

GDPR

ŘEŠENÍ PROBLÉMŮ

V PRAXI ŠKOL

- povinnosti škol a školských zařízení jako správce osobních údajů
- vzory pro plnění povinností
- souhlas se zpracováním osobních údajů
- zveřejňování osobních údajů v prostředí škol a školských zařízení
- předávání osobních údajů žáků třetím osobám
- kamerové systémy ve školství



Eva Janečková

GDPR

ŘEŠENÍ PROBLÉMŮ
V PRAXI ŠKOL



Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována ani šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude trestně stíháno.

Edice Právo pro praxi

JUDr. Eva Janečková

GDPR – Řešení problémů v praxi škol

Vydala GRADA Publishing, a.s.
U Průhonu 22, Praha 7
tel.: 234 264 401, fax 234 264 400
www.grada.cz
jako svou 7497. publikaci

Realizace obálky Vojtěch Kočí
Sazba Jan Šístek
Odpovědná redaktorka Ing. Michaela Průšová
Počet stran 352
První vydání, Praha 2020
Vytiskla Tiskárna v Ráji, s.r.o., Pardubice

© **Grada Publishing, a.s., 2020**
ISBN 978-80-271-1354-5 (ePub)
ISBN 978-80-271-1353-8 (pdf)
ISBN 978-80-271-2579-1 (print)

Obsah

Seznam použitých pojmů 9
Seznam zkratek 11
Úvod 13

I. OBECNÁ ČÁST

1 Základní pojmy používané v oblasti ochrany osobních údajů 19

2 Základní zásady Obecného nařízení (GDPR) a jejich odraz v povinnostech 33

2.1 Zásada zákonnosti, korektnosti a transparentnosti 33

2.2 Zásada účelového omezení 40

2.3 Zásada minimalizace údajů 40

2.4 Zásada přesnosti 42

2.5 Zásada omezení uložení 43

2.6 Zásada integrity a důvěrnosti 45

2.7 Zásada odpovědnosti 46

3 Práva subjektu údajů 47

3.1 Právo na informace 48

3.2 Právo na přístup k osobním údajům 73

3.3 Právo na opravu a doplnění 75

3.4 Právo na výmaz 78

3.5 Právo na omezení zpracování 82

3.6 Právo na přenositelnost 84

3.7 Právo vznést námitku 87

3.8 Právo nebýt předmětem žádného rozhodnutí založeného výhradně na
automatizovaném zpracování, včetně profilování 89

3.9 Právo podat stížnost u dozorového úřadu 91

3.10 Výkon práv 92

4	Souhlas se zpracováním osobních údajů	95
4.1	Základní parametry souhlasu se zpracováním osobních údajů	95
4.2	Souhlasy ve školství	99
4.3	Souhlas žáků	106
5	Záznamy o činnostech	109
6	Posouzení vlivu na ochranu osobních údajů	187
7	Smlouva o zpracování osobních údajů	205
8	Zabezpečení osobních údajů	219
9	Porušení zabezpečení osobních údajů	225
10	Směrnice o zpracování osobních údajů	235
11	Pověřenec pro ochranu osobních údajů	247
12	Dozorový úřad	257
13	Sankce	263

II ZVLÁŠTNÍ ČÁST

1	Přijímání dítěte ke vzdělávání	271
1.1	Mateřská škola	271
1.2	Základní škola	283
2	Poskytování osobních údajů třetím osobám	291
2.1	Poskytování osobních údajů při kontrole České školní inspekce	291
2.2	Poskytování osobních údajů Policii ČR	293
2.3	Předávání osobních údajů žáků pojišťovnám	295
2.4	Spolupráce školy a OSPOD	296
2.5	Předání osobních údajů žáka při jeho přestupu na jinou školu	298

3	Pověření k vyzvedávání dítěte	301
4	Vzájemné povinnosti mezi zákonnými zástupci a školou při předávání osob- ních údajů	305
5	Zveřejňování a zpřístupňování osobních údajů	311
5.1	Zveřejňování smluv podle zákona o registru smluv a ochrana osobních údajů ...	311
5.2	Ochrana osobních údajů při poskytování informací	318
5.3	Povinnost mlčenlivosti a ochrana osobních údajů	327
6	Kamery se záznamem ve školství	331
6.1	Důvody pro instalaci kamerového systému	332
6.2	Zákonné důvody	333
6.3	Zákoník práce	336
6.4	Práva subjektu údajů	337
	Závěr	341
	Seznam použitých materiálů a odborné literatury	343

Seznam použitých pojmů

Obecné nařízení (GDPR)	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 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) (General Data Protection Regulation)
osobní údaje	veškeré informace o identifikované nebo identifikovatelné fyzické osobě – o subjektu údajů
správce	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení
subjekt údajů	identifikovatelná fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
souhlas	jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů
porušení zabezpečení osobních údajů	porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů
adaptační zákon	zákon č. 110/2019 Sb., o zpracování osobních údajů upravuje v souladu s Nařízením některé oblasti specificky pro Českou republiku

zpracovatel	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
zpracování (osobních údajů)	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
zvláštní kategorie osobních údajů	osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje a biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby
Sbor (Skupina WP29)	pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995
dozorový úřad	Úřad pro ochranu osobních údajů
pověřenec (DPO)	osoba dozorující u správce či zpracovatele zpracování osobních údajů
posouzení vlivu (DPIA)	posouzení pravděpodobného rizika zamýšleného zpracování

Seznam zkratk

kontrolní řád – zákon č. 255/2015 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů

občanský zákoník – zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

školský zákon – zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání

správní řád – zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

vyhláška č. 48/2005 Sb. – vyhláška č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky, ve znění pozdějších předpisů

zákon o ochraně veřejného zdraví – zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů

zákon o Policii ČR – zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

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 sociálně-právní ochraně dětí – zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí, ve znění pozdějších předpisů

zákon o svobodném přístupu k informacím – zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

zákoník práce – zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

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

Úvod

Dne 27. dubna 2016 schválil Evropský parlament konečnou podobu Nařízení Evropského parlamentu a Rady 2016/679 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). Obecné nařízení (GDPR) měly členské země do 6. května 2018 převést do vnitrostátní legislativy, platit začalo od 25. května 2018.

