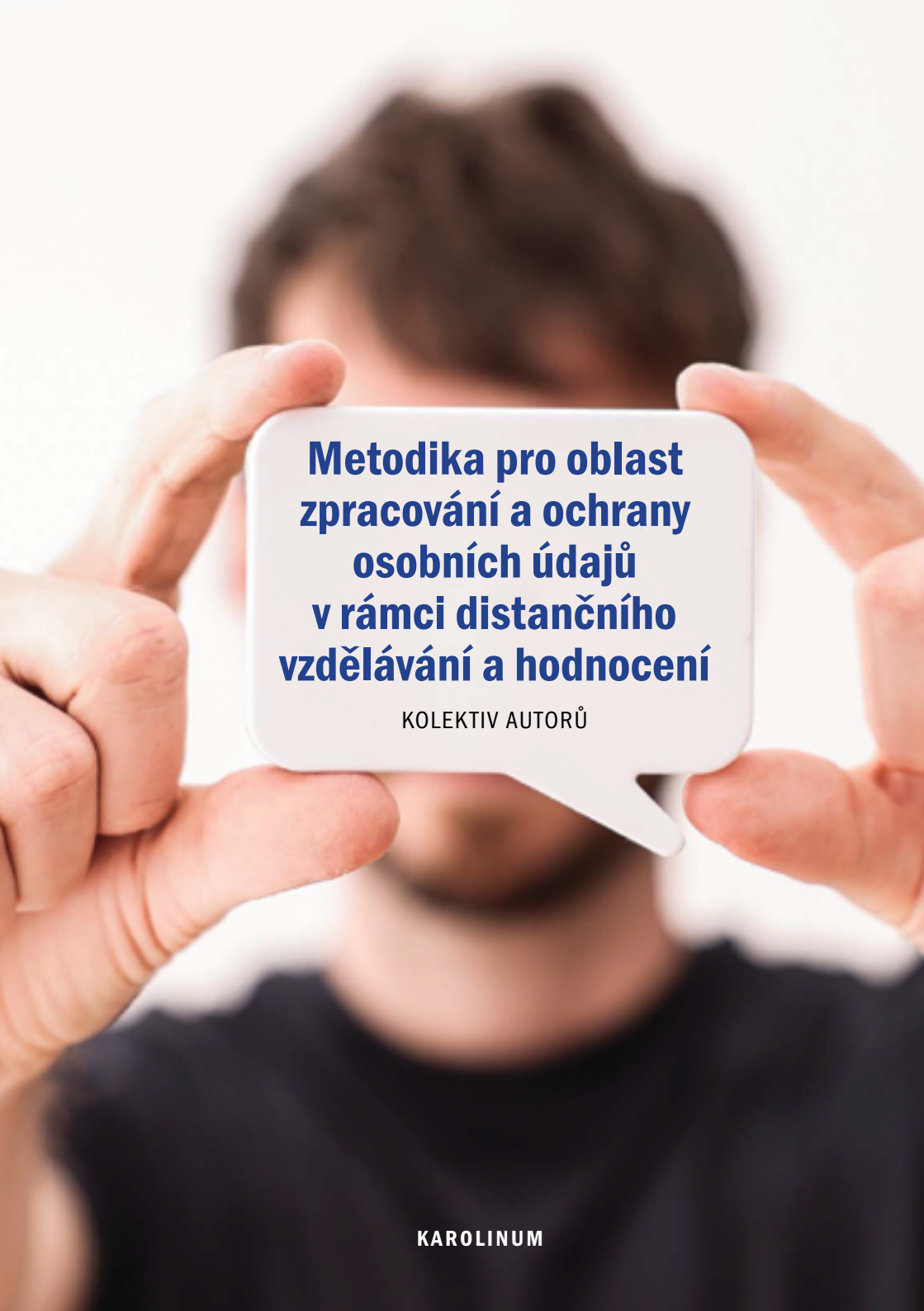

Metodika pro oblast zpracování a ochrany osobních údajů v rámci distančního vzdělávání a hodnocení

KOLEKTIV AUTORŮ

KAROLINUM

METODIKA PRO OBLAST ZPRACOVÁNÍ A OCHRANY OSOBNÍCH ÚDAJŮ V RÁMCI DISTANČNÍHO VZDĚLÁVÁNÍ A HODNOCENÍ

Jan Jindra a kolektiv

———

Autorský kolektiv:
Sabina Březinová (Slezská univerzita v Opavě),
Kateřina Burianová (Jihočeská univerzita v Českých Budějovicích),
Tomáš Cvrček (Univerzita Hradec Králové),
Jan Jindra (Univerzita Karlova),
Karel Nenadál (Vysoká škola ekonomická v Praze),
Martin Pernica (Mendelova univerzita v Brně),
Štěpán Richter (Veterinární univerzita Brno),
Jiří Šafra (Univerzita Pardubice)

Vydala Univerzita Karlova, Nakladatelství Karolinum
Ovocný trh 560/5, 116 36 Praha 1
Praha 2021
Jazyková korektura Václav Hozman
Sazba a grafická úprava DTP Nakladatelství Karolinum
Vydání první

ISBN 978-80-246-5098-2 (online : pdf)

Univerzita Karlova
Nakladatelství Karolinum

www.karolinum.cz
ebooks@karolinum.cz

OBSAH

1

IDENTIFIKACE SUBJEKTŮ ÚDAJŮ V ONLINE PROSTŘEDÍ

Autoři: Jiří Šafra (Univerzita Pardubice),
Kateřina Burianová (Jihočeská univerzita
v Českých Budějovicích)

Úvod

Osobní identifikační údaje jsou údaje, které určují konkrétní fyzickou osobu a odlišují ji od jiných fyzických osob.

Běžně používanou minimální množinou je jméno, příjmení, datum, místo narození a místo trvalého pobytu.

Tyto údaje je možné **získat** různými způsoby, subjekt údajů je může prostým způsobem sdělit, např. vyplněním do elektronické přihlášky ke studiu. Takto sdělené údaje může být zapotřebí **ověřit** ve smyslu jejich existence, tzn., že osoba určená těmito údaji existuje, nebo z hlediska vazby k určité fyzické osobě, to znamená, že osoba, které tyto údaje sděluje, je skutečně osobou, která je těmito údaji určena.

Toto ověření lze provést v zásadě dvěma způsoby:

- kontrolou fyzického dokladu totožnosti, jako je např. občanský průkaz či cestovní pas;
- ověřením elektronické identity.

Kontrolu fyzického dokladu typicky provádí člověk smyslově, tedy „podívá se“ na doklad, přečte na něm uvedené údaje, porovná podobu předkládající osoby s fotografií uvedenou na průkazu, zkontroluje náležitosti dokladu, jako je jeho platnost, bezpečnostní prvky (hologram, 3D prvky, ...), případně si interaktivně vyžádá další informace či doklady. Důležitým prvkem je vlastnictví daného fyzického dokladu. Výsledek ověření je dán **důvěrou kontrolující osoby vůči samotnému dokladu a předkládající osobě**.

Oproti tomu ověření elektronické identity vychází z **důvěry vůči třetí straně**,[1] poskytovateli elektronické identity. Ověřovaná osoba se vůči tomuto poskytovateli prokáže svými autentizačními údaji, kterými jsou typicky uživatelské jméno („kdo je"), heslo („co zná") a běžně již také nějakým dalším faktorem, jako je např. SMS zaslaná na jeho ověřené telefonní číslo, autentizační aplikace v mobilním zařízení, HW zařízením typu token (tedy „co vlastní"). Pokud toto ověření proběhne v pořádku, poskytovatel identity vrátí ověřující straně informace o úspěšném ověření a definovanou množinu údajů.[2]

Výhoda elektronické identity spočívá v tom, že ověření probíhá na straně subjektu k tomu určenému, bez nutnosti přímého zpracování např. biometrických údajů, protože ověření vztahu údajů a osoby je realizováno na jiném principu, než je shoda podoby s fotografií. Dále jsou potřebné údaje získány již v elektronické podobě, a to bez nutnosti zvláštní konverze z obrazových dat (zdrojem je přímo datový zdroj na straně poskytovatele identity) a rizika chyb z nesprávné digitalizace.

U zpracování fyzického dokladu je předpokládána primárně fyzická realizace jeho zpracování – přečtení, vizuální kontrola, případný přepis údajů apod. Může však proběhnout i do určité míry automatizovaně pomocí technologických prostředků, ovšem je zapotřebí digitalizovat fyzickou podobu, zpracovat podobu způsobem, který by mohl být klasifikován jako biometrické zpracování, rozpoznat textové řetězce (OCR), řešit problém případných chyb plynoucích z digitalizace apod.

Rovněž je zapotřebí zmínit, že fyzické doklady často podléhají i legislativní ochraně, která může např. zakazovat pořizování kopií, zakazovat zpracování strojově čitelných údajů, což jsou prvky, které budou při technologickém zpracování typicky prováděné, nebo v těchto případech požadovat získání a případně i prokázání souhlasu se zpracováním osobních údajů od dotyčného subjektu atd.

V úvodní části dalšího textu je uvedena stručná rešerše relevantní legislativy a nelegislativních zdrojů. Následuje souhrn situací, kdy může být online identifikace zapotřebí. Závěrem jsou uvedena doporučení, jak online identifikaci realizovat.

1) Zde je myšleno ztotožňování osob, které ještě organizací ztotožněny nebyly. Po prvotním ztotožnění se předpokládá, že může být dotyčná osoba vybavena interními přihlašovacími údaji, kterými se v dalších situacích prokazuje a při jejichž použití je již pokládána za ztotožněnou.

2) Jde o podobný princip jako u platebních bran, kdy je uživatel z e-shopu přesměrován na stránky zajišťující platbu, kde uživatel zadá údaje pro realizaci platby, a následně se e-shopu vrátí pouze informace o tom, že platba úspěšně proběhla.

Úvodní rešerše

Vybrané termíny

V souvislosti s online identifikací je vhodné definovat některé pojmy, které jsou natolik běžně používané, že jejich definice může být obtížná. Jako zdroj pojmů byl v této kapitole použit **znalostní web Hlavního architekta eGovernmentu**, zejména pak slovník uvedený na adrese https://archi.gov.cz/slovnik_egov. Některé definice však byly pro potřeby tohoto textu zjednodušeny, pro přesná vyjádření je tedy vhodné navštívit uvedené stránky.

Osobní identifikační údaje

- **Soubor údajů umožňujících určit totožnost fyzické** či právnické **osoby** nebo fyzické osoby zastupující právnickou osobu.

Elektronická identifikace

- Postup **používání osobních identifikačních údajů v elektronické podobě**, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu.[3]

Elektronická identita

- Sada vlastností, které jednoznačně určují konkrétní osobu.
- Předpokládá používání osobních identifikačních údajů v elektronické podobě, které jednoznačně identifikují určitou fyzickou osobu.
- Při prokazování totožnosti například občanským průkazem se předkládá určitý soubor informací o osobě, který je na tomto průkazu uveden.
- V online světě se předkládá souhrn informací o osobě v digitální podobě.

Autentizace

- Proces ověření totožnosti, **prokázání, že osoba je skutečně tou identitou, za kterou se prohlašuje** nebo je prohlašována. Jedná se o **poskytnutí záruky, že prohlašovaná charakteristika je správná**.

3) Nařízení EP a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu; čl. 3 odst. 1.

→ Elektronický postup, který umožňuje potvrdit elektronickou identifikaci fyzické či právnické osoby nebo původ a integritu dat v elektronické podobě.[4]

International ID Gateway
→ Způsob uznávání prostředků pro elektronickou identifikaci vydaných v jiném členském státě.

„Fyzický" způsob ověřování

Zákon o občanských průkazech

Původní úprava občanských průkazů byla ukotvena v zákoně č. 328/1999 Sb., o občanských průkazech. Tento zákon byl zrušen k 1. 2. 2022 a v aktuální době (srpen 2021) z něj zbývají pouze dva paragrafy (konkrétně § 17b a § 18d). Tyto paragrafy však nemají zásadní vliv na řešenou problematiku, a tedy zákon č. 328/1999 Sb. lze pokládat z hlediska tohoto textu za bezpředmětný.

Novou právní úpravou občanských průkazů je zákon č. 269/2021 Sb., o občanských průkazech (dále jen „zákon č. 269/2021 Sb." nebo „nový zákon o občanských průkazech"), který je účinný od 2. 8. 2021, s výjimkou několika ustanovení (např. zrušení zákona č. 328/1999 Sb.), které mají účinnost odloženou.

Podle § 2 zákona 269/2021 Sb. je občanský průkaz *veřejnou listinou, kterou držitel občanského průkazu prokazuje svou totožnost a skutečnosti v ní uvedené*.[5]

Údaje uváděné v občanském průkazu se rozlišují na údaje:
→ uváděné v podobě *bezprostředně čitelné nebo vnímatelné člověkem* a
→ údaje uložené ve *strojově čitelné podobě v nosiči dat,*
přičemž § 6 blíže specifikuje, v jaké podobě mají/mohou být jednotlivé údaje uloženy.

Rozsah údajů uváděných na občanském průkaze je specifikován v § 5 nového zákona o občanských průkazech.[6] Z hlediska následujícího textu

4) Nařízení EP a Rady (EU) č. 910/2014 ze dne 23. července 2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu; čl. 3 odst. 5.
5) Dřívější úprava (§ 2 zákona č. 328/1999 Sb.) nehovořila o prokazování *totožnosti*, ale o *prokazování jména, popřípadě jmen, příjmení, podoby a státního občanství České republiky*, jakož *i dalších údajů*.
6) Oproti starému zákonu o občanských průkazech zde není uvedeno rodné číslo a tituly; rodinný stav je uváděn volitelně.

jsou relevantní zejména následující údaje – především z důvodu, že zákon požaduje jejich uvedení vždy v podobě čitelné nebo vnímatelné člověkem:

- jméno, popřípadě jména, a příjmení,
- pohlaví,
- státní občanství,
- datum, místo a okres narození (případně jen kód státu u osob narozených mimo ČR),
- adresa místa trvalého pobytu, je-li držitel občanského průkazu hlášen k trvalému pobytu na území České republiky,
- podoba,
- podpis.

