostupné také z: http://data.europa.eu/eli/reco/2020/518/oj

Důvodová zpráva k vládnímu návrhu zákona o ochraně osobních údajů a o změně některých zákonů: Sněmovní tisk 374/0. In: . Praha, 1999, ročník 1999, číslo 374. Dostupné také z: https://www.psp.cz/sqw/text/tiskt.sqw?o=3&ct=374&ct1=0

EVROPSKÁ UNIE. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (kodifikované znění). In: *EUR-Lex*. Štrasburk, 2015, Úř. věst. L 241/1, 2015/1535. Dostupné také z: http://data.europa.eu/eli/dir/2015/1535/oj

Guidelines 05/2020 on consent under Regulation 2016/679: Version 1.1. *European Data Protection Board Guidlines* [online]. 2020, **2020**(05), 33 [cit. 2021-02-19]. Dostupné z: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů): (Text s významem pro EHP). In: . THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016. Dostupné také z: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014: o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES. In: *EUR-Lex*. Brusel, 2014, Úř. věst. L 257/73, číslo 910. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32014R0910

Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) COM/2017/010 final - 2017/03 (COD) [NÁVRH - NAŘÍZENÍ NENÍ ZATÍM SCHVÁLENO]. In: *EUR-Lex*. Brussels, 2017, ročník 2017. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM:2017:10:FIN

Obecné pokyny Evropského sboru pro ochranu osobních údajů: Obecné pokyny. *The European Data Protection Board (EDPB)* [online]. [cit. 07.01.2021]. Dostupné z: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_cs

Oznámení Ministerstva vnitra, kterým se zveřejňuje národní standard pro elektronické systémy spisové služby VMV čá. 57/2017. Znění účinné od 4. července 2017. In: . Praha: Ministerstvo vnitra, 2017, číslo 57. ISSN ISSN1211-1244. Dostupné také z: https://www.mvcr.cz/clanek/narodni-standard-pro-elektronicke-systemy-spisove-sluzby.aspx

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). In: *Official Journal of the European Union*. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016, L 119/1. Dostupné také z: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. In: *Sbírka mezinárodních smluv*. 2001, částka 52, 115/2001 Sb. m. s. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3571

Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV. In: *EUR-Lex*. Brusel, 2016, L 119/89, 2016/680. Dostupné také z: http://data.europa.eu/eli/dir/2016/680/oj

Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. In: *EUR-Lex*. Brusel, 2016, L 119/132, 2016/681. Dostupné také z: http://data.europa.eu/eli/dir/2016/681/oj

Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *EUR-Lex*. Lucemburk, 1995, Úř. věst. L 281, Svazek 015, 95/46/ES. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:31995L0046

The direct effect of European law: Summaries of EU legislation. In: *EUR-Lex*. Publications Office, 2015. Dostupné také z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14547

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů*. Praha, 1992, ročník 1993, částka 1, číslo 2. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426

Vyhláška č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2005, částka 11, číslo 48. ISSN ISSN1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=4609

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů*. Praha, 2020, ročník 2000, částka 32, číslo 101. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/

Zákon č. 106/1999 Sb. , o svobodném přístupu k informacím. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 1999, částka 39, číslo 106. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=4930

Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, ročník 2019, částka 47, číslo 110. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=63839

Zákon č. 111/2009 Sb., o základních registrech. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2009, částka 33, číslo 111. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5470

Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. In: *Sbírka zákonů*. Praha: Ministerstvo vnitra, 2019, částka 47, číslo 111. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=63840

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). In: *Sbírka zákonů České republiky*. Praha: Ministerstvo vnitra, 2000, ročník 2000, částka 39, číslo 133. ISSN ISSN1211-1244. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3427

Ostatní zdroje:

ČESKÝ ROZHLAS. *GDPR je naprostá blbost, tvrdí naštvaný Václav Klaus ml.: Nařízení o ochraně osobních údajů GDPR začne platit už v pátek 25. května. Předseda sněmovního školského výboru a poslanec ODS Václav Klaus mladší celé nařízení striktně odmítá a dokonce ho považuje za „buzeraci" státu.* [online]. [cit. 2021-01-30]. Dostupné z: https://plus.rozhlas.cz/gdpr-je-naprosta-blbost-tvrdi-nastvany-vaclav-klaus-ml-7226006

MATOUŠOVÁ, Miroslava. *Konzultace pro pověřence pro ochranu osobních údajů, Praha 9. října 2018: Pověřenci pro ochranu osobních údajů ve veřejných subjektech v ČR na startovní čáře*. Praha: Úřad pro ochranu osobních údajů, 2018.

REDAKCE IROZHLAS.CZ. *Začalo platit GDPR. "Česko stále nemá potřebnou legislativu", varuje Jourová.* [online]. [cit. 2020-12-30]. Dostupné z: http://irozhl.as/2Lg

Rozhovor moderátora ČT Tomáše Drahoňovského s Veronikou Křížovou v pořadu 90' ČT24: Nová ochrana osobních dat v praxi, část na téma "Děti a mladiství na internetu" [online]. 25. 5. 2018. Dostupné také z: https://www.ceskatelevize.cz/ivysilani/11412378947-90-ct24/218411058130525/obsah/622542-gdpr-v-praxi-veronika-krizova-a-jaromir-prusa

ŠKUBAL, Jaroslav a Zbyněk LOEBL. *PRK Partners: ASPI Navigátor - Obecné nařízení o ochraně osobních údajů (GDPR)*. Wolter Kluwer, 2020.

7 Přílohy

Příloha 1 - Vzor informací pro subjekty

Zásady zpracování osobních údajů a informace o pořizování fotografií a audio-video záznamů

platné ode dne *xx. xx. 20xx*

Správcem vašich osobních údajů je:

Název školy
se sídlem: *Ulice 123, 456 78, Město*
IČO: *98765432*
právní forma: příspěvková organizace
zřizovaná: *Název zřizovatele*
zastoupená: *Titul. Jméno Příjmení* (ředitelem)

kontaktní údaje:
e-mail: *email@domenaskoly.cz*
telefon: *+420 987 654 321*
(dále také „Správce“ nebo „Škola“)

Pověřencem pro ochranu osobních údajů správce jmenoval:

Titul. Jméno Příjmení

kontaktní údaje:
e-mail: *email@domenaskoly.cz*
telefon: *+420 987 654 321*
(dále jen „Pověřenec“)

Škola Vás tímto v souladu s platnými právními předpisy, zejména se zákonem č. 110/2019 Sb., o zpracování osobních údajů a s nařízením Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, známým jako nařízení GDPR, informuje, že pro **splnění zákonné povinnosti, při plnění úkolů prováděných ve veřejném zájmu nebo při výkonu veřejné moci, pro ochranu životně důležitých zájmů nebo pro účely oprávněného zájmu** („Právní důvod zpracování“) bude zpracovávat osobní údaje (dále také „OÚ“) **žáků** v rozsahu: jméno, příjmení, rodné číslo, datum narození, místo narození, národnost, státní občanství, místo pobytu, druh pobytu, telefonní číslo, e-mailová adresa, zdravotní pojišťovna, obrazový záznam prostřednictvím kamerového systému a případně další údaje, které uvedete v dokumentu „Přihláška do *ZŠ/ZUŠ*“. Dále pak osobní údaje ze zvláštní kategorie (citlivé OÚ): údaje o zdravotním stavu, vyjádření PPP[1] nebo SPC[2].

U zákonných zástupců žáků evidujeme kromě většiny výše uvedených základních OÚ povolání a pracoviště (z důvodu zajištění civilní ochrany) a případné informace o svěření dítěte do péče.