Toto nařízení nahradilo starou právní úpravu obsaženou ve Směrnici Evropského parlamentu a rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů (dále jen „Směrnice 95/46/ES“), která ukládala členským státům, aby ji promítly do tří let do svých právních řádů. Svoje zákony s ní musely samozřejmě harmonizovat i státy, které se chtěly stát členy Evropské unie. Směrnice však pocházela již z roku 1995, a byla tedy 22 let stará. V těchto letech došlo k prudkému rozvoji informačních technologií, ke změnám v kategoriích nejčastěji zpracovávaných osobních údajů, i k určitému smazání hranic mezi státy. Proto vyvstala potřeba úpravu zmodernizovat tak, aby kladla limity pro zpracování osobních údajů v oblastech, kde došlo k největšímu rozvoji a ke zpracování velkého množství osobních údajů, někdy i citlivých (podle nové terminologie „osobních údajů zvláštní kategorie“). Jedná se zejména o oblast marketingu, monitorování a profilování.

Směrnice 95/46/ES nebyla přímo aplikovatelná, byla do právních řádů jednotlivých států implementována národními zákony, které se v mnoha oblastech značně lišily. Cílem nové právní úpravy proto bylo i sjednocení.

V České republice se ochranou osobních údajů zabýval zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Tento zákon byl částečně zrušen Obecným nařízením (GDPR). Poslední ustanovení byla zrušena ke dni 24. 4. 2019, kdy nabyl účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů, tedy tzv. adaptační zákon, který upravuje v souladu s Obecným nařízením (GDPR) některé oblasti specificky pro Českou republiku.

Tento zákon však není obecným zákonem, který by komplexně upravoval oblast zpracování osobních údajů v České republice, jak se někteří domnívají. Týká se především některých specifických oblastí, zmocňuje výslovně některé orgány ke zpracování osobních údajů a stanoví zvláštní podmínky při plnění některých povinností. Je to tedy

pouze doprovodným zákonem, který je vždy třeba aplikovat současně s Obecným nařízením (GDPR).

Současně se zákonem o zpracování osobních údajů nabyt účinnosti i zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů. I tento zákon přináší některé změny, které se dotknou škol a školských zařízení. Jedná se zejména o novelu zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, do něhož byla vyložena nová povinnost. Do ustanovení § 64 byly mimo jiné vloženy následující odstavce:

„(4) Vykonávají-li určení původci spisovou službu v elektronické podobě v elektronickém systému spisové služby, vedou jako samostatnou funkční část evidenční pomůcky jmenný rejstřík v elektronické podobě určený pro automatické zpracovávání údajů o odesílatelech a adresátech dokumentů evidovaných v evidenční pomůcce a jiných osobách, jichž se dokumenty evidované v evidenční pomůcce týkají. Vykonávají-li určení původci spisovou službu v listinné podobě, mohou vést jako samostatnou funkční část evidenční pomůcky jmenný rejstřík v listinné podobě určený pro zpracovávání údajů o odesílatelech a adresátech dokumentů evidovaných v evidenční pomůcce a jiných osobách, jichž se dokumenty evidované v evidenční pomůcce týkají.

(5) Určení původci vedou ve jmenném rejstříku o odesílateli dokumentu, adresátu dokumentu nebo jiné osobě, jíž se dokument týká, alespoň

- a) jméno, popřípadě jména, a příjmení, jde-li o fyzickou osobu,*
- b) jméno, popřípadě jména, a příjmení, popřípadě dodatek odlišující osobu podnikatele nebo druh podnikání vztahující se zpravidla k této osobě nebo druhu podnikání, jde-li o podnikající fyzickou osobu nezapsanou v obchodním rejstříku,*
- c) obchodní firmu nebo název, jde-li o podnikající fyzickou osobu zapsanou v obchodním rejstříku nebo právnickou osobu,*
- d) identifikační číslo osoby, pokud bylo přiděleno,*
- e) identifikátor datové schránky, pokud byla zřízena, a*
- f) bezvýznamový identifikátor pro potřeby výkonu spisové služby, pokud byl určeným původcem přidělen.*

(6) Určení původci mohou vést ve jmenném rejstříku o odesílateli dokumentu nebo adresátu dokumentu, který je fyzickou osobou, a o jiné fyzické osobě, jíž se dokument týká, aniž by byl vyžadován jejich souhlas, údaje spadající do minimálního souboru osobních identifikačních údajů jedinečně identifikujících fyzickou nebo právnickou osobu podle přímo použitelného předpisu Evropské unie upravujícího rámec interoperability, nejde-li o údaje podle odstavce 5.

(7) Určení původci stanoví nejvýše tříletou skartační lhůtu pro údaje o fyzické osobě vedené ve jmenném rejstříku počínající běžet předáním dokumentů a spisů, ke kterým se údaje o fyzické osobě vztahovaly, nebo archivu nebo jejich zničením.

(8) Určení původci jsou oprávněni využívat pro účely vedení jmenného rejstříku údaje o odesílateli dokumentu, adresátu dokumentu nebo jiné fyzické osobě, již se dokument týká, pokud je jejich zdrojem jimi vedený spis.“

Tento jmenný rejstřík má mimo jiné být zásadní pomůckou pro realizaci práva subjektu údajů na přístup k údajům.

Základní povinnosti a práva jsou však nezměnitelná a zůstávají upravena v Obecném nařízení (GDPR) pro všechny členské země stejně.

Obecné nařízení (GDPR) se dotýká velmi podstatně chodu škol a školských zařízení, které zpracovávají velké množství osobních údajů, také zvláštní kategorie osobních údajů, a vzhledem k tomu, že se jedná o osobní údaje dětí, je na místě řešit jejich zpracování velmi obezřetně s velkým důrazem na zabezpečení těchto údajů.

V praxi škol a školských zařízení vznikla celá řada otázek, zejména ve vztahu k nakládání s fotografiemi, při zveřejňování osobních údajů či předávání údajů třetím osobám. Velmi často dochází k neshodám mezi názory Úřadu pro ochranu osobních údajů, názory Ministerstva školství, mládeže a tělovýchovy a názory odborné veřejnosti.

Vzhledem k tomu, že s účinností Obecného nařízení (GDPR) nedošlo ke změně základní legislativy v oblasti školství, není ani oblast zpracování osobních údajů ve školách a školských zařízeních zásadně odlišná od předchozí praxe. Je však třeba uvědomit si některé skutečnosti, které byly v přechozích letech opomíjeny, a zapracovat nové instituty.