Skutečnosti zapsané v občanském průkazu není občan povinen prokazovat jiným způsobem, pokud tak nestanoví zvláštní právní předpis.

Podle § 39 písm. c) a d) se *zakazuje pořizovat kopii*[7] občanského průkazu bez souhlasu držitele občanského průkazu a *zpracovávat*[8] *údaje uvedené v občanském průkazu a data pro elektronické využití občanského průkazu* bez souhlasu držitele občanského průkazu.

Podobné ustanovení bylo uvedeno i v dřívější právní úpravě, která v § 15 hovořila o potřebě *prokazatelného souhlasu* a dále výslovně upřesňovala, že souhlasem je myšlen souhlas se zpracováním osobních údajů. Přestože v nové úpravě toto upřesnění chybí, lze např. i s ohledem na výkladový materiál ÚOOÚ[9] nadále předpokládat, že je myšlen souhlas se zpracováním osobních údajů.

V dřívější úpravě byl přímo v zákoně specifikován rovněž tzv. *bezpečnostní osobní kód (BOK)*, který měl sloužit k *autentizaci držitele při **fyzickém prokázání** jeho totožnosti*, např. v případech pochybností o shodě podoby držitele s průkazovou fotografií, a *identifikační osobní kód (IOK)*.

V nové právní úpravě byly tyto prvky odstraněny z úrovně zákona, ale možnost jejich uložení je uvedena v § 4 vyhlášky č. 281/2021 Sb., k *provedení zákona o občanských průkazech a některých ustanovení zákona o cestovních dokladech a zákona o základních registrech.*

Využití lze předpokládat spíše v budoucích situacích, kdy budou k dispozici elektronické aplikace pro správu dat, pro ohlašování ztráty nebo elektronickou identifikaci a autentizaci držitele občanského průkazu podle § 41 nového zákona o občanských průkazech.

7) Přestupek podle § 65 odst. 1 písm. d) s možnou pokutou do 10 000 Kč.
8) Porušení ustanovení není uvedeno v § 65 jako přestupek, lze tak předpokládat, že by se porušení řešilo např. podle obecného nařízení o ochraně osobních údajů.
9) K prokazování totožnosti a zpracování osobních údajů. *Úřad pro ochranu osobních údajů* (online), https://www.uoou.cz/.

Zákon o cestovních dokladech

Cestovní doklad je veřejná listina opravňující občana k překračování státních hranic České republiky přes hraniční přechod. Cestovním dokladem občan prokazuje své *jméno, popřípadě jména, příjmení, rodné číslo, podobu, státní občanství* České republiky a další údaje zapsané nebo zpracované v cestovním dokladu podle tohoto zákona.

Rovněž zákon o cestovních dokladech neumožňuje bez souhlasu držitele pořizovat jakýmikoliv prostředky kopie cestovního dokladu (§ 2 odst. 3).

Podle § 6 zákona č. 329/1999 Sb., o cestovních dokladech, jsou povinnými údaji zapisovanými do cestovního dokladu:

- jméno, příjmení,
- rodné číslo,
- pohlaví,
- státní občanství,
- datum a místo narození (u občanů narozených mimo území ČR pouze kód státu).

Dalšími údaji mohou být fotografie, otisky prstů rukou aj. Tyto slouží výhradně k ověřování pravosti cestovního dokladu a ověření totožnosti občana. Tyto údaje však nemusí obsahovat všechny typy cestovních dokladů, např. § 6 odst. 2 stanoví, že se jedná o doklady vydávané s dobou platnosti delší než 1 rok.

Další zákony o prokázání totožnosti

Zákon o Policii ČR

Např. podle § 63 zákona č. 273/2008 Sb., o Policii ČR, se prokázáním totožnosti rozumí *prokázání jména, popřípadě jmen, příjmení, data narození a v případě potřeby také adresy místa trvalého pobytu, adresy místa pobytu nebo adresy bydliště v zahraničí, rodného čísla a státní příslušnosti*. Zároveň rozsah a způsob zjišťování osobních údajů musí být přiměřené účelu zjišťování totožnosti.

Zákon o opatření proti legalizaci výnosů z trestné činnosti a financování terorismu

Podle § 8 odst. 2 zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu při identifikaci fyzické osoby[10] se ověřují identifikační údaje z průkazu totožnosti

10) Jedná se o velmi specifickou úpravu, směřovanou spíše do komerčního sektoru, zde je uvedena spíše pro ilustraci, v jakém rozsahu osobních údajů může být ověření totožnosti realizováno.

a *současně ověří shodou podoby s vyobrazením v průkazu totožnosti*. Průkazem totožnosti se podle § 4 odst. 6 rozumí *doklad vydaný orgánem veřejné správy, v němž je uvedeno jméno a příjmení, datum narození a z něhož je patrná podoba, popřípadě i jiný údaj umožňující identifikovat osobu, která doklad předkládá, jako jeho oprávněného držitele*. Identifikačními údaji se podle § 5 odst. 1 písm. a) rozumí *všechna jména a příjmení, rodné číslo, a nebylo-li přiděleno, datum narození a pohlaví, dále místo narození, trvalý nebo jiný pobyt a státní občanství*.

„Elektronický“ způsob

Zákon o právu na digitální služby

Uživatel služby má právo činit digitální úkon vůči orgánu veřejné moci prostřednictvím např.:
- datové schránky,
- ISVS[11] umožňujícího prokázání totožnosti uživatele s využitím elektronické identifikace.

Zákon č. 12/2020 Sb., o právu na digitální služby v § 4 uvádí:

(1) ***Uživatel služby má právo činit digitální úkon vůči orgánu veřejné moci prostřednictvím***
- *a) své datové schránky,*
- *b) kontaktního místa veřejné správy v případě digitálního úkonu, o kterém tak stanoví prováděcí právní předpis,*
- *c) sítě elektronických komunikací dokumentem podepsaným uznávaným elektronickým podpisem nebo opatřeným uznávanou elektronickou pečetí za podmínek stanovených jinými zákony,*
- *d)* ***informačního systému veřejné správy umožňujícího prokázání totožnosti uživatele služby s využitím elektronické identifikace****, autorizaci digitálního úkonu uživatelem služby a zpětné prokázání projevu vůle uživatele služby učinit digitální úkon, nebo*
- *e) jiného způsobu, pokud tak stanoví právní předpis.*

Zákon o elektronické identifikaci

Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze **prostřednictvím kvalifikovaného systému elektronické identifikace** (dále jen „kvalifikovaný systém“).

11) Informační systém veřejné správy podle zákona č. 365/2000 Sb.

Zákon č. 250/2017 Sb., o elektronické identifikaci v § 2 uvádí:
§ 2 Prokázání totožnosti s využitím elektronické identifikace
*Vyžaduje-li právní předpis nebo **výkon působnosti** prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím **kvalifikovaného systému elektronické identifikace** (dále jen „kvalifikovaný systém“).*

Ověřování údajů

Identifikaci lze chápat jako zjištění osobních identifikačních údajů, které jedinečně identifikují určitou fyzickou osobu.

Pro definici rozsahu osobních údajů, které určitou fyzickou osobu určují, lze vyjít z § 3019 Občanského zákoníku (zákon č. 89/2012 Sb.), který stanoví, že:

Údaji, podle nichž lze člověka zjistit, jsou zejména jméno, bydliště a datum narození, popřípadě identifikující údaj podle jiného právního předpisu. Identifikujícím údajem právnické osoby nebo podnikatele je identifikační číslo osoby, bylo-li jim přiděleno.

S ohledem na demonstrativnost uvedeného ustanovení může být vhodné analyzovat přístup různých portálů veřejné správy, při jejichž analýze lze dojít k následující množině údajů:
1. jméno/jména a příjmení (např. PO, DIS),[12]
2. datum narození (např. PO, DIS),
3. místo narození (např. PO),
4. adresa pobytu (např. PO, DIS),
5. rodné číslo, bylo-li přiděleno,
6. státní občanství.

V kontextu VVŠ lze vyjít např. z § 50 odst. 1 zákona č. 111/1998 Sb., o vysokých školách, ve znění pozdějších předpisů (dále jen „ZoVŠ“), který definuje odlišnou množinu údajů pro občany ČR a pro cizí státní příslušníky. U občanů ČR předpokládá tyto údaje:
1. jméno/jména a příjmení,
2. rodné číslo, bylo-li přiděleno,
3. adresa místa trvalého pobytu na území ČR, popř. bydliště mimo území ČR.

U cizích státních příslušníků pak dále předpokládá uvedení:
4. datum narození,
5. pohlaví,

12) PO = portál občana, DIS = daňová informační schránka.

6. bydliště v ČR,
7. státní občanství.

Je otázka, zda zjišťovat i další údaje, jako číslo OP/pasu apod. Toto pravděpodobně není nezbytné, s výjimkou situací, kdy by bylo zapotřebí provádět ověření vůči nějaké databázi neplatných dokladů (např. https://aplikace.mvcr.cz/neplatne-doklady/). S ohledem na to, že se jedná o údaje nad rámec uvedené legislativy však může být problematické nalezení vhodného právního základu, a jejich zjišťování a zpracování tak nelze příliš doporučit.

Tyto údaje mohou být identifikovanou osobou pouze „sděleny" (např. v přihlášce ke studiu). Za určitých okolností však samotné zjištění osobních identifikačních údajů nemusí být dostatečné, může být zapotřebí ověřit sdělené údaje vůči dalšímu zdroji.

Toto ověření může proběhnout vůči fyzickému dokladu totožnosti nebo mohou být ověřeny elektronickým způsobem. U elektronického způsobu se předpokládá schopnost uživatele ověřit svou totožnost pomocí autentizačních údajů (znalostí hesla, vlastnictvím druhého faktoru apod.).

V případě fyzických dokladů se vychází z vlastnictví průkazu a ze shody fotografie. V případně občanských průkazů existuje ještě možnost prokázání BOK, která však vyžaduje speciální HW zařízení a pravděpodobně není využitelná mimo státní orgány.

V případě fyzických dokladů ještě může hrát roli kontrola bezpečnostních prvků proti falšování, jako jsou hologramy, číslo průkazu, vyznačená platnost.

Situace vyžadující ověření

Před studiem

→ **Úkony při přijímací řízení**

V rámci přijímacího řízení může být vyžadováno vykonání testů, talentových zkoušek apod. Již ve chvíli, kdy je uchazeč skládá, by mělo být jisté, že je skládá opravdu on. Při prezenčních zkouškách ověření totožnosti probíhá standardním způsobem, v případě distančního konání však univerzita nemá k dispozici ani fotku uchazeče, pouze jím uvedené údaje.

Kontrolující může samozřejmě nabýt v případě prezenčního i distančního konání zkoušky odůvodněné pochybnosti, zda osoba, která se průkazem prokazuje, je skutečně oprávněným držitelem průkazu.[13]

13) Např. v případě, že osoba má k dispozici doklad staršího data, na kterém její podoba nemusí odpovídat současnosti.

V takovém případě je navrhováno vyžádat si od konkrétní osoby další doklad prokazující její totožnost.[14]

→ **Zápis do studia**
Zápis do studia definuje § 51 ZoVŠ.

§ 51 Zápis do studia
(1) Sdělením rozhodnutí o přijetí ke studiu vzniká uchazeči právo na zápis do studia. Uchazeči se zapisují ve lhůtě stanovené vysokou školou nebo její součástí.
(2) Zápis se koná na vysoké škole nebo její součásti, která uskutečňuje příslušný studijní program.

Přesunem aktu zápisu do online prostoru dojde pravděpodobně (byť ne nezbytně) k přechodu ze „synchronního" režimu zápisu do „asynchronního". Zatímco standardně zápis probíhá v určitý den, v režimu online může proběhnout i dříve, nebo dokonce i v určitém časovém intervalu. To je zapotřebí zohlednit v samotném procesu, kdy referent studijního oddělení a zapisovaný nemusí sedět u PC ve stejném okamžiku.

V průběhu studia

→ **Online komunikace, asynchronní komunikace, e-learningové systémy**
V průběhu studia typicky již byla osoba ztotožněna a byly jí přiděleny univerzitní přístupové údaje, nad jejichž správou má univerzita kontrolu a jsou pro ni tak důvěryhodné.
V průběhu studia je tak možné na tyto autentizační údaje spoléhat a vyžadovat je, např. při komunikaci prostřednictvím školního e-mailu, studijního informačního systému, přihlašování se do komunikačních nástrojů apod.

→ **Provozní potřeby**
Mohou však nastat situace, kdy univerzitní přístupové údaje k dispozici nejsou. Typicky se bude jednat o situace, kdy např. dojde k exspiraci hesla nebo jeho zablokování. V takovém případě je zapotřebí obnovu údajů provést způsobem, který neumožní zneužití procesu obnovy hesla neoprávněnou osobou.
Možností je samozřejmě fyzická návštěva dotyčné osoby. Rovněž je možné mít k dispozici ověřené jiné kontaktní údaje (např. číslo mobilního telefonu), které je možné využít. To však vyžaduje jejich získání

14) U studentů, kteří konají zkoušku do navazujícího nebo další studia může být takovým dokladem např. i průkaz studenta.

ještě před samotnou potřebou a zároveň se jedná o údaje, které budou zpracovávané pravděpodobně na základě souhlasu se zpracováním osobních údajů.

Po skončení studia
Po skončení studia může být zapotřebí ověřovat různé požadavky na potvrzování studia, vystavování kopií diplomů apod. S tím souvisí širší problematika komunikace po skončení studia, kdy již autentizační údaje přidělované univerzitou nejsou aktivní.

