Ochrana osobních údajů - Příručka pro knihovny

Tato příručka si klade za cíl konkretizaci povinností vyplývajících knihovnám z 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, známého též pod zkratkou GDPR (dále jen Nařízení). Příručka odráží stav problematiky k 7. 2. 2018. Postupně budou doplňovány další příklady a úpravy podle vývoje legislativy a získaných zkušeností.

Náměty a dotazy

Obsah

Účel příručky a práce s ní

Tato příručka si klade za cíl konkretizaci povinností vyplývajících knihovnám z 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, známého též pod zkratkou GDPR (dále jen Nařízení). Nařízení vstupuje v účinnost 25. května 2018, a zavazuje osoby v České republice přímo, aniž by jej musel provádět zákon. Některé dílčí záležitosti umožňuje či přímo ukládá Nařízení členským státům upravit podrobněji. Bude tedy ještě přijat prováděcí zákon, který pravděpodobně ponese název zákon o zpracování osobních údajů, aby se nepletl se současným zákonem o ochraně osobních údajů[1]. Tento zákon však v době přípravy této příručky dosud přijat nebyl.

Příručka odráží stav problematiky k 7. 2. 2018. Postupně budou doplňovány další příklady a úpravy podle vývoje legislativy a získaných zkušeností. Pro zasílání námětů a dotazů využijte formulář.

Na úvod je třeba říci, že Nařízení není ve věci ochrany osobních údajů zásadním předělem. Základní principy nakládání s osobními údaji a práva subjektů údajů se příliš nemění. Knihovny, které dodržují pravidla současného zákona, by tak neměly mít s přechodem na režim Nařízení zásadní problém. Nařízení přináší změny především v rovině procesní, snaží se o změnu kultury při nakládání s osobními údaji. Každý by tak měl znovu promyslet způsob, jakým nakládá s osobními údaji, a snažit se co nejlépe naplnit zásady Nařízení. Změny v procesní úrovni se výrazněji dotknou především zpracování osobních údajů v informačních systémech, které samy musí být na změny připraveny a umožňovat knihovnám dodržení nastavených principů v souladu s nařízením. Z toho důvodu je příručka rozdělena na dvě obsahově silně propojené části. V první z nich jsou rozvedeny základní principy definované v Nařízení s důrazem na odlišnosti proti dřívější úpravě v zákoně 101/2000 Sb., a jaká opatření by každá knihovna měla zvážit pro dodržení úpravy v Nařízení. Na to navazuje druhá část, která se zaměřuje na práci s osobními údaji v elektronickém prostředí a na praktická opatření, která knihovny mohou využít.
V závěrečné příloze jsou uvedený příklady vzorových řešení, která lze využít jako podklad pro zpracování pravidel v jednotlivých knihovnách.

Cílem příručky je podat informace především srozumitelně a se zaměřením na praktické problémy knihoven. V textu jsou uváděny odkazy na text Nařízení pro případné zájemce o hlubší vhled do problematiky. Jak vyplývá z odstavce výše, příručka neusiluje o to být kompletním univerzálním návodem pro všechny knihovny. Každá knihovna zpracovává osobní údaje odlišně a právě tyto odlišnosti je nutné posoudit. Příručka by nicméně měla být podkladem pro zvážení, jaké údaje a jakým způsobem jsou zpracovávány a zda něco v této oblasti nezměnit. Příručka je určena zejména pro menší obecní a městské knihovny, může ale pomoci v nastavení procesů i v dalších knihovnách, kdy ale pro větší knihovny bude nutné učinit více opatření, naopak v menších mohou být některé části příručky nerelevantní (např. pokud knihovna nevyužívá automatizovaný knihovní systém).

Příručka byla zpracována díky podpoře dotačního programu Ministerstva kultury ČR - Veřejné informační služby knihoven v roce 2018.

Obecné zásady ochrany osobních údajů v knihovnách

Tereza Danielisová

1 Základní pojmy

1.1 Osobní údaj

Osobním údajem je jakákoliv informace, která se týká konkrétního člověka. Nejde jen o údaje, na základě kterých lze tohoto člověka přímo identifikovat jako je např. číslo občanského či čtenářského průkazu, ale i další údaje, které se ho týkají, jako je např. záznam historie výpůjček či výše dluhu. Nezáleží na tom, zda tyto údaje knihovna získala přímo od dotyčného, nebo je k němu později přiřadila, např. na základě jeho čtenářské aktivity.