I.

Obecná část

1 Základní pojmy používané v oblasti ochrany osobních údajů

Jedním z klíčových ustanovení Obecného nařízení (GDPR) je článek 4, v němž jsou vymezeny základní pojmy. Toto ustanovení patří mezi jedno z nejdůležitějších, neboť pochopení jednotlivých pojmů, resp. jejich definic, je podstatné pro další činnost správce nebo zpracovatele, pro realizaci práv a plnění povinností, která z Obecného nařízení (GDPR) vyplývají.

Nejprve je nutné vyhodnotit, zda informace, s níž správce pracuje, je skutečně osobním údajem, jak jej definuje článek 4 písm. a) Obecného nařízení (GDPR), zda proces s ním prováděný je zpracováním ve smyslu definice, a teprve v případě kladné odpovědi na tyto otázky se správce zabývá dalšími ustanoveními Obecného nařízení (GDPR), jež mu ukládají povinnosti a dávají práva.

Článek 4 definuje řadu základních pojmů; vymezeny jsou všechny základní pojmy ve smyslu jejich hmotného obsahu (např. osobní údaj a další) a také pojmy, které lze označit za „popis procesu“ (např. zpracování). Škola či školské zařízení se nebudou v běžné praxi setkávat se všemi pojmy uvedenými v článku 4 Obecného nařízení (GDPR)¹, zde jsou proto zmíněny pouze ty nezákladnější pojmy, u nichž je porozumění podstatné pro každého správce a zpracovatele a se kterými se bude škola setkávat každodenně.

Osobní údaj

Tento pojem je tím nejzákladnějším a nejpoužívanějším pojmem. Definice zůstala téměř stejná jako v předchozí právní úpravě. Podle definice jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické,

¹ Např. profilování či přeshraniční zpracování se běžně při činnosti škol objevovat nebude.

fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. Ke změně došlo především v příkladném výčtu osobních údajů ve druhé části definice.

Pojem je definován několika parametry. Prvním parametrem je rozsah. Definice říká, že osobním údajem je informace, aniž blíže uvádí charakteristiku informace, kterou je třeba za osobní údaj považovat. Znamená to například, že není kladen důraz na pravdivost informace. Může se také jednat nejen o informace tzv. objektivní, ale také o různé soudy, hodnocení, závěry a podobně.

Osobním údajem je tedy jakýkoli údaj, jenž se vztahuje k nějaké fyzické osobě. Současně je ovšem třeba, aby tato osoba byla těmito údaji či na jejich základě minimálně identifikovatelná. Pro to, zda jde o osobní údaj, je rozhodná skutečnost, zda je možno ze strany správce vytvořit přímý vztah mezi takovým údajem a danou fyzickou osobou. Takový vztah se vytváří prostřednictvím určitých identifikátorů, na jejichž základě lze jednoznačně určit, že se jedná o určitou osobu.

O osobní údaj se však jedná i v případě, že správce sice nedisponuje údaji, jimiž by mohl provést (přímou) identifikaci, ale má možnost si takový údaj opatřit a spojit s údajem, kterým disponuje (např. jméno a příjmení s rodným číslem). V takovém případě lze zjistit identitu subjektu údajů nepřímou. Určenost je tedy stav, kdy správce disponuje údaji, jimiž lze fyzickou osobu přímo jednoznačně identifikovat, o určitelnost jde tam, kdy správce může na základě údajů, která má buď k dispozici, nebo k nimž má přístup, tuto osobu jednoznačně odlišit od jiných subjektů.² V těchto případech bude nezbytné zpracování takových údajů posuzovat zcela individuálně, případ od případu. Bude záležet na rozsahu údajů či zpracovávaných informací, dostupnosti a legálním zdroji případných dalších údajů, přístupu k těmto zdrojům apod.

Obecné nařízení (GDPR) stanoví, že informace se musí týkat subjektu údajů (tedy fyzické osoby) a tato fyzická osoba pak musí být buď identifikovaná, nebo alespoň identifikovatelná. I když nepanuje shoda, které informace mohou subjekt údajů jednoznačně identifikovat, neboť bude vždy záviset na okolnostech, oblasti zpracování apod., nicméně je možné konstatovat, že určit osobu, a to natolik přesně, aby nebyla zaměnitelná za jinou fyzickou osobu, lze nepochybně říci, že těmito údaji obecně bude jméno, příjmení, bydliště a případně i rok narození. Na základě těchto údajů bude fyzická osoba identifikována přímo a subjekt údajů tak bude určen. Fyzická osoba však může být identifikována, a tedy určena, v některých případech i menším rozsahem údajů. Pak se hovoří o určení nepřímém, tedy identifikovatelnosti, resp. určitelnosti subjektu údajů.³

² Mates, P.: Ochrana soukromí ve správním právu. Praha 2004, s. 188.

³ Janečková, E.: GDPR – řešení problémů v praxi obcí, GRADA, Praha 2019, str. 20.

O tom, že mezi osobní údaje patří identifikátory jako jméno, příjmení, adresa, datum narození nebo rodné číslo, nikdo nepochybuje. U dalších kategorií osobních údajů buď může dojít k pochybnostem, nebo správce ani nenapadne, že informace, se kterou pracuje, je osobním údajem. Mezi takové informace – údaje patří například telefonní číslo nebo emailová adresa. Prostřednictvím těchto údajů je totiž možné kontaktovat fyzickou osobu a následně ji identifikovat, prostřednictvím těchto údajů (i každého zvlášť) je tedy fyzická osoba identifikovatelná. Podmínkou je, že se daná informace vztahuje k jedné konkrétní osobě.

Diskutuje se o podobě emailové adresy, o podobě, která je ještě osobním údajem, a která již nikoli. Shoda panuje na tom, že osobním údajem je emailová adresa v podobě jmeno.prijmeni@domena.cz. U tzv. anonymních adres však shoda není. Nicméně pro větší jistotu správce je vhodnější považovat i adresu rakosnicek@seznam.cz za osobní údaj.

Pro zajímavost je možné uvést, že podle judikatury Evropského soudního dvora je osobním údajem i IP adresa (ze které někdo např. přistupuje na školní web), protože ji mohou ke ztotožnění konkrétního člověka využít orgány činné v trestním řízení ve spolupráci s poskytovatelem připojení, pokud se tento člověk z IP adresy dopustí trestného činu. Lze tedy uzavřít, že okruh údajů, prostřednictvím nichž lze identifikovat člověka, je velice široký.