To může být řešeno například formou různých absolventských programů, kde absolvent po ověření totožnosti získá nové autentizační údaje, prostřednictvím kterých pak může se školou dále komunikovat.

Ověření totožnosti v rámci registrace do absolventského programu lze realizovat ještě v čase studia, případně využít autentizace prostřednictvím služeb jiných organizací (např. Česká pošta a doporučení do vlastních rukou) a/nebo pomocí systémů elektronické identifikace.

Doporučení pro oblast ochrany osobních údajů

Vždy je nezbytné si určit, v jakém okamžiku je **nejpozději** nezbytné totožnost osoby ověřit.

Vždy je nezbytné předem definovat, zda je zapotřebí **získat** osobní identifikační údaje, nebo zda je zapotřebí je **ověřit** ve vztahu k fyzické osobě (nebo obojí).

Vždy je nezbytné přesně definovat, jaké **konkrétní údaje** je zapotřebí **získat a** jaké konkrétní údaje je zapotřebí **ověřit**. Nemusí to být totožná množina osobních údajů.

Je zapotřebí určit, **jakým způsobem** má ověření proběhnout, vůči čemu mají být údaje ověřeny. Pokud mají být ověřeny elektronicky, tak vůči jakému poskytovateli (pokud se nejedná o ověření vůči vlastní evidenci).

Pokud má distanční ověření identity proběhnout kontrolou fyzického dokladu, pak určit v jakém režimu, zda bude provádět pracovník v rámci online schůzky nebo informační systém v asynchronním režimu.

Pokud má kontrola fyzického dokladu probíhat v rámci online schůzky, je nezbytné zajistit, aby při kontrole nebyla přítomná jiná osoba, než kontrolovaná a kontrolující. To lze zajistit například vytvořením samostatné privátní schůzky.

Pokud má kontrola fyzického dokladu probíhat prostřednictvím informačního systému, je zapotřebí definovat dobu, po kterou bude digitalizovaná podoba dokladu uchovaná. Může dojít k okamžitému smazání po proběhnutí porovnání podob a OCR textových údajů. V případě asynchronních procesů však může být tato doba delší.

Je zapotřebí rovněž pamatovat na skutečnost, že *subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká* (čl. 22 odst. 1 Obecného nařízení). Čl. 22 sice v dalších odstavcích upravuje situaci, kdy je zpracování založeno na souhlasu se zpracováním osobních údajů, ale zároveň vyžaduje přijetí vhodných opatření. Tedy **možnost napadnout** výsledek a vyžádat si lidský zásah ze strany správce by měla být implementována.

K tomu může být samozřejmě zapotřebí definovat delší dobu uchování digitalizované podoby dokladů.

V případě distanční kontroly totožnosti prostřednictvím občanského průkazu nebo pasu vydávaného na území ČR je zapotřebí předem zajistit **souhlas se zpracováním osobních údajů**. Tato potřeba vyplývá z národní legislativy.[15]

V případě distanční kontroly totožnosti na základě fyzického dokladu prostřednictvím informačního systému je zapotřebí předem zajistit **výslovný souhlas se zpracováním zvláštní kategorie osobních údajů**. Toto se týká případů, kdy má dojít k automatickému ověření shody podoby s fotografií, které bude s největší pravděpodobností implementovat algoritmy biometrického zpracování podoby.

Oba souhlasy by měly být uděleny prokazatelně a informovaně. Jako minimální opatření lze doporučit zaslání textu souhlasů na e-mailovou adresu dotyčného, pro další zvýšení prokazatelnosti (nad rámec zpochybnitelného prostého zaškrtnutí checkboxu) pak může být implementován *double opt-in* formou připojeného odkazu.

V příloze č. 1 je pro inspiraci uvedena část souhlasu, který pokrývá obě výše uvedené potřeby.

V případech, kdy bude zpracování založeno alespoň na jednom souhlasu, je zapotřebí co nejvíce **posílit dobrovolnost tohoto souhlasu**, protože typicky bude vztah se subjektem údajů nerovnovážný, přičemž subjekt údajů bude slabší stranou. K posílení dobrovolnosti přispěje i poskytnutí plnohodnotné alternativy daného procesu, která nebude závislá na udělení souhlasu. Například v případě elektronického zápisu je touto alternativou možnost prezenčního zápisu.

15) Týká se jak kontroly prováděné pracovníkem, tak kontroly založené na informačním systému.

Tato možnost by měla časově následovat **po** době, ve které je možné úkon provést elektronicky. Zároveň by měla být umožněna i těm, u kterých elektronická formace z libovolného důvodu neproběhla nebo neproběhla úspěšně. V neposlední řadě je zapotřebí pamatovat i na odvolatelnost souhlasu, a i v případě odvolání souhlasu by měla být subjektu údajů tato alternativa nabídnuta.

Přestože strojové zpracování fyzických dokladů může svádět k „vytěžení" dalších informací, je vhodné se tohoto vyvarovat, a omezit se pouze na ověření údajů, ke kterým bezpečně existuje právní základ a které byly zadány dříve v rámci procesu, do kterého je ověření zapojeno. Pouze lze uvažovat o strojovém přečtení údajů, které by subjekt údajů tak jako ručně vyplňoval.

Pokud je možné se ověření totožnosti prostřednictvím fyzických dokladů vyhnout, jedná se o bezpečnější variantu. Například v situaci, kdy byla fyzická osoba již dříve ověřena a byly jí přiděleny autentizační údaje (jméno, heslo, ...) v rámci dané školy a tyto údaje jsou stále aktivní, je vhodnější pro ověření používat tyto údaje.

V případě ČR a vybraných zemí EU je vhodnější variantou implementovat ověřování elektronické identity prostřednictvím státem vydávaných nebo alespoň uznávaných prostředků, jako jsou např. datové schránky, bankovní identity, systém *Moje ID*, nebo *International ID Gateway*.

Pokud je možné realizovat nějaký proces elektronicky, měla by tato možnost být dostupná všem, aby nebylo případné dělení chápáno jako diskriminační. Tedy subjekty údajů by neměly být děleny na skupinu, která se může ztotožnit elektronicky, a na skupinu, která musí přijít fyzicky.

Lze však subjekty rozdělit na skupiny, u kterých se bude lišit způsob provedení elektronické identifikace.

PŘÍLOHA Č. 1 – VZOROVÉ ZNĚNÍ SOUHLASU SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

V rámci této přílohy není předkládáno kompletní znění souhlasu. Lze vycházet z toho, že některé náležitosti souhlasu jsou do značné míry generické a každá škola má vlastní vzory, které využívá.

Většina souhlasů definovaných na dané škole se pak liší ve třech bodech, a to „Osobní údaje", „Účel zpracování údajů" a „Doba uchování". Níže uvádíme vzorové texty pro tyto součásti souhlasu se zpracováním osobních údajů, které je možné využít pro inspiraci při přípravě vlastních souhlasů.

Osobní údaje

Osobními údaji, s jejichž zpracováním dává subjekt údajů souhlas, **jsou následující údaje uvedené na průkazu totožnosti** (občanský průkaz, cestovní pas):

- **identifikační údaje** (jméno, popř. jména, příjmení, datum narození, státní příslušnost, rodné číslo, je-li uvedeno),
- **kontaktní údaje** (místo trvalého pobytu),
- **další údaje z průkazu totožnosti** (doba platnosti průkazu),
- **dočasná obrazová kopie průkazu**.

Osobním údajem, který spadá do **zvláštní kategorie osobních údajů**, s jehož zpracováním dává subjekt údajů **výslovný souhlas**, je jeho **podoba**, kterou vyfotí v rámci aplikace pro ztotožnění, a fotografie uvedená na průkazu totožnosti, vůči které je podoba porovnávána s využitím prvků biometrie.

Účel zpracování údajů

Účelem zpracování osobních údajů je ověření totožnosti v rámci **zápisu ke studiu**, na který subjektu údajů vzniklo právo sdělením rozhodnutí o přijetí ke studiu v příslušném studijním programu, a kontrola údajů, které subjekt údajů vyplnil v přihlášce ke studiu.

Účelem biometrického zpracování je pak vyhodnocení shody podoby ztotožňované osoby s fotografií na použitém dokladu totožnosti za účelem ověření, že průkaz předkládá jeho skutečný držitel.

Doba zpracování osobních údajů

Univerzita zpracovává osobní údaje podle tohoto souhlasu jen po dobu nezbytně nutnou k ověření totožnosti v rámci zápisu ke studiu. Tato doba je dána okamžikem úspěšně realizovaného ověření totožnosti. V případě neúspěšně realizovaného ověření totožnosti je pak dána okamžikem, kdy je neúspěšnost ztotožnění potvrzena zaměstnancem univerzity, nejpozději však 14. dnem po neúspěšně realizovaném ověření totožnosti.

2

ZAJIŠTĚNÍ VEŘEJNOSTI U STÁTNÍ ZKOUŠKY Z POHLEDU GDPR

Autoři: Sabina Březinová (Slezská univerzita v Opavě),
Jiří Šafra (Univerzita Pardubice)

Obecná ustanovení

Právní základ

„Veřejnost" u státní zkoušky upravuje zákon o vysokých školách takto:

1. V § 53 odst. 1, kde je uvedeno, že státní zkouška se koná před zkušební komisí; průběh státní zkoušky a vyhlášení výsledku jsou veřejné.
2. V § 95c odst. 1 písm. c), kde je uvedeno, že pokud z důvodu krizového opatření vyhlášeného podle krizového zákona nebo z důvodu nařízení mimořádného opatření podle zvláštního zákona není možná nebo je omezena osobní přítomnost studentů na vzdělávání nebo zkouškách anebo účastníků na státní rigorózní zkoušce, a pokud ministerstvo školství, popřípadě ministerstvo obrany nebo ministerstvo vnitra vůči příslušné státní vysoké škole toto svým rozhodnutím umožní, může vysoká škola využívat při státní zkoušce nástroje distančního způsobu komunikace a konat ji bez přítomnosti veřejnosti za předpokladu, že z jejího průběhu pořídí audiovizuální záznam, který uchová po dobu 5 let; záznam vysoká škola poskytne pouze orgánu veřejné moci při výkonu jeho pravomocí, a to na jeho žádost.

Vzhledem k tomu, že Ministerstvo školství, mládeže a tělovýchovy ČR vydalo pro všechny veřejné vysoké školy rozhodnutí o zvláštních oprávněních při mimořádné situaci, které bylo účinné do 30. 9. 2021, bylo v uvedené době možné použít § 95c odst. 1 písm. c) o distančním způsobu konání státní zkoušky bez přítomnosti veřejnost.

Definice veřejnosti

Veřejnost je velmi obecný pojem. Veřejností se rozumí všichni lidé bez ohledu na věk, pohlaví, rasu, společenské nebo jiné postavení. Pojem veřejnost je také používán v různých právních předpisech, ovšem obecnou definici tohoto pojmu nelze najít v žádném z nich. Proto pro účely této metodiky bude používán pojem veřejnost v širokém smyslu slova jako společenství osob bez ohledu na jakékoli rozdíly, které v rámci populace existují (tj. věk, národnost, rasa, pohlaví, vyznání, atd.).

Pojem veřejnost by však bylo možné chápat také nikoli ve smyslu skupiny osob, ale i ve smyslu atributu průběhu státní zkoušky.

V případě citované legislativy lze vnímat určité riziko související s výkladem tohoto pojmu vzhledem k tomu, že výše uvedené paragrafy zákona o vysokých školách používají odlišnou terminologii. Ustanovení § 53 hovoří o tom, že „průběh je veřejný", zatímco ustanovení § 95c hovoří o „nepřítomnosti veřejnosti". Není zřejmé, zda se z hlediska zákonodárce jedná pouze o synonymní vyjádření, nebo zda v rámci legislativního procesu vnímal určité významové rozdíly a z toho důvodu volil i jinou formulaci.

Zmiňované riziko spočívá v tom, že pokud by se nejednalo o vyjádření téhož, pak by např. níže diskutovaným zveřejněním odkazu na online schůzku mohla být sice zajištěna veřejnost ve smyslu atributu průběhu státní zkoušky, ale nemusela by tím být zajištěna i přítomnost veřejnosti.

V případě výkladu, že jsou oba pojmy shodné, by mohlo dojít v případě online zkoušky se zveřejněným odkazem k tomu, že by nebyl pořízen záznam. Pokud by však z následné judikatury vyplynul opak, tedy že zveřejněním odkazu pro připojení k online schůzce není automaticky naplněn požadavek přítomnosti veřejnosti, mohlo by být nepořízení záznamu hodnoceno jako pochybení. Tyto skutečnosti je tedy nutné akcentovat při úvaze, jakou formou a jakým způsobem bude veřejnost u státní zkoušky zajišťována.

Způsoby konání státní zkoušky z hlediska veřejnosti

Pro základní rozlišení jednotlivých možností bylo navrženo následující rozdělení:

1. za přítomnosti veřejnosti:
   a) osobní,
   b) distanční,
2. bez přítomnosti veřejnosti.

1a) Konání státní zkoušky za osobní přítomnosti veřejnosti
Státní zkouška proběhne se zachováním zásady veřejnosti, tedy bez nahrávání. Taková osobní přítomnost veřejnosti může být zajištěna:

- Možností osobní účasti na státní zkoušce. Veřejnost se v tomto případě bude nacházet ve stejné místnosti, v níž se státní zkouška skládá (za dodržení všech ostatních pravidel, např. hygienických, ohledně maximálního počtu osob v místnosti atd.). V tomto případě není možné bez dalšího státní zkoušku nahrávat.
- Možností osobní účasti na státní zkoušce, a to v jiné k tomu vyhrazené místnosti. Veřejnost se v tomto případě bude nacházet ve stejné nebo např. přilehlé budově, ale v jiné místnosti, než se skládá státní zkouška, ale kam bude zároveň pořizován audiovizuální přenos státní zkoušky. Informace o tomto způsobu účasti veřejnosti na státní zkoušce by měla být sdělena vhodným způsobem před začátkem státní zkoušky a to nejlépe stejnou formou jako sdělení o konání termínu státní zkoušky. Zároveň je možné zajistit (příslušnou pověřenou osobou kontrolu v místnosti), že ze státní zkoušky nikdo nepořizuje neoprávněně záznam (audio, video), který by mohl být následně např. umístěn na sociální sítě či jinak zneužit.