Nařízení osobní údaje přímo nevyjmenovává, je tedy třeba vždy posoudit, zda knihovna disponuje takovou kombinací osobních údajů, na základě kterých lze určit konkrétního člověka. Přitom není nutné, aby konkrétního člověka dokázala určit sama knihovna, ale

stačí, pokud by to dokázala na základě poskytnutých údajů třeba policie (např. na základě fotografie).

Osobními údaji nejsou údaje o právnické osobě, ani údaje o člověku, který již zemřel. Tyto údaje však můžou být chráněny na základě jiných právních předpisů.

1.2 Subjekt údajů

Subjektem údajů je člověk, o jehož údaje se jedná, například uživatel, návštěvník, zaměstnanec knihovny apod.

1.3 Zpracování osobních údajů

Zpracování osobních údajů je jakákoliv operace s nimi, tedy včetně jejich zobrazení na monitoru počítače, uložení v papírové podobě, přepsání do databáze, oprava, vytvoření kopie, anonymizace apod.

1.4 Správce osobních údajů

Správcem osobních údajů je ten, kdo určuje účel a prostředky konkrétního zpracování osobních údajů, v našem případě tedy provozovatel knihovny[2]. Provozovatele knihovny (jehož pro zjednodušení označujeme též jako knihovnu) dále v textu vždy uvažujeme v roli správce.

1.5 Zpracovatel

Zpracovatelem osobních údajů je ten, kdo pro knihovnu s osobními údaji jakkoli nakládá, nikoli však její vlastní zaměstnanec. Typicky půjde o poskytovatele automatizovaného knihovního systému (dále jen AKS) či toho, kdo pro knihovnu vymáhá pohledávky. Může jím ale být například i společnost Google, pokud knihovna využívá její formuláře či cloudové služby.

2 Základní zásady nakládání s osobními údaji

Základní zásady pro nakládání s osobními údaji Nařízení upravuje v čl. 5. V souladu s těmito zásadami musí provozovatel knihovny dbát na to, aby osobní údaje byly:

- zpracovávány pouze na základě konkrétních právních důvodů (více v kapitolách 5 a 6),
- zpracovávány korektně a transparentně (více např. v kapitole 7.1),
- shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely (více v kapitolách 4 a 6),
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány (více v kapitole 7.4),
- přesné a v případě potřeby aktualizované (více v kapitole 7.3),
- uloženy pouze po dobu nezbytnou pro účely, pro které jsou zpracovávány (více v kapitole 7.4),
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů (více v technické části této příručky).

Tyto zásady je třeba mít na mysli při zavádění jakéhokoli opatření, které se týká osobních údajů. Obecně lze říci, že by osobní údaje měly být zpracovávány v souladu s rozumným očekáváním subjektu údajů a v rámci obvyklého očekávání ve společnosti.

2.1 Odpovědnost knihovny jako správce osobních údajů

Nařízení klade na odpovědnost správce vyšší důraz, než činila předchozí úprava. Je na provozovateli knihovny, aby posoudil míru rizika, kterou jeho zpracování osobních údajů přináší, a přijal tomuto riziku odpovídající opatření[3].

S rozšířením odpovědnosti správců také souvisí zrušení oznamovací povinnosti. Knihovny tedy již nebudou muset ohlašovat nová zpracování osobních údajů Úřadu pro ochranu osobních údajů.

Knihovna jako správce osobních údajů odpovídá nejen za dodržování všech povinností, které z výše uvedených zásad vyplývají, ale také musí být schopna dodržování povinností v kterémkoli okamžiku doložit (více v kapitole 8).

Pokud je knihovna organizační složkou obce či jiné právnické osoby, je vhodné řešit problematiku ochrany osobních údajů v rámci celé organizace.

3 Osobní údaje zpracovávané knihovnou

Aby knihovna byla schopna naplnit povinnosti, které jí nařízení ukládá, je nezbytné, aby měla přehled o všech zpracováních, která provádí, což nemusí být tak samozřejmé, jak se zdá. Dále jsou uvedeny typické případy, kdy knihovny zpracovávají osobní údaje. Je však třeba, aby si každá knihovna vytvořila svůj **vlastní kompletní přehled** (.xlsx).