Úprava ochrany osobních údajů se nevztahuje na anonymní informace, tedy na informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že daná osoba není nebo již přestala být identifikovatelná. V čl. 4 Obecného nařízení (GDPR) nalezneme i definici pseudonymizace, kterou může představovat například přidělení číselných kódů jednotlivým uchazečům v přijímacím řízení ke vzdělávání ve střední škole, na základě kterých nebude možné konkrétního uchazeče bez dalších informací identifikovat (identifikace bude možná pouze spojením dokumentu, který obsahuje kód a jméno zároveň, jímž disponuje pouze uchazeč, zákonný zástupce a škola – z toho plyne, že vůči veřejnosti jde o informaci anonymní, ale dovnitř školy jde o informaci spojitelnou s konkrétním subjektem údajů).⁴

Je zjevné, že škola zpracovává velké množství osobních údajů žáků, zákonných zástupců, zaměstnanců, ale i dalších osob.

Obecné nařízení (GDPR) nezná pojem „citlivé osobní údaje“, jak jej obsahoval předchozí zákon. Objevil se termín zvláštní kategorie osobních údajů, jejichž definice však v článku 4 chybí. Tato zvláštní kategorie je upravena v článku 9 Obecného na-

⁴ Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství, <http://www.msmt.cz/file/44592/>

řízení (GDPR). Tento článek uvádí, že se zakazuje zpracování osobních údajů, 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.

Výčet je tedy o něco užší než u předchozí definice. Není bez zajímavosti připomenout, že zvláštní význam citlivých osobních údajů (informací) není výsadní doménou právní úpravy ochrany osobních údajů. Jejich význam je jistě zdůrazněn skutečností, že okruhy informací, resp. skutečností se dotýkají těch právních vztahů, jež jsou relevantní např. pro zákaz diskriminace podle zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), když diskriminace je zakázána také z důvodů rasy, etnického původu, národnosti, pohlaví, sexuální orientace, věku, zdravotního postižení, náboženského vyznání, víry či světového názoru⁵.

Je nutné připomenout, že do zvláštních kategorií osobních údajů patří jen ty údaje, které lze zařadit do kategorií, které jsou výslovně zmíněny v článku 9 Obecného nařízení (GDPR). Jiné údaje, byť mohou být lidmi subjektivně pocíťovány jako velmi citlivé, ve smyslu právní úpravy mezi zvláštní kategorie osobních údajů nespadají.

V praxi škol jsou často zpracovávány údaje o zdravotním stavu, jejichž zpracování je požadováno § 28 zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů (dále jen „školský zákon“), konkrétně § 28 odst. 2 písm. f) a g) – údaje o znevýhodnění dítěte, žáka nebo studenta uvedeném v § 16, údaje o mimořádném nadání, údaje o podpůrných opatřeních poskytovaných dítěti, žákovi nebo studentovi školou v souladu s § 16, a o závěrech vyšetření uvedených v doporučení školského poradenského zařízení, údaje o zdravotní způsobilosti ke vzdělávání a o zdravotních obtížích, které by mohly mít vliv na průběh vzdělávání.

Z § 16 odst. 4 školského zákona vyplývá, že podpůrná opatření prvního stupně uplatňuje škola nebo školské zařízení i bez doporučení školského poradenského zařízení. Podpůrná opatření druhého až pátého stupně lze uplatnit pouze s doporučením školského poradenského zařízení.

Není tedy možné, aby bylo ve školní matrice školy uvedeno, že dané dítě, žák či student má zdravotní obtíže, které by mohly mít vliv na průběh vzdělávání a které vyžadují poskytnutí podpůrných opatření druhého až pátého stupně, aniž by byl v dokumentaci

⁵ Ustanovení § 2 odst. 3 antidiskriminačního zákona.

školy uvedené v § 28 odst. 1 písm. c) školského zákona zároveň veden posudek školského poradenského zařízení, ze kterého by daný závěr vyplýval.

Z posudku školského poradenského zařízení zároveň vždy vyplývá, jakým způsobem je nezbytné zdravotní způsobilost ke vzdělávání a zdravotní obtíže dítěte, žáka či studenta zohlednit při jeho vzdělávání, tak, aby byl respektován § 16 odst. 6 až 9 školského zákona. Proto je také povinností zákonného zástupce dítěte a nezletilého žáka nebo zletilého žáka či studenta podle § 22 odst. 2 písm. a) a c) a odst. 3 písm. c) a e) školského zákona informovat školu o těchto skutečnostech a poskytnout jí nezbytné informace a doklady.

Zvláštní kategorie údajů jsou dále zpracovávány podle ustanovení § 28 odst. 1 písm. i) školského zákona, podle něhož školy a školská zařízení vedou mimo jiné knihu úrazů a záznamy o úrazech dětí, žáků a studentů, popřípadě lékařské posudky. Úrazem žáků je úraz, který se stal žákům při vzdělávání nebo s ním přímo souvisejících činnostech a při poskytování školských služeb. Jedná se tedy zejména o úrazy žáků na vycházkách, výletech, zájezdech, putováních, exkurzích, při koupání, při výuce plavání a lyžařském výcviku, sportovních a turistických kurzech, zahraničních výletech, při účasti na soutěžích a přehlídkách.⁶

Správce a zpracovatel

Mezi klíčová ustanovení právní úpravy náleží vymezení pojmů správce a zpracovatel. Správcem je podle článku 4 odst. 7 Obecného nařízení (GDPR) fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.

Jinak řečeno, toto ustanovení jednoznačně charakterizuje okruh adresátů právní normy z hlediska tzv. osobní působnosti a okruhu věcné působnosti. Z výčtu adresátů normy je zřejmé, že Obecné nařízení (GDPR) dopadá na každý subjekt, který osobní údaje zpracovává, neboť vzhledem k rozsahu vymezení těžko nalezneme subjekt, který by byl ze základního vymezení působnosti tohoto nařízení vyňat, a to bez ohledu na jejich právní subjektivitu.

⁶ Článek 21 Metodického pokynu Ministerstva školství, mládeže a tělovýchovy k zajištění bezpečnosti a ochrany zdraví dětí, žáků a studentů ve školách a školských zařízeních zřizovaných Ministerstvem školství, mládeže a tělovýchovy.