Zde je možné spatřovat riziko ve výkladu pojmu „nástroj distančního způsobu komunikace" použitého v § 95c odst. 1 písm. c) zákona. Pokud by distančním způsobem komunikace byla chápána jakákoli situace, kdy dochází k přenosu obrazu a zvuku mezi dvěma (byť blízkými) místy s využitím technických prostředků (kamery, obrazovky, datové kabely, …), pak by byla naplněna první část věty § 95c odst. 1 písm. c), podle kterého může vysoká škola:

- *„**využívat** při státní zkoušce **nástroje distančního způsobu komunikace** a konat ji bez přítomnosti veřejnosti za předpokladu, že z jejího průběhu*

pořídí audiovizuální záznam, který uchová po dobu 5 let; záznam vysoká škola poskytne pouze orgánu veřejné moci při výkonu jeho pravomocí, a to na jeho žádost."

Pokud by zároveň spojka „a" mezi první a druhou větou nebyla chápána ve smyslu „a zároveň", mohlo by to znamenat, že záznam má být pořízen.

S ohledem na uvedené riziko lze doporučit, aby každá instituce, která se tímto způsobem rozhodne státní zkoušku realizovat, zvážila uvedené riziko a podle toho buď záznam průběhu zkoušky pořídila, nebo nepořídila.

1b) Konání státní zkoušky za tzv. distanční přítomnosti veřejnosti

Veřejnost bude u státní zkoušky zajištěna zveřejněním, a tedy možností veřejnosti účastnit se státní zkoušky, prostřednictvím předem vytvořeného odkazu/linku na videokonferenci (na virtuální místnost), kde se státní zkouška koná. Technické prostředky k připojení si musí veřejnost zajistit sama, mělo by se však jednat o snadno či běžně dostupné prostředky. Není tedy vhodné volit takové platformy, které by byly i pro koncové uživatele placené, které by vyžadovaly pořízení specializovaného hardwarového vybavení apod. Většina běžně používaných platforem (např. MS Teams, Google Meet, apod.) tento požadavek bude splňovat.

Odkaz/link na videokonferenci musí být sdělen veřejnosti na vhodném místě, tzn. nejlépe stejnou formou jako sdělení o konání termínu státní zkoušky.

Lze doporučit, aby forma sdělení odkazu nebyla zbytečně „obstrukční". Odkaz na online schůzku může být poměrně dlouhý a složitý a v případě vytisknutí a vyvěšení na úřední desce sice bude formálně zveřejněn, ale jeho rozumné použití bude velmi omezené. Zájemce by odkaz musel přepsat zcela bez chyby. Je tedy vhodné zvážit použití QR kódu, využití zkracovače URL apod.

Rovněž i zde je zapotřebí důsledně zvážit rizika plynoucí z nejasného výkladu pojmů „veřejnost" a „přítomnost veřejnosti" a ze skutečnosti, že se jedná o použití nástrojů distanční komunikace a na základě toho rozhodnout o případném (ne)nahrávání SZZ.

2) Konání státní zkoušky bez přítomnosti veřejnosti

Pokud se státní zkouška koná prostřednictvím nástroje distančního způsobu komunikace, lze konat státní zkoušku bez účasti veřejnosti za předpokladu, že průběh státní zkoušky bude nahráván. V zákoně o vysokých školách je uvedeno, že musí být pořízen audiovizuální záznam, který se uchová po dobu 5 let. Tento záznam může být poskytnut pouze orgánům veřejné moci na jejich žádost. Tuto žádost o nahlédnutí je třeba uchovávat společně se záznamem.

V tomto případě, tedy při pořizování audiovizuálního záznamu státní zkoušky není nutné zajištění účasti veřejnosti.

Při nahrávání státní zkoušky je povinnost nahrát všechny části zkoušky, tzn. teoretickou i praktickou část, pokud je součástí státní zkoušky.

Rizika a upozornění z hlediska GDPR

Některá rizika plynoucí z legislativní úpravy byla prezentovaná v předchozím textu. **V případě varianty 1b) za tzv. distanční přítomnosti veřejnosti u státní zkoušky lze z pohledu GDPR spatřovat i další následující rizika.**

V případě přihlášení většího množství osob k videokonferenčnímu hovoru mohou vznikat vyšší nároky na technické zajištění videohovoru (kvalita hovoru, rychlost přenosu), které může v důsledku znamenat riziko nezajištění veřejnosti u státní zkoušky.

Jako riziko může být vnímána i možnost nahrávání státní zkoušky další osobou a následné sdílení na sociálních sítích nebo webových stránkách bez možnosti dohledat administrátora nebo osobu, která záznam/odkaz vložila.

Pořízení záznamu jinou připojenou osobou pravděpodobně nelze a priori zakázat, protože není možné spolehlivě vyloučit odvolání se dotyčného na ustanovení nějakého dalšího obecně závazného právního předpisu. Zároveň případnému pořízení záznamu nelze ani technologicky zamezit.

V případě pořízení záznamu jinou osobou by se mohla tato osoba stát správcem osobních údajů (pokud by se např. nejednalo o výlučně osobní činnost, viz čl. 2 odst. 2 písm. c) Obecného nařízení) a v takovém případě by bylo její povinností identifikovat právní základ, na jehož základě tak bude činit. Je možné, že by tímto základem mohl být souhlas se zpracováním osobních údajů, který by tato jiná osoba musela získat, ale rovněž si lze představit i jiné právní základy (např. veřejný zájem, oprávněný zájem apod.). Vyhodnocení, které by musela provést tato jiná osoba, a stejně tak i případná informační povinnost, by byla na její straně.

Určité riziko lze i tak spatřovat v tom, že vysoká škola je tím, kdo online přenos zrealizoval a vznik podobné nahrávky umožnil, a nelze tedy vyloučit ani její odpovědnost, pokud by toto zveřejnění bylo shledáno jako neoprávněné nebo rozsah zveřejněného průběhu jako nepřiměřený.

Současně by mohlo dojít i k situaci, kdy by škola záznam nepořídila a nedokázala by se pak bránit hypotetickému, tendenčně sestříhanému záznamu, který pořídila jiná osoba.

Vhodná upozornění pro veřejnost v případě 1b), tedy u tzv. distanční přítomnosti veřejnosti u státní zkoušky:

- Informovat, že prokazování totožnosti studenta a hlasování zkušební komise probíhá bez účasti veřejnosti; zároveň je nezbytné technicky zajistit, aby tomu tak skutečně bylo – ověření totožnosti provádět takovým způsobem, aby bylo zřejmé, že k identifikaci došlo, ale identifikační prostředky a osobní údaje na nich uvedené nebyly zobrazeny veřejnosti, o výsledku kontroly by mělo proběhnout základní oznámení apod.

Upozornění/informace pro veřejnost je třeba umístit před začátkem státní zkoušky, a to na místech (odkazech), které jsou k tomu vhodné.

Upozornění pro studenta ohledně veřejnosti státní zkoušky:

- Informovat studenta ohledně způsobu zajištění veřejnosti jeho státní zkoušky – tzn., že byl na webové stránky umístěn veřejně přístupný odkaz na videokonferenci, příp. že veřejnost se účastní v jiné místnosti a dochází k videokonferenčnímu přenosu, NEBO
- informovat studenta o nahrávání státní zkoušky.

Závěrečné doporučení

Na základě výše uvedeného rozboru a s přihlédnutím k identifikovaným rizikům se jako nejbezpečnější jeví buď standardní prezenční způsob konání státní zkoušky, nebo online způsob konání státní zkoušky bez přítomnosti veřejnosti s pořízením oficiálního záznamu, nad kterým má vysoká škola plnou kontrolu. Byť ani tím není možnost vzniku dalšího záznamu zcela eliminována (záznam může pořídit např. zkoušená osoba), bude mít v případě sporu založeném na hypoteticky tendenčně upraveném neoficiálním záznamu škola k dispozici důkazní materiál vypovídající o skutečném průběhu.

Další přednesené způsoby konání jsou jistě možné, ale již zde existují určitá rizika, která byla uvedena v předchozích kapitolách a která si každá vysoká škola musí vyhodnotit.

3

NAHRÁVÁNÍ, UKLÁDÁNÍ A ZVEŘEJŇOVÁNÍ AUDIOVIZUÁLNÍCH ZÁZNAMŮ (NÁSTROJE, DOBA ULOŽENÍ A ÚLOŽIŠTĚ)

Autor: Tomáš Cvrček (Univerzita Hradec Králové)

Úvod

V souvislosti s distančním způsobem plnění studijních povinností se nabízí otázka, jak je to s pořizováním, uchovávání, případně zveřejňováním audiovizuálních záznamů (dále jen „AVZ“) vysokými školami z průběhu plnění těchto studijních povinností, zejm. pak zkoušek a státních závěrečných zkoušek, a to jak bakalářských a magisterských, tak doktorských studijních programů.

Tato kapitola pak nabízí návrh možného řešení předestřené otázky, a to jak z pohledu teoretického (právní základ), tak z pohledu praktického (nástroje pro uchovávání).

Právní předpoklady pro zpracování

Pořizování a další způsoby zpracování AVZ z průběhu plnění studijních povinností distančním způsobem by mělo být možné pouze při splnění určitých legislativních předpokladů. Předně platí zásada, že zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.[16] Není tedy

16) § 84 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

možné pořizovat AVZ bez toho, aniž by o tom student, popř. zkoušející, člen zkušební komise apod., věděl a alespoň konkludentně[17] k tomu nedal svolení.

Je sice pravdou, že z uvedené zásady platí výjimka, kdy svolení není třeba, pokud se AVZ pořizuje nebo používá k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob, případně pokud se AVZ pořizuje nebo používá na základě zákona k úřednímu účelu, nicméně s ohledem na skutečnost, že pořizováním a používáním AVZ se vstupuje do sféry ochrany osobnosti v AVZ zachycovaných osob, lze doporučit tyto výjimky s ohledem na minimalizaci takového zásahu spíše nepoužívat a postupovat v souladu se shora uvedenou zásadou, tedy pokud kterákoli ze zaznamenávaných osob vyjádří protest proti pořízení AVZ, tento nepořizovat a postupovat jiným dostupným způsobem, např. standardním prezenčním plněním dané studijní povinnosti.

Z hlediska ochrany osobních údajů (jakékoli informace o osobách zachycených v AVZ) by si pak každá vysoká škola měla stanovit právní základ pro pořizování, uchovávání, případně zveřejňování či jiné používání (obecně zpracování) AVZ, účel takového zpracování, dobu uchovávání AVZ, technická nebo organizační opatření proti neoprávněným či protiprávním způsobům zpracování a proti náhodné ztrátě, zničení nebo poškození AVZ, tyto informace vést v záznamech o činnostech zpracování[18] a o podstatných bodech těchto skutečností rovněž informovat dotčené osoby.[19]

Z hlediska účelu pořizování a uchovávání AVZ z distančního plnění studijních povinností se jako legitimní účel[20] zpracování nabízí následná kontrola řádného plnění dané studijní povinnosti (zejm. zkoušky a státní závěrečné zkoušky) a zajištění rovného přístupu studentů ke studiu (tj. včetně plnění studijních povinností), kdy v případě, že je určitému studentovi umožněno konat příslušnou studijní povinnost prostřednictvím nástrojů distančním způsobem, musí být zajištěno, že vůči ostatním studentům nebude nepřiměřeně zvýhodněn, resp. musí být přijata taková opatření, která zvýhodnění alespoň určitým způsobem kompenzují.

17) Konkludentním jednáním se rozumí projev vůle učiněný jiným způsobem než slovně (tedy nikoliv ústně nebo písemně), mimo jiné i nevyjádřením protestu.
18) Čl. 30 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).
19) Jak vyplývá z čl. 12 a násl. obecného nařízení o ochraně osobních údajů.
20) Čl. 5 odst. 1 písm. b) obecného nařízení o ochraně osobních údajů.

Zatímco v případě prezenčního způsobu konání studijních povinností má vysoká škola řadu nástrojů, jak kontrolovat řádný průběh studijních povinností a zamezit podvodům při studiu (mimo jiné i přítomností veřejnosti, pokud to v případě běžných zkoušek stanoví vnitřní předpis vysoké školy, zejm. studijní a zkušební řád; průběh a vyhlášení výsledku státní zkoušky je ze zákona veřejné[21]), v případě distančního způsobu konání příslušné studijní povinnosti tyto nástroje nejsou, resp. jsou velice omezené, případně zasahují do soukromí studenta více než je nezbytné (zejm. nástroje proctoringu).

Jako vhodná forma alespoň nějaké kontroly (samozřejmě, AVZ neodhalí úplně každou formu jednání, které by řádný průběh plnění příslušné studijní povinnosti ohrožovalo, to však není jeho cílem, protože ani v případě prezenčního způsobu plnění studijních povinností nelze těmto nežádoucím jevům úplně předejít) se jeví právě pořízení AVZ záznamu, který bude po určitou dobu uchován právě pro účely dokumentace řádného průběhu plnění příslušné studijní povinnosti.

Mimo jiné i s ohledem na zásadu minimalizace zpracování osobních údajů[22] by pak mělo být i nadále upřednostňováno plnění studijních povinností bez pořizování AVZ, přičemž plnění uvedených studijních povinností za využití nástrojů distančního způsobu komunikace by mělo být spíše okrajové a uskutečňováno pouze v mimořádných případech.