3.1 Registrovaní uživatelé

Podpisem čtenářské přihlášky uzavře uživatel s knihovnou smlouvu o poskytování služeb, na základě které mu knihovna umožňuje využívat výpůjční a jiné knihovnické a informační služby, a stává se tak uživatelem registrovaným.

Následující výčet osobních údajů zpracovávaných k registrovanému uživateli je pouze ilustrativní. Neznamená, že všechny tyto údaje každá knihovna zpracovává. Některé údaje může knihovna zpracovávat pouze za určitých podmínek, které vyplynou dále z textu!

- identifikační údaje (jméno a příjmení, datum narození, rodné číslo, druh a číslo osobního dokladu, číslo čtenářského průkazu, pohlaví, titul, občanství)
- kontaktní údaje (adresa trvalého pobytu, korespondenční adresa, email, telefon)
- fotografie
- číslo bankovního účtu
- údaj, zda je držitelem průkazu ZTP či ZTP/P
- údaj o vzdělání
- heslo ke čtenářskému kontu
- historie výpůjček
- historie zobrazení konta
- údaje o provedených peněžitých transakcích
- IP adresa a cookie
- údaje o zákonném zástupci
- údaje o vymáhání dluhu
- a další

3.1.1 Děti a jejich zákonní zástupci

Nařízení zdůrazňuje potřebu zvýšené ochrany dětí, spíše však v té podobě, že je třeba jejich zájmům přikládat větší váhu. Často zmiňovaná hranice 16 let, která může být zákonem o zpracování osobních údajů snížena až na 13 let, se vztahuje pouze ke službám informační společnosti, tedy takovým, které jsou poskytovány elektronicky na dálku. Ohledně uzavření právního vztahu s knihovnou platí nadále občanský zákoník, tedy že děti jsou způsobilé k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jejich věku.[4] Hranici 15 let, kterou většina knihoven pro samostatný zápis do knihovny vyžaduje, tak není třeba upravovat.

Smlouvu o poskytování služeb uzavírají jménem dětí jejich zákonní zástupci, knihovna tedy zpracovává i jejich osobní údaje. Pro nakládání s nimi platí víceméně totéž, jako pro nakládání s údaji registrovaných čtenářů.

Vzor knihovního řádu malé knihovny a poučení pro uživatele (.docx)
Vzor přihlášky - děti do 15 let (.docx)
Vzor přihlášky dospělí starší 15 let (.docx)

3.2 Další uživatelé

Uživatelem je pro účely této příručky každý, kdo využívá jakékoliv služby poskytované knihovnou, tedy i ty které nejsou vyhrazeny pouze uživateli registrovanému, např. účastní se akce knihovnou pořádané, využívá internet či knihy ve volném výběru apod. Uživatelem je rovněž každý, kdo se zdržuje v prostorách knihovny.

Údaje o těchto uživatelích knihovna zpracovává, pokud provozuje kamerový systém se záznamem a také, pokud pro poskytnutí služby poskytnutí osobních údajů požaduje (např. registrace na akci pomocí formuláře). Zpracováním osobních údajů může být za určitých okolností i fotodokumentace akce.

3.3 Zaměstnanci

Provozovatel knihovny bezpochyby zpracovává osobní údaje svých zaměstnanců, a to i těch, jejichž pracovněprávní vztah je založen dohodou o práci konané mimo pracovní poměr. Při vytváření přehledu o zpracovávaných osobních údajích je důležité nezapomenout na údaje o uchazečích o zaměstnání a též o bývalých zaměstnancích.

3.4 Smluvní partneři

Jde o fyzické osoby, se kterými knihovna spolupracuje na základě jiných smluv než zaměstnaneckých (příkazní, o dílo), například dobrovolníci, lektoři, stážisté apod., vede-li si jejich seznam.

3.5 Autoři a jiné autority

V katalozích knihoven je možné dohledat nejen jména a příjmení autorů, ale i další osobní údaje včetně data narození. Knihovny také často vytvářejí databáze dalších regionálních osobností. Osobní údaje se nacházejí i v článkových databázích.