Správce je každý, kdo určuje prostředky a účel zpracování osobních údajů, přičemž není rozhodné, zda se jedná o fyzickou či právnickou osobu, rozhodná není ani její povaha (může jít o podnikatelský subjekt, orgán veřejné moci či jednotlivce). Významné je, že se dotýčný rozhodl osobní údaje systematicky zpracovávat nebo je mu zpracování uloženo zákonem jako povinnost (např. orgány veřejné správy). Zpracováním osobních údajů může správce provádět sám, nebo může k této činnosti někoho zmocnit nebo pověřit. Touto osobou je zpracovatel, jenž je Obecným nařízením (GDPR) charakterizován jako fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Do definice jsou tak zahrnuty veškeré subjekty bez ohledu na jejich povahu či právní subjektivitu.

Na rozdíl od správce, zpracovatel „pouze“ provádí zpracovávání osobních údajů. Zpracovatel, na rozdíl od správce, neurčuje účel a prostředky zpracování osobních údajů. Zpracovatel nemusí provádět zpracování od začátku do konce, tedy veškeré operace, ale může provádět jen některou (či některé) činnost související se zpracováním. Nemusí tedy jít vždy o subjekt, který osobní údaje shromáždil.

Zpracovatel může zpracovávat údaje buď na základě výslovného zákonného zmocnění, nebo je-li k tomu zmocněn správcem nebo na základě smluvního ujednání. Z dosavadních zkušeností však vyplývá, že vztah mezi správcem a zpracovatelem se v naprosté většině případů odehrává na základě smluvního vztahu.⁷

V některých případech je však stanoveno, že zpracování provádí jiný subjekt, jímž je zpracovatel, přímo zákonem. Takové zákonné zmocnění se obvykle týká jen určitých způsobů zpracování (nejčastěji shromažďování údajů) a správce pak provádí další způsoby (např. uchovávání údajů a jejich předávání).

Z pohledu odpovědnosti za zpracování osobních údajů nelze být zároveň v postavení správce a zpracovatele, resp. při zpracování za jedním účelem nelze být v obou pozicích, subjekt však může být pro jeden účel správce a pro jiný zpracovatelem. Jestliže určitý, např. podnikatelský subjekt je správcem osobních údajů, nemůže žádná z jeho organizačních složek být současně vůči těmto zpracování týmům zpracování těchto osobních údajů zpracovatelem. Případné nesprávné nebo jinak nepřesné používání termínů správce a zpracovatel na postavení a povinnostech podnikatelského subjektu nic nemění.⁸

Podstatné pro rozlišení jejich postavení a určení vzájemného vztahu je, že se správce rozhodl (nebo mu to bylo určeno zákonem) vykonávat nějakou činnost, jejíž nezbytnou součástí je zpracování osobních údajů, a dále skutečnost, že určí prostředky zpracování.

⁷ Bartík, V. – Janečková, E.: Zákon o ochraně osobních údajů s komentářem. Nakladatelství ANAG, Olomouc 2010, s 58.

⁸ Poradce č. 3/2005, Zákon o ochraně osobních údajů s komentářem, str. 17.

Zpracovatel vykonává svou činnost ve chvíli, kdy se správce rozhodne, že některou z činností nebude provádět sám, ale využije služeb jiného subjektu, který vykonává tuto činnost pro správce, resp. místo něj a stává se tak v oblasti ochrany osobních údajů dodavatelem služeb.

Často také dochází k diskuzím, které vychází ze znění článku 4 odst. 2 Obecného nařízení (GDPR), podle něhož je zpracováním 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. Tato problematika se týká zejména oblasti IT, především provádění různých servisních prací.

Vzhledem k tomu, že zpracovatel je subjekt odlišný od správce, v drtivé většině určený správcem, aby za něj prováděl zpracování osobních údajů, z povahy věci tak musí jít o subjekt, který je pověřen, na základě pokynů správce, provádět operace zpracování s osobními údaji, které by jinak prováděl správce sám. Lze zjednodušit, že zpracovatel představuje pouze náhradu prostředků zpracování, kterými správce sám nemusí nebo nechce z různých důvodů disponovat. V případě, že poskytování servisních prací, jejichž předmět v žádném aspektu nespočívá v operacích zpracování osobních údajů, ale při jejichž výkonu nelze vyloučit nahlédnutí na osobní údaje servisním pracovníkem, bychom považovali za zpracování s výskytem zpracovatele, tvrdili bychom de facto, že „teoretické nahlížení na osobní údaje“ je operací zpracování, kterou správce pověřil zpracovatele.

Smlouvou o zpracování osobních údajů se velmi často kryje právě riziko vyplývající z možného zneužití osobních údajů (informací) i v těch případech, kdy osobní údaje nejsou předmětem činnosti poskytovatele servisních (IT) služeb, ale jsou možná teoretická možnost nahlédnutí, a tedy i zneužití. Taková praxe je však nesprávná.⁹

Škola vždy bude patřit mezi správce, jejichž postavení je určeno zákonem. Zákon stanoví povinnost zpracovávat osobní údaje za určitými účely (např. vedení školní matriky). Mezi právní předpisy, které se nejvíce dotýkají činnosti škol a školských zařízení, patří školský zákon, vyhláška č. 48/2005 Sb., o základním vzdělávání a některých náležitostech plnění povinné školní docházky, ve znění pozdějších předpisů, zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, vyhláška MŠMT č. 27/2016 Sb., o vzdělávání žáků se speciálními vzdělávacími potřebami a žáků nadaných, ve znění pozdějších předpisů, zákon č. 359/1999 Sb., o sociálně-právní ochraně

⁹ Zveřejněno na LinkedIn.com

dětí, ve znění pozdějších předpisů, vyhláška MŠMT č. 72/2005 Sb., o poskytování poradenských služeb ve školách a školských poradenských pracovištích, ve znění pozdějších předpisů.

Zároveň škola obvykle spadá i do skupiny správců (může, ale nemusí), kteří samostatně rozhodují o rozsahu, účelu a prostředcích zpracování určitých osobních údajů (např. v případě, kdy se škola rozhodne instalovat kamerový systém se záznamem).

Účelem se chápe cíl, smysl dané činnosti, to, proč ke zpracování osobních údajů dochází. Při zpracování osobních údajů, které škole ukládá zákon, škola neurčuje účel zpracování, ten je určen tímto zákonem. Přesto je vhodné i tyto účely identifikovat a nazvat pro účely vedení záznamů o zpracování osobních údajů.