Z hlediska právního titulu pro pořizování a uchovávání AVZ se nabízí splnění právní povinnosti, která se na vysokou školu vztahuje na základě právního předpisu[23], a plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.[24] V případě právní povinnosti, která se na vysokou školu vztahuje na základě právního předpisu, je tato povinnost v případě mimořádných situací dána pro pořizování AVZ ze státních zkoušek § 95c odst. 1 písm. c) zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů (zákon o vysokých školách), resp. v roce 2020 byla dána zákonem č. 188/2020 Sb., o zvláštních pravidlech pro vzdělávání a rozhodování na vysokých školách v roce 2020 a o posuzování doby studia pro účely dalších zákonů. V obou případech je stanovena doba uchování AVZ na 5 let.

21) § 53 odst. 1 zákona o vysokých školách.
22) Čl. 5 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů.
23) Čl. 6 odst. 1 písm. c) obecného nařízení o ochraně osobních údajů a § 5 písm. a) zákona č. 110/2019 Sb., o zpracování osobních údajů.
24) Čl. 6 odst. 1 písm. e) obecného nařízení o ochraně osobních údajů a § 5 písm. b) zákona č. 110/2019 Sb., o zpracování osobních údajů.

V případě ostatních studijních povinností, zejm. zkoušek, či plnění státních zkoušek mimo mimořádné situace, tak jak je předvídá zákon o vysokých školách, by pořizování a uchovávání AVZ mělo být opřeno o právní titul plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen, a to na základě právního předpisu, podloženého nadto vnitřním předpisem vysoké školy (studijním a zkušebním řádem). Zde by měly být ideálně stanoveny určité mimořádné situace (nikoliv ve smyslu zákona o vysokých školách), ve kterých je možné konat studijní povinnosti distančním způsobem a pořizovat z nich AVZ. Vnitřním předpisem vysoké školy nebo jiným interním normativním řídícím aktem by pak měly být stanoveny konkrétní podmínky pro pořizování a uchovávání AVZ.

Konkrétním právním základem pro pořizování a uchovávání AVZ v těchto případech by pak mohl být (ve vazbě na § 1 písm. b) zákona o vysokých školách) část první, písm. A., čl. II, odst. 6, věta první[25] a část druhá, písm. C., čl. IV, odst. 5 písm. b)[26] přílohy nařízení vlády č. 274/2016 Sb., o standardech pro akreditace ve vysokém školství. Tyto články stanoví, že vysoká škola má mít nastaven účinný systém zajišťující rovný přístup ke studiu všem uchazečům o studium a studentům, a dále, že vysoká má přijmout dostatečně účinná opatření proti úmyslnému jednání proti dobrým mravům při studiu; zejména proti plagiátorství a podvodům při studiu.

Jinými slovy, na základě shora uvedeného úkolu stanoveného vysoké škole právním předpisem vyplývá veřejné vysoké škole povinnost zajišťovat přístup k vysokoškolskému vzdělání (tj. včetně plnění studijních povinností) v souladu s demokratickými principy, které se dále projevují v požadavku na rovný přístup studentů ke studiu (tj. včetně plnění studijních povinností) a požadavku na přijetí účinných opatření proti úmyslnému jednání proti dobrým mravům při studiu, zejména pak proti podvodům při studiu. V takovém případě lze uvažovat o zpracování osobních údajů, které je nezbytné pro splnění úkolu prováděného ve veřejném zájmu.

Za tímto účelem se jeví jako vhodný nástroj následné kontroly a omezení možného nežádoucího jednání v případě studijních povinností konaných distančně právě pořízení a uchování AVZ. V případě, že by následně došlo ke zpochybnění řádného průběhu plnění příslušné po-

25) „Vysoká škola má nastaven účinný systém zajišťující rovný přístup ke studiu všem uchazečům o studium a studentům."

26) „Vysoká škola přijala dostatečně účinná opatření... proti úmyslnému jednání proti dobrým mravům při studiu, zejména proti plagiátorství a podvodům při studiu."

vinnosti, je tento AVZ použitelný jako důkazní prostředek jak v rámci disciplinárního řízení (především v případě dílčí zkoušky), tak i v případě řízení o vyslovení neplatnosti vykonání státní závěrečné zkoušky nebo její součásti nebo obhajoby závěrečné práce, ve kterém vysoká škola vystupuje jako orgán veřejné moci, resp. správní orgán.

Při použití uvedeného postupu je však třeba upozornit na jeho možné důsledky a zdůraznit, že je doporučován pouze jako výjimečná alternativa, nikoliv jako standardní proces. Jedním z důsledků použití AVZ jako důkazního prostředku může být rozpor se zásadou proporcionality, která je jednou ze základních zásad obecného nařízení. Situaci je totiž možné řešit např. zajištěním dostatečného počtu zkoušejících, kteří detailně sledují průběh zkoušky a zaznamenají případné nesrovnalosti do protokolu, v takovém případě by pak mohlo být pořízení AVZ považováno za nepřiměřený zásah do práv subjektů údajů.

Pro srovnání uveďme příručku dozorového úřadu pro ochranu osobních údajů spolkové země Bádensko-Württembersko,[27] zabývající se mj. právě přiměřeností nahrávání. Jako principy uplatnitelné také v české prostředí uvádí, že opatření proti neetickému nebo podvodnému jednání při distančním zkoušení nemají být významně širší, než je tomu v případě prezenčních zkoušek. Shromažďování AVZ výhradně pro hypotetické důkazní účely není doporučováno, stejně jako není doporučováno monitorování místností studentů (snímání celých studentských pokojů, zkoumání prostředí analýzou zvuků apod.). V neposlední řadě příručka radí nevyužívat individuální monitorovací technologie, jako je sledování pozornosti, automatizované vyhodnocování pohybů očí, hlavy apod.).[28]

V každém případě je tedy postup pořizování AVZ využitelný pouze v minimu případů, kdy skutečně neexistuje jiná cesta pro zajištění kontroly. Vysoká škola by pak měla zcela jasně definovat, za jakých mimořádných okolností (na straně školy nebo i studenta) bude k nahrávání přistoupeno a o těchto okolnostech dostatečně informovat před samotným pořízením AVZ.

Doba uchování AVZ, jejichž pořízení a uchování nepředpokládá přímo zákon o vysokých školách, by pak neměla být delší než ta, která je zákonem o vysokých školách předpokládána pro distanční konání státních zkoušek v případě mimořádných situací podle zákona o vysokých

27) Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

28) Srov.: Handreichung zu online-Prüfungen an Hochschulen (online), https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/07/20210715_Handreichung-Online-Pruefungen.pdf (cit. dne 1. 12. 2021).

školách, tedy nejdéle 5 let. S ohledem na zákonné lhůty potřebné pro případné odvolání proti výsledku zkoušky však lze doporučit přiměřené zkrácení této lhůty.

Pokud jde o technická nebo organizační opatření proti neoprávněným či protiprávním způsobům zpracování a proti náhodné ztrátě, zničení nebo poškození AVZ, měl by mimo jiné být dostatečným způsobem omezen přístup k AVZ na co nejnižší možný počet oprávněných osob. Z hlediska pořízení a uložení AVZ záznamu by měl mít přístup k AVZ pouze příslušný vyučující/předseda zkušební komise, případně referentky kateder a studijních oddělení, které AVZ mohou shromažďovat do centrálního úložiště.

Přístup k AVZ záznamům uloženým v centrálním úložišti by pak měli mít pouze pověření zaměstnanci ICT oddělení pro účely správy úložiště jako takového. Na základě žádosti by pak měl mít k AVZ přístup pouze děkan, resp. rektor, a to vždy ke konkrétnímu AVZ záznamu pro účely vedení případného správního (disciplinárního) řízení, případně na vyžádání jiné orgány veřejné moci.

Pokud jde o zveřejňování AVZ, důrazně se nedoporučuje je zveřejňovat. Na rozdíl od pořízení a uchovávání AVZ, případně použití AVZ orgánem veřejné moci (rektor/děkan jím je v případě disciplinárního řízení), pro zveřejnění nelze najít dostatečně odůvodnitelný právní titul vyjma souhlasu všech AVZ dotčených osob. Vzhledem k tomu, že na souhlas jsou kladeny vysoké formální nároky, vysoká škola pak má být schopna jej doložit po celou dobu zpracování a nadto jej lze kdykoliv odvolat, obecně se nedoporučuje tento právní titul využívat.

Nástroje pro uchování

Jak již bylo nastíněno výše, jako nejvhodnější místo pro ukládání AVZ by mělo být zvoleno určité centrální datové úložiště.

Takové centrální datové úložiště by pak mělo být ideálně buď provozované přímo samotnou vysokou školou v rámci infrastruktury dané vysoké školy (disková pole, SAN apod.), případně alespoň v rámci infrastruktury CESNET, rovněž však lze akceptovat i datové úložiště mimo infrastrukturu vysoké školy na základě centrálně nebo individuálně uzavřené smlouvy s příslušným provozovatelem (při řádném ošetření GDPR a SLA). Tato datová úložiště by pak rovněž měla ideálně být chráněna dalšími opatřeními, jako jsou přístupová hesla, šifrování a rovněž již výše zmínění řízení přístupů.

Z opačné strany, AVZ by neměly být rozhodně uchovávány na přenosných médiích, lokálních discích či jiných úložištích a v síťových a cloudových úložištích určených pro veřejnost. Na tomto místě je vhodné definovat alespoň základní rozdělení datových úložišť a zmínit alespoň základní úskalí, která při použití úložišť mohou vyvstat.

Za nejméně vhodné úložiště pro uložení lze považovat přenosná média, kam patří flash disky, paměťové karty, externí disky či překvapivě stále hojně využívaná CD a DVD. Obecně tedy mluvíme o médiích, která nejsou pevnou součástí žádného hardwaru. Právě v přenositelnosti pak tkví největší úskalí z hlediska zabezpečení dat, neboť při manipulaci s těmito médii může snadno dojít k jejich ztrátě (např. prostým ponecháním zapojeného flash disku v PC), nebo krádeži. Tato média také často nelogují přístupy, nelze tedy v důsledku zjistit, kdo a kdy k datům přistupoval a zda si nepořídil jejich kopii. Navíc nejsou tato úložiště dostatečně zálohována, tedy chráněna proti případné ztrátě dat.

Další typ úložišť představují různé lokální disky, které tvoří pevnou součást dalšího hardwaru, myšleny jsou především harddisky PC a notebooků, či jiných mobilních zařízení (tablety, mobilní telefony apod.). U většiny z nich lze samozřejmě narazit na obdobný problém jako u přenositelných úložišť. Náchylnější jsou také tato úložiště na různé kybernetické útoky (phishing, ransomware), takže je vhodné zopakovat známé základní zásady, které mohou podobný útokům předcházet či zabránit, jako je dostatečně silné zabezpečení heslem, aktualizovaný antivirus i další doplňkové aplikace a pravidelně proškolený uživatel. Zmíněný typ úložišť je vhodný spíše pro data, ke kterým je nutný (pravidelný) rychlý přístup, který zároveň nevyžaduje další sdílení uložených dat.

Poslední základní typ úložišť představují různá cloudová a síťová úložiště, jejichž podrobnější rozdělení by přesáhlo limity této kapitoly, proto se omezíme jen na několik obecných zásad. Tato datová úložiště mohou být provozována přímo na infrastruktuře veřejné vysoké školy, nebo může být jejich provoz zajišťován externím poskytovatelem.

V případě, že úložiště provozuje příslušná škola, je třeba vždy věnovat pozornost nastavení procesů. V kontextu ochrany a zabezpečení dat nás zajímá především správa rolí a přístupů k datům, způsob zálohování dat, způsob zabezpečení dat proti neoprávněným zásahům (uživatelsky „zevnitř“ i případným útokem „zvenčí“), a také doba jejich uložení. Pokud jsou jako součást datových sad ukládány i osobní údaje, je nezbytné stanovit maximální lhůtu pro uložení vyplývající z příslušného právního důvodu a tuto lhůtu vždy dodržet.

Provoz úložišť zajišťovaných externím poskytovatelem musí být vždy ošetřen smlouvou, jejíž součástí je i specifikace zpracování

a ochrany osobních údajů, čemuž se podrobněji věnují další kapitoly této metodiky. Při nastavení správných procesů pak cloudová a síťová úložiště představují z hlediska ochrany a zabezpečení osobních údajů nejvhodnější řešení.

4

NEJČASTĚJŠÍ POCHYBENÍ Z HLEDISKA PROBLEMATIKY OSOBNÍCH ÚDAJŮ PŘI DISTANČNÍM VZDĚLÁVÁNÍ A HODNOCENÍ

Autoři: Jan Jindra (Univerzita Karlova),
Kateřina Burianová (Jihočeská univerzita
v Českých Budějovicích)

Přechod na masivní využívání nástrojů a prostředků pro distanční výuku a přenesení výuky do online prostoru v důsledku koronavirové krize se v některých případech neobešlo bez pochybení v oblasti ochrany a zabezpečení osobních údajů. Obecně pozitivním faktorem je, že tato pochybení se mnohdy netýkala špatného procesního a systémového nastavení na straně vysokých škol, ale spíše nezáměrných chyb jednotlivců, mnohdy pramenících z jejich nedostatečného proškolení či obecně nedostatku informací.

Nepochybně se jedná o důsledek živelného přechodu do online prostředí, kdy jednoduše ani nebyl k dispozici dostatečný prostor pro dokonalé informování a proškolení subjektů údajů (ať již z řad akademiků, či studentů) o úskalích, na která může distanční výuka narážet při aplikaci pravidel a principů vyplývajících z obecného nařízení GDPR.