Škola Vás informuje, že OÚ budou zpracovávány pro účely splnění všech zákonných povinností vyplývajících z provozu školy, z organizace základního *.../uměleckého* vzdělávání, vedení školní matriky, pro organizaci soutěží, exkurzí, seminářů, workshopů, uměleckých vystoupení, zajištění bezpečnosti v budově školy, provozování kamerového systému se záznamem v budovách školy s cílem zajistit nezbytnou ochranu osob a práv žáků i návštěvníků školy ve veřejných a společných prostorách („Účel“), a to na základě legitimního Právního důvodu zpracování. Osobní údaje budou zpracovávány automatizovaně i ručně, a to při dodržení všech bezpečnostních zásad pro správu a zpracování osobních údajů.

Škola Vás informuje, že bude pořizovat a používat fotografie, časově omezené videozáznamy a audiozáznamy během práce s žáky školy bez souhlasu se zpracováním osobních údajů a bez souhlasu se zachycením podobizny člověka v souladu s § 89, zákona č. 89/2012 Sb. (občanský zákoník) a v souladu s nařízením GDPR formou reportážních fotografií nebo záznamů zejména v těchto případech:

- pro umělecké účely, akademickou nebo literární činnost;
- dokumentace kulturních a soutěžních vystoupení;
- přiměřeným způsobem pro nekomerční propagační účely a prezentaci školy a školského zařízení;
- publikování poznatků v odborných publikacích;
- dokumentace pracovních (pedagogických) přístupů v případě nemožnosti demonstrovat práci s žáky přímo;
- zpracování vědeckých, diplomových a podobných prací.

[1] Pedagogicko-psychologická poradna
[2] Speciálně pedagogické centrum

V jiných případech bude vždy Správcem osobních údajů (v souladu s § 84–90 zákona č. 89/2012 Sb., občanský zákoník) ještě před započetím zpracování fotografií a audio/video záznamů vyžadován souhlas subjektu údajů se zpracováním takových údajů a před případným započetím fotografování nebo nahrávání audio/video záznamu bude vyžadován souhlas fyzické osoby se zachycením podobizny člověka či s pořízením záznamu.

Žák nebo zákonný zástupce má právo požadovat bezodkladné zablokování či odstranění informace, fotografie či záznamu týkajícího se jeho osoby, který zveřejňovat nechce. Platí to i o fotografiích či záznamech žáka bez uvedení jména v rámci obecné dokumentace školních akcí a úspěchů.

Škola Vás jakožto zákonné zástupce dětí (žáků) informuje, že bude zveřejňovat výsledky školních prací a úspěchů Vašeho syna/dcery (jde zejména o výkresy, literární díla, umělecké a reportážní fotografie a audio/video záznamy) v rámci školních a mimoškolních soutěží, výstav a přehlídek, a to formou uvedení jména, příjmení, věku, ukázky práce, umístění v soutěži, fotografie a popř. videozáznamu v propagačních materiálech školy, ve výroční zprávě školy, na internetových stránkách školy, na nástěnkách umístěných ve škole, na veřejných výstavách pořádaných školou a v publikacích, zabývajících se činností školy.

Škola Vás informuje o tom, že na základě vzájemné spolupráci a platné smlouvy bude předávat osobní údaje SRPDŠ[3] v rozsahu: jméno, příjmení, adresa, kontaktní údaje, rodné číslo (pro jednoznačnou identifikaci žáka), číslo bankovního účtu a údaje o zákonných zástupcích.

Škola Vás informuje o tom, že mezi další příjemce OÚ patří externí poskytovatelé služeb, s nimiž má Škola uzavřenou smlouvu o zpracování osobních údajů (dále jen „Zpracovatel“) a poskytují dostatečné záruky ochrany Vašich osobních údajů, dále příjemci, kterým je umožněn přístup z důvodu plnění zákonných povinností a příjemci, kteří nejsou zpracovateli, ale zprostředkovávající či vykonávající pro školu služby nebo dodávky zboží a mají se školou uzavřenou dohodu o mlčenlivosti.

Škola Vás informuje, že nebude předávat bez Vašeho výslovného souhlasu Vaše OÚ příjemcům nebo zpracovatelům do třetí země mimo Evropský hospodářský prostor (EHP), pokud mají horší pravidla pro nakládání s osobními údaji než Česká republika.