Prostředky se rozumí nástroje a zvolené postupy pro konkrétní zpracování. Obecné nařízení (GDPR) rozeznává zpracování:

- a) automatizované, kdy dochází ke zpracování osobních údajů v elektronické podobě a prostředky zpracování osobních údajů jsou např. počítače, kamerové systémy, a
- b) manuální, kdy dochází ke zpracování osobních údajů v listinné podobě a prostředky zpracování osobních údajů jsou např. kartotéky vedené v listinné podobě.

Subjekt údajů

Dalším důležitým pojmem je pojem subjekt údajů. Zákon o ochraně osobních údajů obsahoval definici, která uváděla, že subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují.¹⁰

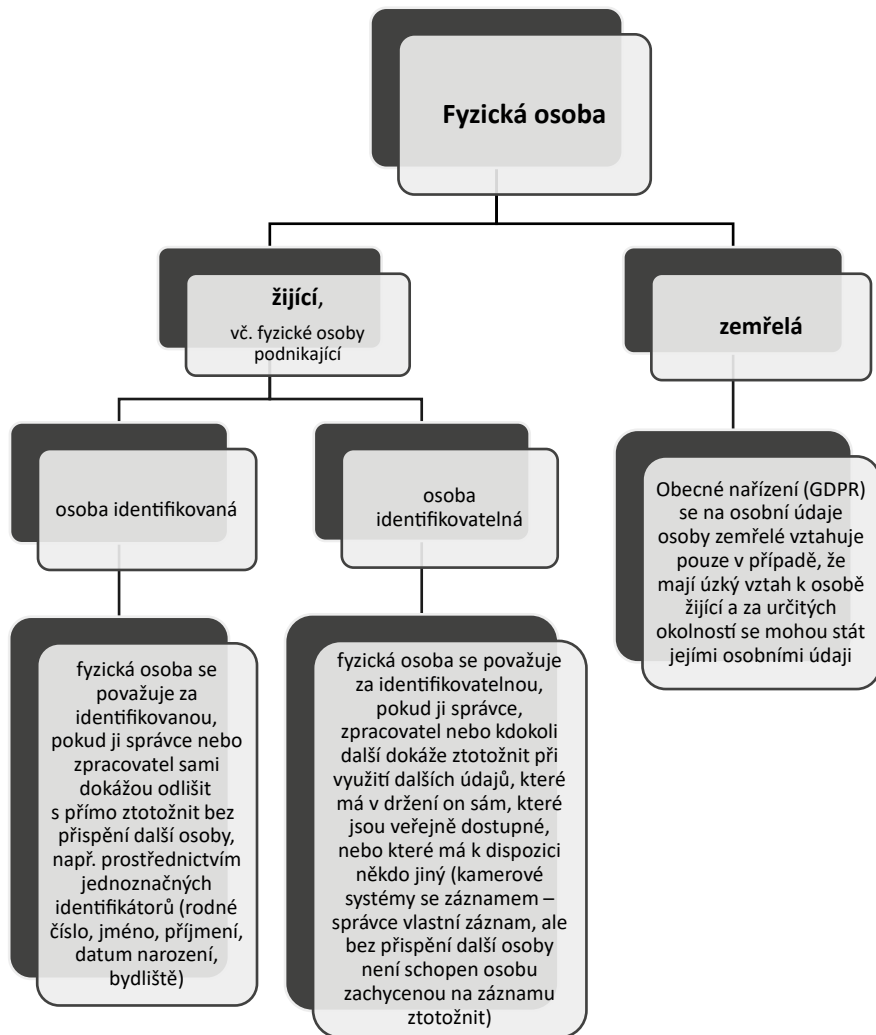
Obecné nařízení (GDPR) samostatnou definici subjektu údajů neobsahuje. Je součástí definice osobního údaje –veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“).

Obecné nařízení (GDPR) se tedy vztahuje pouze na údaje osob fyzických, nikoli osob právnických. Problémy však v minulosti nastávaly u fyzických osob podnikajících. Pohled byl takový, že i fyzická osoba podnikající může být subjektem údajů a jako taková může být zasažena ve svém soukromí, avšak pouze v závislosti na skupině zpracovávaných osobních údajů. Pokud byly zpracovávány pouze osobní údaje týkající se osoby coby podnikatelského subjektu a údaje, které se týkaly pouze její podnikatelské aktivity, nemohlo – vzhledem k tomu, že podnikání není činností, jež by byla s to zasáhnout do soukromí, neboť se netýká soukromí tak, jak jej chápe občanské právo –

¹⁰ Ustanovení § 4 písm. d) zákona o ochraně osobních údajů.

dojít k neoprávněnému zásahu do soukromí. Takovým údajům proto nebyla přiznána ochrana podle tohoto zákona.

Graficky je možné výše uvedené znázornit takto:



Tento výklad však již byl překonán. Postupně se ukázalo, že většina údajů týkající se fyzických osob podnikajících jakožto podnikatele se překrývá s osobními údaji vztahujícími se k jejich soukromí. Osobní údaje fyzické osoby podnikající jsou proto v současné době považovány za údaje, které požívají ochrany Obecného nařízení (GDPR).

Cílem právní úpravy ochrany osobních údajů je přispět k ochraně soukromí dotčených osob. Právě možný, byť nepřímý, a nikoli významný, resp. bagatelní dopad do

soukromí by měl být limitou při rozhodování, zda určitá informace je či není osobním údajem. Charakter údajů, tedy to, zda vypovídají pouze o soukromém životě dotčené osoby, pouze o profesní činnosti, nebo mají dopad do obou sfér, bude mít význam při posuzování přípustnosti jejich zpracování a míry zásahu, resp. přiměřenosti tohoto zásahu do soukromí dané osoby^{11, 12}

Zpracování

Jak již bylo uvedeno výše, Obecné nařízení (GDPR) charakterizuje pojem zpracování, kterým se rozumí 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.

Tuto definici lze logicky rozdělit na několik částí. Především říká, že „zpracováním osobních údajů je jakákoliv operace nebo soustava operací“. Definice tak zahrnuje každý zásah do informace. Podstatnou částí této definice je tedy skutečnost, že se nemusí vždy jednat o celý soubor činností, ale může jít v některých případech jen o některé z nich, dokonce se může jednat o operaci jedinou.