Cílem této kapitoly je podrobněji analyzovat vzniklé problémy, případně navrhnout jejich řešení, na základě konkrétních příkladů poskytnout doporučení pro jejich předcházení, a napomoci tak zkvalitňování procesu zabezpečení a zpracování osobních údajů jako důležité součásti akademické integrity.

Smlouva nebo licence k nástroji používanému pro účely distančního vzdělávání a hodnocení

Jednou z klíčových procesních otázek při distančním vzdělávání a hodnocení je použití vhodného nástroje. Jakkoliv je obvykle celkem samozřejmě řešena příslušná smlouva nebo

licence pro použití konkrétního nástroje, již méně často je pamatováno na skutečnost, že takový nástroj by měl splňovat požadavky kladené obecným nařízením GDPR. Součástí smluv uzavíraných pro distanční nástroje v současnosti často bývá i příslušná kapitola věnovaná zpracování a ochraně osobních údajů, případně jsou takové podmínky stanoveny i samostatnou smlouvou o zpracování osobních údajů (data processing agreement, tedy „DPA").

Některé nástroje pro distanční vzdělávání však mohou řešit otázku zpracování a zabezpečení údajů pouze velmi obecně, setkat se lze dokonce i se situacemi, kdy je součástí smlouvy pouhý odkaz na všeobecné podmínky na webových stránkách poskytovatele nástroje (typicky např. u systémů využívaných pro proctoring). Při posuzování smluv či licencí z hlediska požadavků GDPR jsou nejčastějšími problematickými body následující oblasti:

→ **Nástroj předává zpracovávané osobní údaje mimo prostor Evropské unie**

V počátcích koronavirové krize bylo možné se v případě častého předávání údajů do USA zaštítit tzv. EU-US Privacy Shield. Štít EU-USA na ochranu soukromí byl nástroj schválený v roce 2016 Evropskou komisí, který za přesně stanovených podmínek určoval předávání dat. Dříve uzavřené smlouvy pro některé distanční nástroje stavěly předání osobních údajů právě na tomto ujednání. Rozsudek Soudního dvora EU C-311/18 (tzv. Schrems II) ze dne 16. července 2020[29] však znamenal faktické zneplatnění tohoto štítu.

Ve smlouvách pro distanční nástroje uzavřených před tímto datem, tak může být skryt podstatný problém znamenající rozpor s obecným nařízením GDPR. V současnosti tak platí, že jakékoliv předávání osobních údajů (zpracovávaných v nástrojích pro distanční výuku) do USA je v rozporu s obecným nařízením GDPR.

→ **Nástroj předává údaje třetím stranám**

Jakékoliv předání třetí straně, které není smluvně či licenčně dostatečně ošetřeno, a o kterém není správce (vysoká škola) jednoznačně informován, přináší problém z hlediska GDPR. Obzvláště problematické může být použití nástrojů pro analýzu dat nebo předávání dat jiným společnos-

29) https://www.uoou.cz/rozsudek-sdeu-c-311-18-schrems-ii-a-jeho-dusledky/ds-6338

tem (či sociálním sítím) pro účely cílené reklamy. Problematické může také být skryté využívání služeb či funkcionalit jiných subdodavatelů, kteří nejsou uvedeni ve smlouvě či licenci.

→ **Ve smlouvě není jasně definován rozsah zpracovávaných osobních údajů**

Ve smlouvě musí být vždy jednoznačně definováno, jaký rozsah osobních údajů je předáván zpracovateli (dodavateli softwaru), a spolu s tím musí být stanoven i jednoznačný účel, za kterým jsou osobní údaje zpracovávány. Jinak řečeno, smlouva o zpracování osobních údajů by měla jasně definovat, proč zpracovatel konkrétní kategorii osobních údajů vyžaduje. Nadbytečný rozsah zpracovávaných údajů představuje jednoznačný problém z hlediska GDPR.

→ **Ve smlouvě není jasně definována doba zpracování osobních údajů a možnost jejich výmazu**

Dle článku 28 odst. 3, písm. g) GDPR musí být součástí smluv o zpracování osobních údajů zakotvení povinnosti zpracovatele v souladu s rozhodnutím správce všechny osobní údaje buď vymazat, nebo je vrátit správci po ukončení poskytování služeb spojených se zpracováním, a vymazat existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů. Neměl by tak existovat důvod, proč by měl poskytovatel nástroje dále zpracovávat či dlouhodobě uchovávat osobní údaje, zvlášť po ukončení platnosti smlouvy (ukončení používání nástroje), v praxi však nebývá ve smlouvách dostatečně ošetřena doba zpracování osobních údajů, u některých poskytovatelů se lze setkat i s případy, kdy není jasně definováno, co se s osobními údaji stane po vypršení smlouvy. Správce (vysoká škola) by také měl mít možnost vždy jasně označit konkrétní údaje, u kterých si nepřeje jejich další zpracování. Tento požadavek také souvisí s možnou žádostí o výmaz ze strany subjektu údajů.

→ **Smlouva nedefinuje součinnost při porušení zabezpečení, možném úniku dat nebo aplikuje právní ustanovení zemí mimo prostor Evropské unie**

V kritickém případě, kdy by došlo k porušení zabezpečení na straně zpracovatele (poskytovatele nástroje) nebo dokonce úniku zpracovávaných osobních údajů, měla by smlouva vždy jasně definovat procesy pro řešení, míru součinnosti jednotlivých smluvních stran, stejně jako míru zodpovědnosti a s ní související sankce. Součástí standardních smluv také bývá možnost a definice způsobu auditní kontroly ze strany správce (vysoké školy) či konkrétního dozorového úřadu.

V neposlední řadě je doporučeno, aby se smlouva řídila ideálně českou legislativou, případně legislativou některého z členských států EU. V případě, že smlouva sice jasně definuje vše řečené výše, ale následné řešení problémů se bude řídit právem např. v Kalifornii, jen těžko si lze představit větší disproporci a reálné vyřešení případných vzniklých problémů. V praxi může vyjednávání uvedených podmínek bohužel často narážet na neochotu dodavatelů měnit příslušná smluvní ustanovení.

Otázku zabezpečení a ochrany osobních údajů však nelze vnímat pouze v úzkém kontextu používaného distančního nástroje, tedy platformy, která zajistí audiovizuální přenos. Stejnou optikou je nutné nahlížet i na případné nástroje, které jsou používány pro zveřejnění či streamování záznamu. I v takovém případě je nutné dbát na dostatečné zabezpečení takového nástroje, jeho soulad s GDPR a ideálně takový nástroj ošetřit smlouvou či licencí. Některé vysoké školy řeší tuto situaci vytvořením vlastních streamovacích platforem, v mnoha případech jsou však používány volně dostupné nástroje bez dostačeného smluvního či licenčního ošetření, což do budoucna může přinést řadu problémů a vysoké školy se tak mohou stát snadným terčem stížností studentů či akademiků, kteří budou v lepším případě požadovat pouhé stažení audiovizuálního záznamu.

Pokud už vytvoříme audiovizuální záznam v nástroji, jehož použití je dle výše řečeného dostatečně ošetřeno, vyvstává klasická nerudovská otázka „Kam s ním?“. Uložení záznamu na vhodném úložišti je totiž další podstatnou částí zpracování a zabezpečení osobních údajů. Je nepochybné, že převážná část vysokých škol věnuje problematice uložení dat velkou pozornost, příklady pochybení z praxe však ukázaly, že především nedostatečná informovanost akademických pracovníků může vést k situaci, kdy je lákavé použít některé známé úložiště (provozované typicky některým z poskytovatelů mailových klientů). Použití takového úložiště pro soukromé účely jistě nelze nikomu upírat, ale v prostřední veřejné vysoké školy je z hlediska GDPR zcela nepřípustné.

Nemusíme v tomto kontextu hovořit pouze o uložení záznamu přednášky, prostším příkladem pochybení budiž např. požadavek na studenty, aby dílčí úkoly v rámci studia nahrávali do nezabezpečeného úložiště některého z komerčních poskytovatelů. Student se pak může celkem oprávněně bránit použití nezabezpečené platformy a upozorňovat na porušení GDPR, obzvlášť v případě, že veřejná vysoká škola disponuje dostatečně zabezpečeným robustním řešením.

Posledním příkladem, kdy může distanční výuka narazit na požadavky kladené obecným nařízením, je použití nevhodného nástroje pro komunikaci, resp. sdílení souborů. Myšleny jsou především některé chatovací aplikace provozovatelů sociálních sítí apod.

Sluší se stručně shrnout, proč jsou výše uvedené příklady použití nevhodných nástrojů pro distanční vzdělávání, resp. uložení dat, problematické. Téměř vždy při použití jakéhokoliv nástroje dochází ke zpracování osobních údajů třetí stranou, jakkoliv mohou být osobní údaje jen v rozsahu titul, jméno, příjmení, e-mail. V takovém případě je vždy nezbytné disponovat zpracovatelskou smlouvou, jinak jakékoliv pochybení při zpracování a zabezpečení osobních údajů nese jednoznačně správce, tedy veřejná vysoká škola. Správce však zároveň bez smlouvy či licence fakticky ztrácí kontrolu nad svými daty.

Freewarové nástroje či úložiště, tedy nástroje poskytované bezplatně, jsou nezřídka financovány právě na základě vytěžování dat, jejich předávání třetí straně nebo jejich použití pro cílenou reklamu. Smluvní zabezpečení placeného nástroje má pak tomuto postupu zamezit.

Obecně platí, že nástroj, jehož instalace a používání se může jevit jako výhodný, neboť je poskytován zdarma, může být z hlediska GDPR ve výsledku drahou variantou pro veřejnou vysokou školu.

Pořizování audiovizuálních záznamů v rámci distančního vzdělávání

Spolu s přechodem výuky do online prostředí začalo být pro veřejné vysoké školy celkem obvyklou praxí pořizovat z různých důvodů audiovizuální záznamy z distančního vzdělávání. V jiných částech této metodiky se věnujeme otázkám souvisejícím s pořizováním záznamů v rámci státní závěrečné zkoušky, kde legislativa stanovila celkem jasné mantinely. Při pořizování jiných druhů záznamů však může docházet k pochybením z hlediska GDPR, z nichž některé nemusejí být zcela zjevné na první pohled. Připomeňme v této souvislosti, že zachycení podoby či hlasu v kombinaci se jménem a příjmením osoby přihlášené do nástroje pro distanční výuku je jednoznačně osobním údajem.

Obecně platí, že zachytit podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením. Pro rozšiřování této podoby je pak taktéž třeba svolení dotyčné osoby.[30]

30) Viz §§ 84 a 85 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

V některých případech, kam nepochybně patří i zmiňované státní závěrečné zkoušky, lze pro pořízení záznamu využít i jiné právní důvody, než je souhlas. V mnoha případech však souhlas subjektu údajů zůstává jediným relevantním právním důvodem, který lze pro pořízení záznamů použít.

Typickým příkladem je nahrávání dílčích zkoušek studia, které s přechodem do distančního prostředí poměrně narostlo. Veřejné vysoké školy při pořizování záznamu často argumentují možností kontroly průběhu zkoušky, kdy právě distanční konání může svádět k tendenci podvádění při zkoušce, a záznam by pak posloužil jako případný důkaz pro potvrzení či vyvrácení takového jednání.[31]

Proti tomu ale stojí skutečnost, že možnosti případného neetického či podvodného jednání jsou v online světě téměř nekonečné. Tím, že prostředí (hardware, software, ale i stavební dispozice) na straně zkoušeného je téměř zcela pod jeho kontrolou, je možnost technologické realizace podvodu nadmíru vysoká. Nahrávání pak může odhalit pouze prosté, nikoliv sofistikované podvody. Držení audiovizuálního záznamu také přináší vysoké škole i mnoho povinností – například vydat tomu, kdo o to požádá, tu část záznamu, kde je zachycen, a to tak, že na záznamu nebudou zachyceny ostatní osoby. V případě mnoha souběžných žádostí (ať již sabotáže nebo náhodné shody) by to mohlo být problematické.

Pořízení záznamu z dílčí zkoušky studia je proto nejlépe podmínit souhlasem všech stran, tedy jak zkoušejícího, tak zkoušeného studenta. Student musí mít možnost odmítnout nahrávání, je to jeho právo, které mu nelze odpírat a není možné studenta za využití tohoto práva nijak trestat.

I pokud student souhlasí s nahráváním, neexistuje ani poté důvod k dlouhodobému uchovávání záznamu z dílčí zkoušky studia, neboť na studenta může být při udělení souhlasu nahlíženo jako na „slabší stranu". Není tedy dodržena zásada proporcionality při udělení souhlasu, navíc do hry vstupuje i faktor odvolatelnosti souhlasu. Student i akademik tedy kdykoliv mohou odvolat svůj souhlas s pořízením záznamu a je povinností veřejné vysoké školy tento záznam neprodleně odstranit.

Při pořizování záznamů z výuky rozlišme dvě situace. V prvním případě je pořizován čistě záznam přednášejícího z frontální výuky, na záznamu není zachyceno auditorium a ani přednášející nevstupuje do přílišné interakce s účastníky přednášky, součástí záznamu tedy není

31) Za výjimečných okolností lze sice uvažovat na základě veřejného zájmu o pořízení audiovizuálního záznamu dílčí zkoušky studia, tento postup však je pouze navrhován jako možná alternativa kvůli případným důsledkům pro veřejnou vysokou školu. Více o tom pojednává předcházející kapitola.

hlas či podoba jiných osob, pouze samotného akademika. V takovém případě postačuje k pořízení záznamu souhlas přednášejícího. Streamování, dlouhodobé uchování či zveřejnění záznamu přednášky však není bez souhlasu přednášejícího možné.