Škola Vás informuje, že OÚ uloží po dobu nezbytně nutnou pro splnění daného účelu zpracování, a že máte právo požadovat přístup k OÚ, jejich opravu nebo výmaz, omezení zpracování nebo vznést námitku proti zpracování a právo na přenositelnost OÚ (tj. získat od Správce OÚ ve strukturovaném, běžně používaném a strojově čitelném formátu a předat je jinému správci), že lze podat stížnost u Úřadu pro ochranu osobních údajů („Dozorový úřad“), že poskytnutí OÚ není povinností a že nedochází k automatickému rozhodování ani k profilování. Škola sděluje, že máte právo získat potvrzení, zda OÚ jsou či nejsou zpracovávány. Pravidla se řídí nařízením GDPR a související legislativou.

Škola sděluje, že máte právo na výmaz OÚ:

- jestliže OÚ již nejsou potřebné pro Účel;
- jestliže odvoláte souhlas a neexistuje další právní důvod pro zpracování;
- jestliže vznesete námitky proti zpracovávání OÚ na základě oprávněného zájmu Správce nebo námitky proti automatizovanému individuálnímu rozhodování nebo proti profilování;
- jestliže OÚ byly zpracovávány protiprávně;
- jestliže OÚ musí být vymazány ke splnění právní povinnosti;
- jestliže OÚ byly shromážděny v souvislosti s nabídkou služeb informační společnosti.

Škola výslovně upozorňuje, že máte právo vznést kdykoli námitku proti zpracování OÚ, které se Vás týkají, a byly získány ke splnění úkolu ve veřejném zájmu nebo na základě oprávněného zájmu Správce, včetně profilování. Dále máte právo vznést kdykoli námitku proti zpracování OÚ, které se vás týkají, pro marketingové účely. Škola upozorňuje, že máte právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování včetně profilování, které pro vás má právní účinky nebo se vás významně dotýká, ledaže je to nezbytné k uzavření nebo plnění smlouvy nebo je založeno na výslovném souhlasu.

Škola sděluje, že při porušení zabezpečení OÚ, které bude představovat riziko zásahu do Vašich práv a svobody, oznámí toto porušení bez zbytečného odkladu Dozorovému úřadu a v případě vysokého rizika budete školou neprodleně informováni.

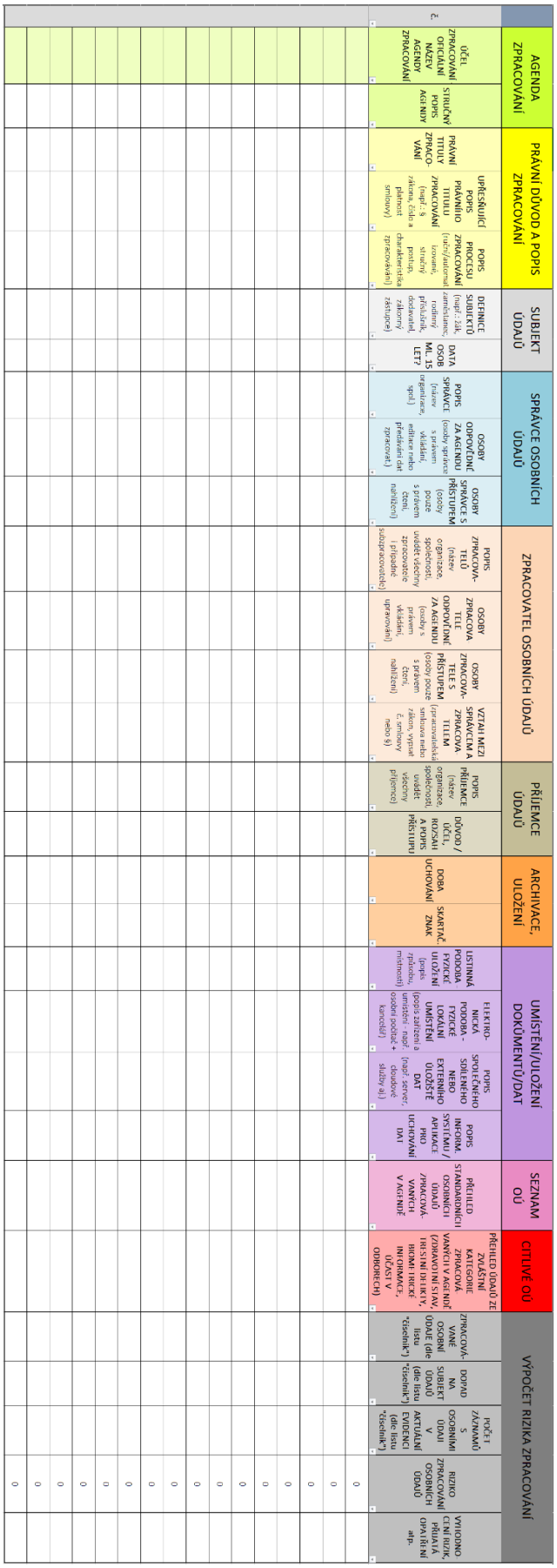
[3] Sdružení rodičů, přátel a dětí školy