4 Účel

Jakmile si knihovna vytvoří přehled, jaké osobní údaje shromažďuje, je třeba ke každému zpracování přidělit účel, proč tak činí. Vymezení účelu je velmi důležité zejména proto, že knihovna smí v souladu se zásadou účelového omezení[5] zpracovávat osobní údaje pouze pro výslovně stanovené účely, které navíc musí být subjektům osobních údajů sděleny. Osobní údaje lze zpracovávat i pro více účelů.

Příklad: Zpracování osobních údajů registrovaných uživatelů může knihovna činit například za těmito účely:

- vedení evidence uživatelů dle knihovního zákona
- poskytování knihovnických, informačních a dalších služeb dle knihovního zákona
- ochrana knihovního fondu
- informování uživatelů o službách a akcích knihovny
- hodnocení spokojenosti uživatelů
- statistika

5 Právní důvody

Zpracování musí vždy probíhat na základě alespoň jednoho z právních důvodů vyjmenovaných v čl. 6 odst. 1 Nařízení, kterými jsou:

- plnění smlouvy (více v kapitole 5.1)
- plnění právní povinnosti (více v kapitole 5.2)
- plnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci (více v kapitole 5.3)
- oprávněný zájem (více v kapitole 5.4)
- ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (více v kapitole 5.5)
- souhlas se zpracováním osobních údajů (více v kapitole 5.6)

Alespoň jeden z těchto právních důvodů tak musí provozovatel knihovny mít ke každému jednotlivému zpracování, tj. ke každému účelu ve vztahu k určité kategorii subjektů. Pokud žádný z těchto důvodů přidělit nelze, pak samozřejmě nemůže zpracování provádět ani osobní údaj žádat. V této kapitole jsou pouze uvedeny jednotlivé právní důvody, příklady právních důvodů pro typická zpracování osobních údajů knihovnami jsou uvedeny v kapitole 6.

5.1 Plnění smlouvy

Provozovatel knihovny může na základě tohoto právního důvodu zpracovávat osobní údaje, které jsou nezbytné pro plnění smlouvy, např. smlouvy o poskytování služeb (přihlášky do knihovny). K těmto osobním údajům tedy nemusí získávat další právní důvod, např. souhlas. Tento právní důvod však lze aplikovat pouze po dobu, po kterou trvá smluvní vztah mezi provozovatelem knihovny a subjektem údajů.

5.2 Plnění právní povinnosti

Právní titul plnění právní povinnosti lze aplikovat v případě, pokud nějaký právní předpis provozovateli knihovny přímo ukládá, aby osobní údaje zpracovával. Musí však jít opravdu o právní povinnost, a nikoliv o pouhé oprávnění. Například k vedení evidence uživatelů je provozovatel knihovny oprávněn, nikoli povinen. Tento právní důvod je však relevantní pro většinu osobních údajů zaměstnanců.

5.3 Plnění úkolu prováděného ve veřejném zájmu

Je-li ke splnění úkolu prováděného ve veřejném zájmu nezbytné zpracovávat osobní údaje, může tak správce činit na základě tohoto právního důvodu. Tento úkol musí mít svůj právní základ, rámec úkolu tedy musí být stanoven zákonem[6], ne však přímo ve

formě právní povinnosti (pak by totiž šlo o jiný právní důvod). Správce má určitou volnost v tom, jakým způsobem úkol ve veřejném zájmu splní, a zda tedy bude k tomuto plnění třeba zpracovávat osobní údaje. Není podmínkou, aby úkol prováděl veřejný subjekt či orgán veřejné správy, podstatné je, aby byl úkol plněn ve veřejném zájmu. Takovým zájmem může být například naplňování práva veřejnosti na informace (více v kapitole 6.7).

5.4 Oprávněný zájem

Oprávněný zájem je na jednu stranu nejvolněji pojatým právním důvodem, na druhou stranu si vyžaduje důkladné posouzení, neboť oprávněný zájem knihovny nesmí převážit nad zájmy subjektu osobních údajů. Ještě důkladněji je třeba vážit zájmy dětí. Před zpracováním osobních údajů z důvodu oprávněného zájmu je tedy třeba provést tzv. balanční test. V jeho rámci je třeba si odpovědět na tyto otázky:

- O jaký oprávněný zájem jde?
- Nelze daného účelu dosáhnout jiným způsobem?
- Jaké mohou být důsledky pro subjekt údajů? (Nejsou nepřiměřené? Jak velké je riziko, že nastanou?)
- Převažuje oprávněný zájem knihovny nad zájmy subjektů údajů?