Teoreticky lze v této souvislosti doporučit postup, kdy je nahrávání přednášek stanoveno jako součást povinností zaměstnance, tedy jako nezbytná podmínka jeho práce. Jistě však není možné dát plošný souhlas s pořizováním záznamů jako textaci do uzavírané pracovní smlouvy. Vhodnější je proto získání souhlasu se zpracováním osobních údajů, který však nesmí být nezbytnou podmínkou pro uzavření pracovní smlouvy.

Jako druhou vzorovou situaci vezměme pořizování záznamů z cvičení či praktických seminářů. V takovém případě lze logicky předpokládat větší interakci přednášejícího se studenty, kteří se do výuky aktivněji zapojují a nástroj pro distanční vzdělávání tak zachycuje jejich hlas, podobu, obvykle pak ve spojení se jménem. V takovém případě je třeba velmi pečlivě zvažovat důvody pro nahrávání a uchovávání záznamů tohoto charakteru, neboť student participující ve výuce může vyslovit svůj nesouhlas s pořizováním záznamu. Řešením není ani implicitně předjímat souhlas účastníka přednášky, pokud jasně neprojeví svůj nesouhlas s pořizováním záznamu, neboť svoje právo může uplatnit i kdykoliv později a požadovat výmaz.

Rozhodně však není ke škodě věci, pokud přednášející vždy na začátku semináře upozorní, že seminář je nahráván a zeptá se připojených účastníků, zda s tím jsou srozuměni a zda jim pořízení záznamu nevadí. Vhodnou součástí tohoto úvodu je i informace, co se dále bude se záznamem dít, např. že bude umístěn na některém z úložišť a přístupný pouze studentům daného ročníku apod.

Nikdy bohužel nelze zcela zabránit situaci, kdy si účastník přednášky pořídí vlastní záznam z přednášky či semináře a tento záznam dále rozšíří bez souhlasu ostatních zúčastněných. I když většina dnes používaných nástrojů dokáže při správném nastavení tomuto kroku zamezit, může účastník použít i jiný software a záznam pořídit. Vždy je proto vhodné apelovat ať již v předpisech, či před samotnou přednáškou/seminářem na účastníky a upozornit je, že pořizování a rozšiřování záznamu bez souhlasu ostatních zúčastněných může být porušením zákona.

Osobní údaje třetích stran jako součást audiovizuálního záznamu

Pokud dochází ke streamování nebo nahrávání záznamu z distanční výuky, je třeba mít vždy na zřeteli, že záznam může zachytit nejen přednášejícího a studenty, kteří se nezbytně výuky účastní a jejichž osobní údaje jsou zpracovávány. Součástí samotné výuky může být i použití výukových materiálů, které obsahují osobní údaje. Zachycení těchto materiálů jako součásti záznamu, který je následně zveřejněn širšímu publiku, může znamenat porušení zabezpečení osobních údajů a zásah do práv subjektů údajů.

Jako příklad může posloužit použití jména osoby při prezentaci výsledků sociologického výzkumu při výuce. Jakkoliv přednášející může i disponovat dřívějším souhlasem konkrétní osoby, že materiály mohou být použity při výuce, je nezbytné vždy znovu posoudit, zda je původní souhlas dostačující pro účel použití. Subjekt údajů (respondent sociologického výzkumu) mohl sice v minulosti udělit výslovný souhlas pro použití odpovědí jako součásti výuky, avšak dost pravděpodobně předjímal použití při prezenční výuce, nikoli ve výuce distanční. Použití při distanční výuce tak nemusí odpovídat původnímu účelu, pro který byl udělen souhlas. Pokud je navíc z distanční výuky pořízen záznam, který je přístupný širší veřejnosti, nebo je taková distanční výuka sdílena prostřednictvím streamu, nelze dostatečně podchytit okruh osob, kterým mohou být osobní údaje zpřístupněny a nemusí se tedy účel použití výukových materiálů shodovat s původním souhlasem konkrétního subjektu údajů (respondenta).

Na podobnou situaci problematickou z hlediska zabezpečení osobních údajů lze například narazit i při výuce budoucích pedagogů. Často je v takovém případě součástí studijního programu i praktická výuka, realizovaná v mateřských školkách a na základních či středních školách. Pokud je z takové výuky pořízen záznam, jehož součástí je zachycení dalších osob (např. dítěte, žáka nebo třídního učitele), mohou se v něm objevit i osobní údaje spadající do zvláštní kategorie osobních údajů, např. pokud bude v rámci výuky probíráno téma náboženství. Takové zpracování již zcela jednoznačně podléhá souhlasu. V případě zachycení podoby jakékoliv osoby spolu se záznamem jeho hlasu a uvedením jména lze uvažovat již i o zpracování biometrických údajů dle čl. 9 obecného nařízení.

Záznamy o činnostech zpracování v rámci distančního vzdělávání a hodnocení

Podle čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů vede správce záznamy o činnostech zpracování, za které odpovídá. Příslušný článek pak dále uvádí typy informací, které musí konkrétní záznam obsahovat. V praxi nejčastěji zodpovídá za vedení a korektní správu záznamů o činnostech zpracování pověřenec pro ochranu osobních údajů jmenovaný správcem, nejinak je to mu i v případě vysokých škol. Živelný přechod na distanční vzdělávání sebou přinesl i četné pořizování audiovizuálních záznamů, které jsou následně po určitou dobu ukládány na úložištích.

O vhodných úložištích pojednává jiná kapitola tohoto textu, stejně jako tato kapitola zmiňuje možné problémy z hlediska ochrany a zabezpečení osobních údajů, které může přinést nevhodně zvolené úložiště.

Pro správné systémové nastavení procesů při ukládání nahrávek, jejichž součástí jsou osobní údaje, je nedílnou součástí pamatovat na zahrnutí tohoto typu agendy do záznamů o činnostech zpracování, a to včetně přiměřených lhůt pro toto uložení. V rámci záznamů se může jednat jak o samostatné nové zpracování, tak i o rozšíření již existujících záznamů o zpracování.

Jakkoliv legislativa určila jednoznačnou lhůtu pěti let pro uložení audiovizuálního záznamu pořizovaného ze státní závěrečné zkoušky, v případě záznamů pořizovaných v rámci standardní výuky není lhůta zdaleka jednoznačná. Je tak vždy na vysoké škole jako správci osobních údajů, aby stanovila vhodné a přiměřené lhůty, po které budou záznamy ukládány. Stejně tak je nedílnou součástí i stanovení místa uložení a následného procesu pro vyřazení těchto záznamů. Jako vhodné vodítko může posloužit spisový řád vysoké školy, neboť i audiovizuální záznam lze dle legislativy nahlížet jako typ dokumentu.

V závěru této kapitoly nezbývá, než konstatovat, že nejúčinnějším způsobem, jak se vyhnout pochybením z hlediska GDPR při distančním vzdělávání, je těmto pochybením předcházet. Vhodné nastavení vnitřních procesů, např. pro pořizování i používání nástrojů pro distanční výuku by mělo být jedním z prvních kroků z hlediska veřejné vysoké školy. Stejně důležitou roli však hraje komunikace, vysvětlování úskalí, které používání nových nástrojů může přinést a nastavení systému technické podpory a školení (nejen) v problematice GDPR.

5

DISTANČNÍ HODNOCENÍ A ZKOUŠENÍ (PROCTORING) A OCHRANA OSOBNÍCH ÚDAJŮ

Autor: Štěpán Richter (Veterinární univerzita Brno)

Termín proktoring (nebo proctoring) znamená dozorování studentů při online testování. Cílem proktoringu je, stejně jako u jakéhokoli jiného typu dozorování, zabránit studentům v podvádění při zkoušce.

Přínos proktoringu je pak rovněž stejný: zajištění rovných podmínek potlačením rizika nepoctivého jednání. Osoba provádějící proktoring se nazývá proktor. Vzhledem k absenci osobního styku při online zkoušení musí proktor kontrolovat činnost studentů technickými prostředky. Tyto prostředky mohou mít mnoho podob, od prostého sledování studentů přes webkamery až po software v zařízení studentů, který zaznamenává jejich činnost.

Základními právními předpisy upravujícími ochranu osobních údajů je 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) (dále jen „GDPR“) a zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „zákon o zpracování osobních údajů“).

Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je základním právem. Ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie a čl. 16 odst. 1 Smlouvy o fungování Evropské unie přiznávají každému právo na ochranu osobních údajů, které se jej týkají. Toto platí za každé situace, tedy i při proktoringu. Vysoká škola jako zpracovatel ani proktoring jako činnost nejsou vyňaty z působnosti GDPR či zákona o zpracování osobních údajů.

Podle čl. 4 GDPR jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě. 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 identity této fyzické osoby. Zpracováním osobních údajů je pak jakákoliv operace s osobními údaji, která je prováděna pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití atd. Tyto definice, byť velmi široké, jsou jasně aplikovatelné na situaci ohledně proktorinku: Studenti jsou identifikovatelnými fyzickými osobami (neboli subjekty údajů) a při proktoringu je o nich shromažďováno, a tedy zpracováváno, velké množství osobních údajů. Pokud je student nahráván na kameru, jsou zpracovávány jeho údaje, pokud mu program sbírá data ze zařízení, na kterém vykonává test, jsou zpracovávány jeho údaje.

Příklady identifikátorů, které mohou být při proktoringu o studentech shromažďovány:

- podoba studenta,
- hlas studenta,
- informace, které o sobě student během záznamu prozradí, protože musí – např. řekne nahlas své jméno nebo ukáže občanský průkaz na kameru,
- jakékoli nahodilé informace, které zjistí kontrolní software ze zařízení studenta a které odpovídají definici osobních údajů.

Při zpracování osobních údajů platí zásady vymezené v čl. 5 GDPR: zákonnost, korektnost a transparentnost, účelové omezení, minimalizace, přesnost, omezení uložení, integrita a důvěrnost.

Zákonnost zpracování osobních údajů je postavena na konceptu tzv. zákonného titulu. Tyto jsou vyjmenovány v čl. 6 GDPR. Z těchto titulů pro VŠ připadají v úvahu dva: souhlas subjektu údajů dle písm. a) a nezbytnost pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce (tj. VŠ), podle písm. e) a shodně § 5 písm. b) zákona o ochraně osobních údajů.

Postup na základě souhlasu je pracnější, nicméně bezpečnější variantou, neboť pokud student dá ke zpracování údajů výslovný souhlas, je VŠ významně kryta při jakémkoli následném problému. Tento souhlas může být dán písemně i elektronicky, např. v rámci informačního systému školy. Základním problémem tohoto přístupu je nutnost souhlas sepsat a vymezit v něm všechny údaje, které budou zpracovávány. Rovněž je třeba dodržet podmínky souhlasu dle čl. 7 GDPR a mít na paměti, že student

může souhlas kdykoli odvolat, a to musí být stejně snadné, jako jej udělit. Zejména je nezbytné pamatovat na dobrovolnost souhlasu. S ohledem na nerovnovážné postavení subjektu údajů (studenta) a správce (vysoké školy) je zpochybnitelná i svobodná vůle subjektu údajů při udělení souhlasu.

Pokud VŠ nechce z jakéhokoli důvodu od studentů vyžadovat souhlas, je přípustná i argumentace, že VŠ údaje potřebuje pro splnění úkolu prováděného ve veřejném zájmu/při výkonu veřejné moci. Zde je ovšem třeba počítat s tím, že pojmy jako veřejný zájem a veřejná moc jsou dosti diskutabilní a dostatečně determinovaný student by mohl zpracování napadnout u příslušných orgánů. O to více je pak v této variantě nutné dodržet principy zpracování osobních údajů, zejména minimalizaci a účelové omezení.

Je třeba mít na paměti, že ochrana osobních údajů není jen soubor doporučených postupů. Při porušení GDPR nebo zákona má Úřad pro ochranu osobních údajů právo ukládat nemalé pokuty a může rovněž provádět kontroly, aby tato porušení zjistil.

Doporučení ohledně zpracování osobních údajů při proktoringu

Pokud je to jen trochu administrativně možné, měla by VŠ od studentů získat souhlas se zpracováním osobních údajů, pokud se účastní proktorovaného testu.

V souladu s principem omezení uložení by VŠ neměla ponechávat záznamy ze zkoušek uloženy déle, než je nezbytně nutné. Praktickým milníkem v tomto směru je moment, kdy již nelze rozporovat výsledek zkoušky – tedy se již nezmění, a tedy již de facto nezáleží na tom, zda při zkoušce student podváděl.

VŠ by měla nastavit své systémy tak, aby bylo zpracování osobních údajů co nejplynulejší a maximálně automatizované – souhlas se zpracováním předložit studentovi při přihlašování na zkoušku, a student tedy udělá pouze klik navíc. Automatické mazání záznamů ze zkoušek, které již nejsou k ničemu třeba.

Určitá práva nelze studentům odepřít (odvolání souhlasu se zpracováním, právo vědět, jak jsou jeho osobní údaje zpracovány a kde jsou uloženy, …). S jejich výkonem by neměly být spojovány žádné následky: např. pokud student odvolá souhlas se zpracováním před zkouškou, nebude na zkoušku připuštěn, pokud jej odvolá po zkoušce, vzdává se tím práva na odvolání apod. „Souhlas by neměl být považován za svobodný,

pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen."[32]

Minimalizace slouží všem: VŠ by si měla stanovit, zda jí některé metody kontroly stojí za zásah do osobních údajů studentů a z toho vyplývajících následků. Zejména programy na kontrolu aktivity zařízení studentů jsou často regulérní špehovací software a vysoká škola se jejich používáním vystavuje nezanedbatelnému riziku. Efektivita těchto kontrol aktivity je navíc poměrně diskutabilní.