231

[231] Vlastní zpracování (r. 2018, revize 2019, 2021)

Příloha 2 - Vzor tabulky pro analýzu zpracování osobních údajů

List AGENDY ZPRACOVÁNÍ:



List ČÍSELNÍK:

Zpracovávané osobní údaje

Body	Popis
1	základní kontaktní osobní údaje (zejména veřejně dostupné)
2	standarní osobní údaje, jejichž zvěřejnění nepředstavuje rizika pro subjekty
3	běžné osobní údaje s vyšším rizikem zneužití
4	agenda obsahuje rodné číslo nebo jeden údaj ze zvláštní kategorie
5	agenda obsahuje více údajů ze zvláštní kategorie

Dopad na subjekt údajů

Body	Popis
1	zpracování údajů včetně předání dat externímu zpracovateli neidentifikuje konkrétní subjekt údajů
2	zpracování údajů včetně předání dat externímu zpracovateli nemá vliv na subjekt údajů
3	zpracování údajů včetně předání dat externímu zpracovateli může mít za následek malá rizika pro subjekt údajů (zneužití pro marketingové účely, spam)
4	zpracování údajů včetně předání dat externímu zpracovateli může mít za následek střední rizika pro subjekt údajů (možnost zneužití údajů a zjištění informací o chování subjektu, jeho preferencích a denních činnostech)
5	zpracování údajů včetně předání dat externímu zpracovateli může mít za následek značná rizika pro subjekt údajů (zneužití údajů ze zvláštní kategorie pro vydírání nebo manipulaci se subjektem údajů, krádež identity)

Počet záznamů s osobními údaji v a Riziko zpracování osobních údajů

Body	Popis
1	do 100 údajů
2	101 - 1 000 údajů
3	1 001 - 5 000 údajů
4	5 001 - 10 000 údajů
5	více než 10 000 údajů

Rozmezí bodů	Riziko
1 - 2	zanedbatelné
3 - 12	nízké
13 - 36	střední - nutné přijmout organizační opatření
37 - 64	vysoké - nutné přijmout organizační a technická opatření
65 - 125	kritické - nutné přijmout organizační a technická opatření, zvážit konzultaci s ÚOOÚ a provedení DPIA, v případě kritické hodnoty 125 nutné provést DPIA

[232]

[232] Vlastní zpracování (r. 2017, revize 2018 a 2021)

Příloha 3 - Vzor souhlasu se zpracováním osobních údajů

Souhlas fyzické osoby se zpracováním osobních údajů č. ……..