Odpovědi na otázky ovlivňuje rozsah zpracování či míra zabezpečení. Knihovna tedy může přijmout další opatření, které sníží míru rizika, a tím naklonit výsledek balančního testu ve prospěch zpracování. Veškeré toto posuzování je třeba provést písemně, příklady jsou uvedeny dále v textu.

Oprávněný zájem musí být aktuální a reálný, není možné shromažďovat osobní údaje, protože by se někdy mohly hodit. Může jít o oprávněné zájmy provozovatele knihovny, ale i společnosti jako celku.

Subjekt údajů má právo proti zpracování osobních údajů na základě oprávněného zájmu vznést námitku. Provozovatel knihovny má v takovém případě povinnost znovu posoudit nezbytnost zpracování se zohledněním konkrétní situace konkrétního subjektu osobních údajů. Pokud zájem subjektu převáží a není dán pro zpracování jiný důvod, musí provozovatel knihovny osobní údaje vymazat.

5.5 Ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby

Jde o právní důvod, který pravděpodobně v činnosti knihovny své uplatnění nenalezne.

5.6 Souhlas se zpracováním osobních údajů

Žádost o souhlas musí být srozumitelná a jasně graficky odlišená od jiných sdělení.[7]Souhlas je třeba žádat pro konkrétní účel. Nebude tedy již například možná formulace: „Uživatel souhlasí, aby knihovna zpracovávala jeho osobní údaje v rozsahu a v souladu s účelem uvedeným v knihovním řádu.“

Souhlas musí být poskytnut jednoznačně, např. podepsáním souhlasu na listině, zaškrtnutím nepředvyplněného políčka v listinné či elektronické podobě nebo zasláním e-mailu. Jeho poskytnutí musí být knihovna schopna doložit po celou dobu, po kterou na jeho základě s údaji nakládá.

Souhlas nesmí být podmíněný a musí být odvolatelný. Není tedy možné poskytnutím souhlasu podmiňovat poskytnutí služby, např. v této podobě. „Pokud uživatel nebude souhlasit s poskytnutím rodného čísla, nemůže využívat služeb knihovny.“ Souhlas lze

kdykoli odvolat, není proto vhodné jej vyžadovat v situaci, kdy nelze po odvolání souhlasu údaje přestat zpracovávat, protože je knihovna potřebuje a užívá je na základě jiného právního důvodu. To si lze představit na následujícím příkladu: Abychom mohli uživateli zapůjčit knihovní dokument, musíme znát jeho identifikační údaje. Nemůžeme tedy vyžadovat jeho souhlas s jejich zpracováním, protože v případě jeho nesouhlasu je samozřejmě nemůžeme smazat.

Pokud je možné užít osobní údaje z jiného právního důvodu (viz ostatní právní důvody uvedené v této kapitole), nelze zároveň žádat o souhlas s užitím těchto osobních údajů!

6 Příklady zpracování osobních údajů prováděného knihovnou

6.1 Poskytování služeb registrovaným uživatelům

Provozovatel knihovny v souladu s knihovním zákonem[8] eviduje uživatele, se kterými uzavřel smlouvu o poskytování služeb. Na základě této smlouvy shromažďuje jednak identifikační údaje, jednak kontaktní údaje. Z tohoto důvodu je vhodnější přihlášku do knihovny jako smlouvu označit, ačkoli je jí z podstaty věci, i když se tak nejmenuje. Přihláška/smlouva pak odkazuje na knihovní řád, v němž jsou vymezena podmínky a podrobnosti poskytování služeb.

Účely zpracování osobních údajů jsou

- evidence uživatelů, se kterými má provozovatel knihovny uzavřenu smlouvu,
- poskytování knihovnických, informačních a dalších služeb na základě knihovního zákona a blíže vymezených knihovním řádem a
- zasílání zpráv přímo se vztahujících k plnění těchto služeb.

Právním důvodem ke zpracování osobních údajů je **plnění smlouvy**.