Zvlášť u proctoringových nástrojů a systémů je před jejich implementací doporučeno zaměřit se na problematické body z hlediska GDPR. Předchozí kapitola věnovaná nejčastějším pochybením z hlediska problematiky osobních údajů při distančním vzdělávání a hodnocení důrazně doporučuje věnovat pozornost smlouvám uzavíraným pro nástroje – systémy, jejichž součástí musí vždy být i příslušná ustanovení o ochraně a zpracování osobních údajů. Některé proctoringové nástroje pak častěji než jiné využívané systémy naplňují tuto povinnost poněkud volněji, například pouhým odkazem na všeobecné obchodní podmínky na webu. Lze se také častěji setkat s vytěžováním údajů poskytnutých správcem (veřejnou vysokou školou) prostřednictvím analytických nástrojů třetích stran včetně sociálních sítí. Důležité je také u poskytovatelů nástrojů mimo prostor Evropské unie vést v patrnosti možné dopady zrušení Štítu EU-USA na ochranu soukromí, které taktéž detailněji shrnuje předchozí kapitola.

32) Cit. dle: Obecné nařízení o ochraně osobních údajů, bod odůvodnění 42.

6

ONLINE ZÁPIS KE STUDIU NA VYSOKÉ ŠKOLE Z HLEDISKA GDPR

Autor: Martin Pernica (Mendelova univerzita v Brně)

Samosprávná působnost veřejné vysoké školy

Do samosprávné působnosti veřejné vysoké školy, dále jen „VVŠ“, patří dle §6 odst. 1 písm. b) zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, dále jen „ZVŠ“ mj. určování počtu přijímaných uchazečů o studium, podmínek pro přijetí ke studiu a rozhodování v přijímacím řízení a dále dle §6 odst. 1 písm. f) ZVŠ rozhodování o právech a povinnostech studentů.

Proces od zahájení přijímacího řízení uchazeče až po zápis ke studiu

Uchazeč o studium na vysoké škole, dále jen „VŠ“ doručí přihlášku ke studiu na vysoké škole, která uskutečňuje příslušný studijní program, čímž je zahájeno přijímací řízení dle §50 odst. 1 ZVŠ. Přijímací řízení je zahájeno na žádost ve smyslu §44 odst. 1 zákona č. 500/2004 Sb., správní řád, dále jen „SŘ“.

Přihláška ke studiu na VŠ v České republice bývá obvykle elektronická. Rozsah osobních údajů poskytnutých uchazečem VŠ vyplývá zejména z §50 odst. 1 ZVŠ, §2 vyhlášky č. 277/2016 Sb., o předávání statistických údajů vysokými školami, dále jen „Vyhláška“ a podmínek zveřejňovaných Ministerstvem školství, mládeže a tělovýchovy, dále jen „MŠMT“ pro účely sběru výkazu o přijímacím řízení ke studiu na VŠ na webu MŠMT [https://dsia.msmt.cz//uch2021b.html].

Osobní údaje, potažmo informace, které uchazeč poskytuje obvykle již v rámci e-přihlášky VŠ, reflektují také specifické případy dle §48 a 49 ZVŠ a od toho se odvíjející podmínky pro přijetí k určitému studiu. VŠ ve smyslu čl. 4 odst. 7 Nařízení Evropského parlamentu a Rady (EU) č. 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), dále jen „Obecné nařízení o ochraně osobních údajů" určuje účely a prostředky zpracování osobních údajů a ve vztahu ke svým uchazečům a studentům je správcem osobních údajů.

Osobní údaje uchazečů potažmo studentů zpracovávají osoby, které jsou v souladu s čl. 29 Obecného nařízení o ochraně osobních údajů k tomu správcem pověřené, což jsou zejména studijní oddělení. Právní základ pro zpracování údajů poskytovaných uchazečem pro účely zajištění přijímacího řízení ze strany VŠ je dle čl. 6 odst. 1 písm. c) Obecného nařízení o ochraně osobních údajů splnění právní povinnosti, která se na správce vztahuje.

Mezi nejvýznamnější obligatorní podmínky pro přijetí ke studiu v bakalářském nebo v magisterském studijním programu na VŠ patří, v souladu s §48 ZVŠ, dosažení středního vzdělání s maturitní zkouškou. Pro přijetí ke studiu v navazujícím magisterském studijním programu postačuje řádné ukončení studia v kterémkoliv typu studijního programu.

V případě přijetí do doktorského studijního programu je nutnou podmínkou pro přijetí uchazeče dle §48 odst. 3 ZVŠ řádné ukončení studia v magisterském studijním programu. VŠ může kromě toho v souladu s §49 ZVŠ fakultativně stanovit další podmínky ke studiu ve smyslu znalostí, schopností, případně zdravotního stavu uchazeče, pokud to vyžaduje povaha studijního programu.

VŠ je povinna, v souladu s §49 odst. 5 ZVŠ, zveřejnit podmínky pro přijetí uchazeče ve veřejné části internetových stránek nejpozději čtyři měsíce před koncem lhůty pro podávání přihlášek ke studiu. Zejména ověřování znalostí uchazeče může probíhat prostřednictvím přijímací zkoušky v souladu s §49 odst. 4 ZVŠ.

O výsledku přijímacího řízení je uchazeč dle §50 ZVŠ spraven rozhodnutím. O přijetí ke studiu do studijního programu realizovaného na fakultě rozhoduje dle §50 odst. 2 ZVŠ děkan. Pokud je studijní program realizován VŠ, rozhoduje rektor. Rozhodnutí děkana, resp. rektora se vyhotovuje v písemné formě a zahrnuje náležitosti dle § 67 odst. 2 SŘ, §68 a §69 SŘ. Po sdělení rozhodnutí o přijetí ke studiu vzniká uchazeči v souladu s §51 ZVŠ právo na zápis do studia. Dnem zápisu do studia se uchazeč stává studentem VŠ.

Online zápis ke studiu na vysoké škole z hlediska GDPR

V rámci výše popsaného procesu přijímání uchazeče ke studiu, kdy poskytování osobních údajů ze strany uchazeče a komunikace s VŠ probíhá většinou na dálku a elektronicky, lze identifikovat několik potenciálně problematických míst týkajících se zpracování osobních údajů.

Mezi nejvýznamnější lze zařadit:

1. Potvrzení zájmu uchazeče zapsat se ke studiu,
2. doložení uchazečova vzdělání dle §48 odst. 1 ZVŠ, respektive dle §48 odst. 4 a §48 odst. 5 ZVŠ u uchazečů, kteří získali vzdělání v zahraničí, případně dalších podmínek pro přijetí ke studiu dle § 49 ZVŠ odst. 1 ZVŠ,
3. ověření uchazečovy totožnosti,
4. předání studentovy podobenky (fotografie) pro účely výroby průkazu studenta dle §57 odst. 1 písm. a) ZVŠ,
5. odsouhlasení a výzva k doplnění osobních údajů studenta při zápisu do studia.

K jednotlivým bodům:

1. Právo na zápis ke studiu vzniká každému uchazeči, který obdržel rozhodnutí o přijetí ke studiu. ZVŠ neukládá uchazeči povinnost se zapsat do studia, v rámci kterého úspěšně absolvoval přijímací řízení, což je pochopitelné, pokud podává přihlášku např. na více VŠ. ZVŠ ovšem ani neukládá uchazeči povinnost projevit „závazně" zájem o konkrétní studium poté, co obdržel rozhodnutí o přijetí. To dále komplikuje VŠ situaci, zejména pokud probíhá celý proces přijímacího řízení až po zápis ke studiu na dálku.

Uchazeč by měl mít možnost v rámci autentizované části informačního systému elektronicky požádat o zápis do studia.

2. V případě prezenčního zápisu uchazeč obvykle dokládá vzdělání dle §48 odst. 1 ZVŠ prostřednictvím úředně ověřené kopie maturitního vysvědčení, případně prostřednictvím úředně ověřené kopie vysokoškolského diplomu (resp. dokladu o ukončení studia), pokud se hlásí ke studiu do navazujícího magisterského studijního programu nebo doktorského studijního programu. Uchazeči, kteří úspěšně absolvovali studia

na školách v zahraničí, dokládají dokumenty dle §48 odst. 4 ZVŠ a §49 odst. 5 ZVŠ.

V případě zápisu, který probíhá na dálku, se jeví jako nejvhodnější prostředek pro předání dokumentu uchazečem předložení dokumentu prostřednictvím autentizované části informačního systému VŠ na základě autorizované konverze. Tato umožňuje převést dokument z listinné podoby do podoby elektronické a zároveň zajistit shodu obsahu elektronické formy dokumentu s listinným originálem připojením doložky o provedení konverze.

Stejný postup lze využít pro doložení podmínek dle § 49 ZVŠ odst. 1 ZVŠ, jsou-li pro studium VŠ vyžadovány (přehled známek ze střední školy, různá osvědčení apod.).

3. V případě prezenčního zápisu se provádí ztotožnění uchazeče studijní referentkou obvykle prostřednictvím předložení osobního dokladu uchazečem.

V případě zápisu, který probíhá na dálku, se nabízí ztotožnění uchazeče prostřednictvím video hovoru se studijním oddělením. Tento způsob ztotožnění uchazeče vyžaduje, aby měl k dispozici laptop, či mobilní telefon s webkamerou a mikrofonem připojený k Internetu a osobní doklad. Během video hovoru uchazeč poskytne svoji podobu a údaje z osobního dokladu. Smyslem je konfrontovat vzhled obličeje uchazeče s podobou na fotografii z osobního dokladu, a dále konfrontovat identifikační a adresní osobní údaje z osobního dokladu s údaji zaznamenanými v informačním systému VŠ z e-přihlášky.

I když budou uchazeči poskytnuty instrukce, jak ztotožnění prostřednictvím video hovoru provádět, není tento způsob vhodný. Představuje riziko zachycení jiných osob během uchazečova ztotožnění, nežádoucí ingerenci do uchazečova soukromí (zejména pokud jde o sociální postavení uchazeče) a v neposlední řadě riziko úniku, či ztráty osobních údajů uchazeče, např. pokud je záznam uložen přímo v nástroji, odkud může být znovu stažen.

VŠ přináší dodatečné náklady vyplývající ze zajištění dostatečného úložného prostoru pro data. V neposlední řadě vyžaduje dostatek času ze strany studijních oddělení, ať už je totožnost uchazeče ověřována v reálném čase, či následně. V případě vyšších stovek nebo tisíců uchazečů se toto jeví jako nereálné.

Jako vhodnější způsob ztotožnění uchazeče na dálku se jeví užití portálu „eidentita.cz“, který nabízí řadu možností od ověření prostřednictvím elektronického občanského průkazu s čipem až po ověření prostřed-

nictvím mobilní klíče e-Governmentu, pokud má uchazeč aktivovanou bankovní identitu.[33] I v těchto případech však můžeme narazit na různá úskalí, jako jsou náklady za ověření prostřednictvím bankovní identity. Uchazeči ze zahraničí, především ze zemí mimo Evropskou unii, kteří nemusejí obdobnými nástroji disponovat. Navíc nedochází k fyzické kontrole osoby, uchazeč může své přihlašovací údaje poskytnout i jiné osobě, která se za něj bude s jeho souhlasem vydávat. Vynucovat zřízení bankovní identity po uchazeči navíc může být velmi problematické.

4. Jedním z dokladů o studiu dle §57 odst. 1 ZVŠ je průkaz studenta, který slouží zejména k ověření jeho totožnosti během studia, umožňuje přístup do poslucháren, laboratoří, seminárních místností, mensy, či kolejí.

V případě prezenčního zápisu ke studiu se studenti fotografují na průkazy obvykle na pracovištích VŠ.

V případě zápisu, který probíhá na dálku, se nabízí možnost, aby student do autentizované části informačního systému VŠ sám vložil svoji podobenku, která bude odpovídat „pasové fotografii" o ideálních rozměrech 35 mm x 45 mm. Student se může nechat vyfotografovat u fotografa, který poskytuje možnost elektronicky exportovat takové fotografie, případně vyfotografovat svépomocí prostřednictvím webkamery svého laptopu, či mobilního zařízení. Je však třeba počítat i s variantou, že bude vložena podobenka jiného člověka, kterému tak bude školní doklad osvědčovat falešnou totožnost.

Je třeba, aby byl student poučen o tom, jak má taková podobenka co se týče rozměru, velikosti dat a vzhledu vypadat. Musí být aktuální, nesmí na ni být zachyceny jiné osoby, v pozadí by měla být např. prázdná stěna. Většina provozovatelů operačních programů Microsoft, Apple, Google a dalších nabízí v rámci obchodu s aplikacemi pro vývojáře software na úpravu (ořezání) takto pořízených fotografií, tak aby naplňovaly podmínky pasové fotografie. Studenti si je mohou nainstalovat do svých zařízení za drobný poplatek.

5. Rozsah zpracovávaných osobních údajů ze strany VŠ jako správce osobních údajů pro účely přijímacího řízení v případě uchazečů a pro účely vedení studijní evidence a zejména vedení matriky studentů dle §88 ZVŠ, respektive dle §3 Vyhlášky a podmínek zveřejňovaných „MŠMT" pro účely sběru matriky SIMS [https://sims.msmt.cz/DataMatriky/PopisDat.aspx] v případě studentů, se podstatným způsobem

33) Podrobněji rozpracováno v Kapitole 1: Identifikace subjektů údajů v online prostředí.

odlišuje. Právní základ pro zpracování osobních údajů pro účely vedení studijní evidence a matriky studentů zůstává stejně jako v případě zajištění přijímacího řízení nezměněn, a to splnění právní povinnosti, která se na správce vztahuje – čl. 6 odst. 1 písm. c) Obecného nařízení o ochraně osobních údajů.

Student by měl být vyzván k doplnění osobních údajů ze strany VŠ prostřednictvím autentizované části informačního systému a zároveň k odsouhlasení těch osobních údajů, které jsou pro uchazeče a studenta společné. Jedná se zejména o identifikační, případně adresní osobní údaje. Jako poslední krok v souvislosti se zápisem do studia by měl student v autentizované části informačního systému VŠ potvrdit, že údaje, které VŠ předal, jsou správné a pravdivé.