Já, níže podepsaná/ý
Jméno, příjmení: ……..
Datum narození: ……
Bydliště: ……..,
(„Subjekt údajů“)

Název školy
se sídlem: *Ulice 123, 456 78, Město*
IČO: *98765432*
právní forma: příspěvková organizace
zřizovaná: *Název zřizovatele*
zastoupená: *Titul. Jméno Příjmení* (ředitelem)
kontaktní údaje:
e-mail: *email@domenaskoly.cz*
telefon: *+420 987 654 321*
(dále také „Správce“ nebo „Škola“)

v souladu s platnými právními předpisy, zejména se se zákonem č. 110/2019 Sb., o zpracování osobních údajů a s nařízením Evropského parlamentu a Rady EU 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, známým jako nařízení GDPR **tímto výslovně prohlašuji,**

že souhlasím se zpracováním těchto osobních údajů v rozsahu *jméno, příjmení, datum narození, bydliště, telefonní číslo, e-mailová adresa* …… (dále jen OÚ) pro účel …….. …… (dále jen „Účel“) a prohlašuji, že mě Správce informoval, že OÚ jsou zpracovávány pro Účel, a to na základě mého souhlasu, který je právním titulem zpracování OÚ. Dále pak souhlasím s tím, aby OÚ byly poskytnuty dalším příjemcům OÚ, mezi které patří zpracovatelé, s nimiž má Správce uzavřenu smlouvu o zpracování osobních údajů („Zpracovatel“) a poskytují dostatečné záruky ochrany OÚ, a příjemcům, kteří nejsou pro Správce Zpracovatelé, ale zprostředkovávající či vykonávající pro Správce služby nebo dodávky zboží a mají se Správcem uzavřenou dohodu o mlčenlivosti. Dále beru na vědomí, že budou OÚ poskytnuty příjemcům, kterým je umožněn přístup z důvodu plnění zákonných povinností.

Správce mě informoval, že:

a) mám právo požadovat informaci, kterým zpracovatelům byly mé OÚ poskytnuty v rámci jejich dalšího zpracování a další informace s tím související a že nebude předávat bez mého výslovného souhlasu mé OÚ příjemcům nebo zpracovatelům do třetí země mimo Evropský hospodářský prostor (EHP), pokud mají horší pravidla pro nakládání s osobními údaji než Česká republika.

b) osobní údaje uloží po dobu …… *roku/roků/let / do doby odvolání souhlasu se zpracováním* u Správce.

c) mám právo požadovat od Správce přístup k OÚ, jejich opravu nebo výmaz popř. omezení zpracování nebo vznést námitku proti zpracování a právo na přenositelnost OÚ (tj. získat od Správce OÚ, které jsem mu poskytl, ve strukturovaném, běžně používaném a strojově čitelném formátu a předat je jinému správci), že **souhlas mohu kdykoliv odvolat osobně v sídle Správce nebo zasláním žádosti prokazující totožnost Subjektu údajů na adresu sídla nebo kontaktní e-mail Správce**, že mohu podat stížnost u Úřadu na ochranu osobních údajů, že poskytnutí OÚ není povinností a že nedochází k profilování OÚ. Správce mi sdělil, že mám právo získat od Správce potvrzení, zda OÚ jsou či nejsou zpracovávány.

d) mám právo na výmaz OÚ, jestliže odvolám souhlas a neexistuje další právní důvod pro zpracování.

Tento souhlas činím svobodně, pro konkrétní účel a v konkrétním rozsahu, při plné informovanosti o všech mých právech ze zpracování osobních údajů plynoucích.

V …… dne ……

……..……..…
Podpis Subjektu

233

[233] Vlastní zpracování (r. 2018, revize 2019 a 2021)

Příloha 4 - Oznámení o jmenování pověřence

Název školy
Ulice 123, 456 78, Město, datová schránka, kontaktní údaje

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7
Datová schránka: qkbaa2n

V …… dne ……

OZNÁMENÍ O JMENOVÁNÍ POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

Název školy, zastoupená ***Titul. Jméno Příjmení*** (ředitelem), jako správcem osobních údajů tímto dle článku 37, odst. 7 nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES **sděluje dozorovému úřadu kontaktní údaje na pověřence pro ochranu osobních údajů**.