K tomu, aby bylo možno hovořit o zpracování, stačí, je-li uskutečňována jen některá z uvedených činností. Výčet je demonstrativní vzhledem k tomu, že s ohledem na vývoj technologií nemohl zákonodárce předvídat, která další zpracování se mohou i v blízké budoucnosti ještě objevit.

Zpracování je tedy operace prováděná s osobními údaji za účelem dosažení cíle, který si stanoví sám správce nebo pro realizaci činnosti, kterou správci ukládá zvláštní zákon. Na druhé straně, ne každý případ, kdy někdo k datům přistoupí, je zpracováním ve smyslu definice. Např. ad hoc přístup k datům nezbytným k servisu poskytovaného hardwaru nebo softwaru nebo jiný zásah do nastavení softwaru či databáze jako takové zpracování osobních údajů ve smyslu definice představovat nebude.¹³

¹¹ Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J.: GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Wolters Kluwer, Praha 2017, s. 81.

¹² Janečková, E.: GDPR – řešení problémů v praxi obcí, GRADA, Praha 2019, str. 23.

¹³ Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J.: GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Wolters Kluwer, Praha 2017, s. 85.

Zpracováním je jakákoli činnost od začátku do konce, počínaje shromažďováním, které je už zpracováním, konče likvidací, která je také zpracováním. Zpracování končí ve chvíli, kdy osobní údaje zcela přestávají existovat.

Souhlas

Jedním z nejdůležitějších pojmů pro celou oblast zpracování osobních údajů, je pojem souhlas. Definice souhlasu se zpracováním osobních údajů je uvedena v článku 4 odst. 11 Obecného nařízení (GDPR). Podle tohoto ustanovení se souhlasem subjektu údajů rozumí jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.

Ani Obecné nařízení (GDPR) tedy neklade požadavek písemnosti souhlasu se zpracováním osobních údajů. Souhlas musí být konkrétní a jednoznačný. To potvrzuje i recitál 32, který říká, že souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení. Mohlo by se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které v této souvislosti jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů.

Obecné nařízení (GDPR) zároveň upozorňuje na známou poučku, že mlčení neznamená souhlas, když uvádí, že mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas.

Obecně je poskytnutí souhlasu právním úkonem, a to právním úkonem, který je svým charakterem jednoznačně jednostranným. Nejedná se tedy o dohodu mezi správcem nebo zpracovatelem na straně jedné a subjektem údajů – fyzickou osobou na straně druhé. Pro posouzení jeho platnosti je proto nutné vzít v potaz i úpravu právních úkonů v obecném právním předpisu, jímž je v tomto případě zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“) (více viz kapitola IV).

Porušení zabezpečení osobních údajů

Obecné nařízení (GDPR) definuje „porušení zabezpečení osobních údajů“ v čl. 4 odst. 12 jako „porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů“.

Co se rozumí pod pojmem „zničení“ osobních údajů, by mělo být zcela jasné: jedná se o situaci, kdy údaje již vůbec neexistují nebo již neexistují ve formě, která je pro správce jakkoli použitelná. Pojem „poškození“ by měl být taktéž poměrně jasný: jedná se o situaci, kdy osobní údaje byly změněny, narušeny nebo již nejsou úplné. Výraz „ztráta“ je nutno v případě osobních údajů vykládat tak, že údaje sice ještě možná existují, ale správce nad nimi ztratil kontrolu, nemá k nim přístup nebo je již nemá ve svém držení. A konečně neoprávněné nebo protiprávní zpracování může zahrnovat zpřístupnění osobních údajů příjemcům, kteří nejsou oprávněni tyto údaje přijímat (nebo k nim mít přístup), (nebo přístup uvedených příjemců k těmto údajům), nebo jakoukoli jinou formu zpracování, která porušuje ustanovení Obecného nařízení (GDPR).

Příklad

Příkladem ztráty osobních údajů může být situace, kdy zařízení obsahující osobní údaje žáků bylo ztraceno nebo odcizeno, nebo když byly odcizeny nebo ztraceny dokumenty obsahující osobní údaje, popřípadě došlo k zašifrování databáze takovým způsobem, že ji není možné zpětně rozšifrovat.

Mělo by být jasné, že porušení je druhem bezpečnostního incidentu. Jak však uvádí čl. 4 odst. 12, Obecné nařízení (GDPR) se vztahuje pouze na případy, kdy došlo k porušení zabezpečení osobních údajů. Důsledkem takového porušení je, že správce nebude schopen zajistit dodržování zásad zpracování osobních údajů uvedených v článku 5 Obecného nařízení (GDPR). To poukazuje na rozdíl mezi bezpečnostním incidentem a porušením zabezpečení osobních údajů – zatímco v podstatě všechna porušení zabezpečení osobních údajů představují bezpečnostní incidenty, ne všechny bezpečnostní incidenty jsou nutně porušením zabezpečení osobních údajů.¹⁴

¹⁴ Pokyny k ohlašování případů porušení zabezpečení osobních údajů podle nařízení (EU) 2016/679, https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31894

Nejčastější typy porušení zabezpečení osobních údajů ve školách či školských zařízeních jsou:

- a) ztráta nebo odcizení dokumentů,
- b) neoprávněný přístup osoby (např. žáka) do databáze,
- c) zaslání osobních údajů prostřednictvím emailu třetí osobě/osobám,
- d) zaslání dokumentů (např. rozhodnutí o nepřijetí) třetí osobě.

2 Základní zásady Obecného nařízení (GDPR) a jejich odraz v povinnostech

Základní zásady zpracování osobních údajů jsou uvedeny v článku 5 Obecného nařízení (GDPR). Ze všech těchto zásad vyplývají pro správce a zpracovatele povinnosti, jež je třeba dodržovat v rámci jejich běžné činnosti. Téměř všechny tyto povinnosti jsou odrazem povinností, které byly dříve obsaženy v § 5 odst. 1 a 2 zákona o ochraně osobních údajů.

2.1 Zásada zákonnosti, korektnosti a transparentnosti

Všechna zpracování osobních údajů je možné realizovat pouze na základě zákonných titulů, které musí být dostatečně specifické, korektní a transparentní. Tato zásada vyžaduje povinnost nalézt ke zpracování osobních údajů vždy minimálně jeden z důvodů uváděných v Obecném nařízení (GDPR). Díky analýze, která byla provedena prakticky u všech správců a zpracovatelů před samotnou implementací Obecného nařízení (GDPR), byl (měl být) vytvořen kompletní přehled o zpracování osobních údajů, které ve školách probíhají.