K identifikaci uživatele potřebuje knihovna alespoň jméno, příjmení a datum narození, případně adresu trvalého pobytu. Další údaje potřebuje k zasílání zpráv vztahujících se k plnění služeb (informace o splněných rezervacích, končící výpůjční lhůtě apod.). Je na volbě uživatele, zda pro tyto účely poskytne další adresy, email, telefon, či všechny tyto kontakty. Provozovatel knihovny nemůže na poskytnutí kontaktních údajů s výjimkou adresy trvat a podmiňovat jím přihlášení do knihovny. Pokud však uživatel tyto údaje poskytne knihovně za tím účelem, aby jej mohla v případě potřeby kontaktovat, pak i tyto údaje zpracovává knihovna na základě plnění smlouvy a není třeba speciálního souhlasu k jejich užití. Účel by měl být z přihlášky zřejmý, např. „Následující údaje nejsou povinné, ale v případě potřeby slouží lepší komunikaci s Vámi."

Na základě právního důvodu plnění smlouvy je možné tyto údaje ukládat po dobu trvání smluvního vztahu, tedy po dobu registrace. Ani poté však není nutné mazat osobní údaje okamžitě po vypršení registračního období. Na základě oprávněného zájmu je možné údaje uchovávat ještě nějakou dobu poté, např. jeden rok.

Vzhledem k užití oprávněného zájmu jako důvodu k uchování údajů, je třeba provést balanční test:

- **O jaký oprávněný zájem jde?** Uchování osobních údajů registrovaných uživatelů po skončení registračního období za účelem řešení případných právních nároků, ať již na straně provozovatele knihovny či uživatele, a dále za účelem zjednodušení případné nové registrace uživatele a uchování jeho dat.

- **Nelze daného účelu dosáhnout jiným způsobem?** Sledovaných účelů nelze účinně dosáhnout jinou cestou. V případě anonymizování veškerých údajů o uživateli by nebylo možné ani jeden z výše uvedených účelů naplnit.
- **Jaké mohou být důsledky pro subjekt údajů?** Důsledky pro subjekt údajů mohou být jednak pozitivní, pokud by chtěl reklamovat služby knihovny, jednak negativní, ale přiměřené, pokud by vyšel najevo právní nárok, který vůči němu knihovna má.
- Registrovaní uživatelé považují svůj vztah s knihovnou za dlouhodobý. Přesto, že neuhradí poplatek za další registrační období před vypršením předchozího, považují se za uživatele knihovny a očekávají, že ta jejich data po nějakou uchová. Jednak neztratí svou čtenářskou historii, jednak nemusí znovu vyplňovat přihlášku a administrativa spojená se zápisem se tak výrazně zjednoduší, což je výhoda pro obě strany.
- **Převažuje oprávněný zájem knihovny nad zájmy subjektů údajů?** Zájem knihovny na uchování osobních údajů registrovaných uživatelů po skončení registračního období převažuje nad individuálním zájmem subjektů údajů, aby nebyly jeho údaje uchovány, zejména proto, že osobní údaje provozovatel knihovny uchovává pouze po přiměřenou dobu; nemá-li vůči uživateli právního nároku, nijak je více nezpracovává, dokud není uživatelem osloven.

Na žádost uživatele by měl provozovatel knihovny anonymizovat veškeré osobní údaje, pokud nemá proti danému uživateli právní nároky, a to i v průběhu registračního období. Podmínkou je, že se uživatel vzdá možnosti využívat služeb s registrací spojených i případných reklamací.

Má-li uživatel vůči knihovně dluh, je samozřejmě možné veškeré údaje potřebné k prokázání právního nároku uchovávat, dokud není dluh vymožen. Více v kapitole o vymáhání pohledávek.

Vzor knihovního řádu malé knihovny a poučení pro uživatele (.docx)
Vzor přihlášky - děti do 15 let (.docx)
Vzor přihlášky dospělí starší 15 let (.docx)

6.2 Ochrana knihovního fondu

6.2.1 Ochrana před zneužitím služeb a duplicitními zápisy

Oprávněným zájmem provozovatele knihovny je rovněž zpracování osobních údajů nezbytné pro účely zamezení podvodům.[9] Pro řádné zajištění ochrany knihovního fondu musí mít knihovna dostatečné množství údajů k jednoznačné identifikaci uživatele, kterému je knihovní dokument půjčován.