Pověřencem pro ochranu osobních údajů byl/a jmenován/a:
Titul. Jméno Příjmení
tel.: ……
e-mail: ……..

Svůj souhlas se jmenováním do funkce pověřence pro osobních údajů vyjadřuje *Titul. Jméno Příjmení* podpisem této listiny.

…… ……

Titul. Jméno Příjmení
Pověřenec pro ochranu osobních údajů

Název školy
zastoupená *Titul. Jméno Příjmení*

234

[234] Vlastní zpracování (r. 2018)

Příloha 5 - Dodatek k pracovní smlouvě

Dodatek k pracovní smlouvě č. *xxx* ze dne: *01. 01. 2020*

(dále jen „**Dodatek**“)

Zaměstnavatel:
Název školy
se sídlem: *Ulice 123, 456 78, Město*
IČO: *98765432*
zastoupená: *Titul. Jméno Příjmení* (ředitelem)
(dále jen „**Zaměstnavatel**“) a

Zaměstnanec:
Titul. Jméno Příjmení
datum narození: *01. 01. 2000*
bydliště: *Ulice 123, 456 78, Město*
(dále jen „**Zaměstnanec**“)

I. Předmět dodatku

Zaměstnavatel a Zaměstnanec tímto dodatkem ujednali následující rozšíření vzájemných práv a povinností ve vztahu k ochraně fyzických osob v souvislosti se zpracováním osobních údajů.

II. Mlčenlivost a ochrana osobních údajů

1. Zaměstnanec je povinen při výkonu práce zajistit, aby nedošlo k neoprávněnému zpřístupnění osobních údajů třetím osobám a dodržovat mlčenlivost o osobních údajích všech fyzických osob, se kterými přijde při výkonu práce do styku. Zaměstnanec je rovněž povinen dodržovat mlčenlivost o svých přístupových údajích a heslech do počítačových systémů zaměstnavatele.
2. Zaměstnanec zpracovává osobní údaje fyzických osob pouze na pokyn zaměstnavatele a při dodržení základních zásad zpracování osobních údajů, tj. zákonně, korektně, transparentně, k účelu, ke kterému byly údaje subjektem údajů poskytnuty, v minimálním nezbytném rozsahu, přesně, po dobu ne delší, než je nezbytné pro účel zpracování, a způsobem, který zajistí náležité zabezpečení osobních údajů včetně jejich ochrany před ztrátou, zničením, poškozením nebo neoprávněným zpřístupněním.
3. Zaměstnanec je povinen listinné nosiče osobních údajů (dokumenty) v době, kdy s nimi nepracuje, odpovídajícím způsobem zabezpečit před neoprávněným přístupem.
4. Zaměstnanec je povinen se odhlásit z počítačového systému nebo uzamknout prostředí operačního systému při vzdálení se od počítače zaměstnavatele, na kterém pracuje a prostřednictví kterého může vzniknout riziko neoprávněného přístupu k osobním údajům fyzických osob.
5. Zaměstnanec je povinen dodržovat veškeré povinnosti spojené s ochranou osobních údajů fyzických osob uložené zaměstnavatelem či právními předpisy, zejména pak povinnosti vyplývající z vnitřních předpisů zaměstnavatele, jakož i z právních předpisů upravujících ochranu osobních údajů.
6. Zaměstnanec je povinen veškeré povinnosti vztahující se k ochraně osobních údajů plnit pečlivě a odpovědně, přičemž je srozuměn, že v případě porušení povinností v oblasti ochrany osobních údajů odpovídá zaměstnavateli za škodu tím způsobenou.
7. Povinnost mlčenlivosti dle tohoto dodatku trvá i po skončení pracovního poměru.

III. Závěrečná ustanovení

Tento dodatek je sepsán ve dvou vyhotoveních, z nichž každá ze smluvních stran obdrží po jednom výtisku.

V *Město* dne *01. 01. 2020*

.....
Zaměstnavatel

V *Město* dne *01. 01. 2020*

.....
Zaměstnanec [235]

[235] Vlastní zpracování (r. 2018, revize 2020)