Takový přehled mimo jiné obsahuje:

- ke každému zpracování osobních údajů účely zpracování osobních údajů (účelem zpracování je účel, pro jaký jsou osobní údaje zpracovávány. Obvykle jím bývá každá konkrétní agenda např. evidence úrazů žáků, zpracování osobních údajů v souvislosti s poskytováním podpůrných opatření, zpracování osobních údajů v souvislosti s prezentací školy. Velmi často jde o zákonem stanovenou povinnost zpracovávat osobní údaje pro určitý účel a většinou i ve stanoveném rozsahu);
- právní titul, na jehož základě zpracování probíhá.

Tak správce získal přehled účelů a k nim přiřazených zákonných důvodů pro zpracování osobních údajů. U některých účelů bylo nutné zvažovat, který z nabízených titulů bude nejvhodnější, v jiných případech je možné opřít se hned o dva zákonné důvody (obvykle se jedná o plnění právní povinnosti a o výkon veřejné moci).

Z Obecného nařízení (GDPR) vyplývá, že pro zpracování osobních údajů musí vždy být minimálně jeden z důvodů. V případě, že zákonný důvod není nalezen nebo pomine, je nezbytné osobní údaje zlikvidovat. Jestliže od počátku neexistoval řádný právní důvod zpracování, jedná se o nelegální zpracování a tento nedostatek nelze zhojit bezvadným plněním ostatních povinností stanovených Obecným nařízením (GDPR). Zásada zákonnosti, tj. přítomnost právního důvodu zpracování, je tedy základním předpokladem, aby bylo možné hovořit o zpracování osobních údajů jako o zákonném.¹⁵

Zásada zákonnosti také stanoví, že zpracování nesmí být protiprávní, což znamená, že nesmí probíhat za nelegálním či nelegitimním účelem. Zákaz protiprávního zpracování přitom neznamená pouze to, že zpracování nesmí probíhat v rozporu s Obecným nařízením (GDPR), ale také to, že nesmí být v rozporu s právním řádem obecně. Pokud tedy zpracování bude splňovat nároky plynoucí z Obecného nařízení (GDPR), ale nebude probíhat např. v souladu s občanským zákoníkem, bude to znamenat porušení zásady zákonnosti. Porušením této zásady je také získání či jiné zpracování osobních údajů v rozporu se smluvní povinností, povinností mlčenlivosti nebo základním právem na soukromí.¹⁶

Součástí transparentnosti je kromě dále zmíněného plnění informační povinnosti to, že správce nejen nebude zastírat pravý účel, pro který byly osobní údaje shromážděny a jsou dále zpracovávány, ale že také nebude zastírat svou pravou identitu, způsob zpracování atd.

Výčet zákonných titulů obsahuje Obecné nařízení (GDPR) v článku 6, kde uvádí, že zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) *subjekt údajů udělil souhlas* se zpracováním svých osobních údajů pro jeden či více konkrétních účelů. Souhlasem a jeho parametry se Obecné nařízení (GDPR) zabývá především v článku 7, ale věnuje se mu i několik recitálů (viz následující kapitola).

Školy se souhlasem pracují poměrně často. Otázkou zůstává, zda je souhlas skutečně nutný, nebo zda škole svědčí jiný zákonný důvod. Školy totiž často z opatrnosti

¹⁵ Žůrek, J.: Praktický průvodce GDPR. ANAG, Olomouc 2017, s. 59.

¹⁶ Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J.: GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Wolters Kluwer, Praha 2017, s. 106.

vyžadují souhlas i v situacích, kdy je možné deklarovat jiný právní důvod, a dostávají se tak do problémů. Lze konstatovat, že škola jakožto správce osobních údajů by měla při zahájení zpracování nejprve zjistit, zda může využít jinou podmínku legálního zpracování (zda neexistuje jiný zákonný důvod), než je souhlas subjektu údajů. Souhlas by měla škola využívat teprve tehdy, když legální zpracování osobních údajů na základě jiné podmínky není možné.

Škola by v praxi měla se souhlasem pracovat jen v několika málo případech. Jedná se například o situaci, kdy docházím ke zveřejnění fotografií zaměstnance z propagačních či jiných účelů, které nesouvisí s jeho pracovněprávním vztahem.

- 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.

V první situaci zohledněné tímto zákonným důvodem je smluvní vztah mezi subjektem údajů a další osobou, tedy správcem, již uzavřen (jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů) a je třeba údaje buď uchovávat, nebo i v průběhu smluvního vztahu získávat jiné než původně poskytnuté osobní údaje. Formální souhlas se zpracováním není vyžadován, neboť lze dovodit, že osobní údaje budou správci poskytnuty právě subjektem údajů, a to proto, aby smluvní vztah mohl být realizován, a je tak v zájmu subjektu údajů takové údaje poskytnout.

Druhou možností je situace, kdy „smluvní iniciativu“ vyvine subjekt údajů sám a pro přípravu smlouvy poskytne druhé smluvní straně (správci) takové osobní údaje, aby smlouva mohla být vůbec uzavřena nebo případně změněna. I zde tedy platí, že subjekt údajů je plně informován, jaké osobní údaje poskytne, jakému správci, pro jaký účel (plnění smlouvy) a na jak dlouho, tedy minimálně po dobu od poskytnutí údajů po ukončení smluvního vztahu, pokud nějaký jiný právní předpis nestanoví dobu delší.

Tento zákonný důvod se tedy vztahuje pouze na zpracování vztahující se k plnění ze smlouvy, nikoli na vymáhání nesplněných závazků, které plynou ze smlouvy, ze strany subjektu údajů. Ať už se jedná o podání žaloby, předání exekutorovi k vymáhání či jiný způsob, kterým se správce snaží domoci svých práv, je nutné tento úkon opřít o jiný zákonný důvod. Tím obvykle bývá ochrana oprávněných zájmů správce.¹⁷

V praxi škol se tento zákonný důvod může objevit hned v několika oblastech:

- smlouvy nájemní – např. pronájem tělocvičny
- dohoda o zasílání platu na bankovní účet
- smlouva o poskytování vzdělávání za úplatu apod.

¹⁷ Janečková, E.: GDPR – Praktická příručka implementace, Wolters Kluwer Praha 2018.