Za účelem ochrany vypůjčovaného knihovního fondu tak knihovny mohou uchovávat některé dodatečné údaje, např. druh a číslo osobního dokladu a stát, který tento doklad vydal.

Za výše uvedeným účelem některé knihovny uchovávají fotografie uživatelů. Prokázání oprávněného zájmu je v tomto případě složitější, i když ne zcela nemožné. Na zachycení podoby se vztahuje i občanský zákoník[10], svolení dle něj nemusí splňovat požadavky Nařízení. Pokud by knihovna na rozpoznávání obličejů navíc používala speciální software, jednalo by se o zpracování biometrických údajů, na které Nařízení klade další požadavky.[11]

Doporučení: Knihovna by mohla fotografii umístit pouze na čtenářský průkaz a neuchovávat ji ve svých databázích. Účel by tak byl naplněn, aniž by bylo nutné oprávněný zájem prokazovat.

Funkci jednoznačného identifikátoru by dobře plnilo i **rodné číslo**, to však má jako národní identifikátor zvláštní režim[12]. Knihovny by jej tedy mohly využívat **pouze se souhlasem** subjektu údajů, který musí splňovat podmínky dle Nařízení. Souhlas zejména nesmí být podmíněný a musí být odvolatelný. Za těchto okolností není využívání rodných čísel praktické, a proto ho nedoporučujeme.

6.2.2 Kamerový systém

Účelem provozování kamerového systému je zvýšení bezpečnosti veřejného prostoru a ochrana majetku, zejména knihovního fondu před odcizením, k čemuž je provozovatel knihovny povinen dle knihovního zákona[13].

Právním důvodem ke zpracování osobních údajů je **oprávněný zájem** provozovatele knihovny na plnění účelu uvedeného výše. Je tedy třeba provést balanční test:

- **O jaký oprávněný zájem jde?** Monitorování veřejných prostor kamerovým systémem za účelem zvýšení bezpečnosti veřejného prostoru a ochrany majetku, zejména knihovního fondu před odcizením.
- **Nelze daného účelu dosáhnout jiným způsobem?** Sledovaného účelu nelze účinně dosáhnout jinou cestou. Knihovní fond je z podstaty věci umístěn ve veřejně přístupném prostoru.
- **Jaké mohou být důsledky pro subjekt údajů?** Důsledky pro subjekt údajů mohou být jednak pozitivní, pokud se sám stane obětí protiprávního jednání, jednak negativní, ale přiměřené, neboť takové jsou pouze pro ty, kteří jednali protiprávně.
- **Převažuje oprávněný zájem knihovny nad zájmy subjektů údajů?** Zájem na ochraně základních práv a svobod i zájem na ochraně veřejného majetku, zejména knihovního fondu je významným veřejným zájmem. Jako takový převažuje nad individuálním zájmem subjektů údajů, aby nebyl monitorován, zejména proto, že záznamy nejsou zveřejňovány, přístup k nim má pouze omezený okruh osob, jsou užívány pouze v souladu s účelem a jsou uchovávány pouze po nezbytnou dobu.

Samozřejmostí je umístění kamer takovým způsobem, aby opravdu plnily daný účel a nezasahovaly nepřiměřeně do soukromí uživatelů, a důkladné zabezpečení záznamu, aby se k záběrům nedostal nikdo nepovolaný.

Záznamy z kamerových systémů lze uchovávat pouze po dobu nezbytnou ke splnění účelu, tedy přiměřenou k tomu, aby bylo možné zjistit událost poškozující důležité, právem chráněné zájmy, která se odehrála ve sledovaném prostoru, a vyhledat záznam takové události.

Doporučení: Dobou přiměřenou pro uchování běžných záznamů by mohl být týden. Záznamy zachycující škodní událost je samozřejmě třeba uchovat do vyřešení nebo odložení řešení této události.

6.2.3 Vymáhání pohledávek

Užití osobních údajů za účelem vymáhání pohledávek je bezpochyby **oprávněným zájmem** provozovatele knihovny. Za tímto účelem je vhodné uchovat veškeré identifikační i kontaktní údaje dlužníka i údaje dokumentující okolnosti vzniku pohledávky. Osobní údaje lze za tímto účelem uchovávat i v případě, že nebyl určen již při shromáždění údajů, neboť jde o takzvané další zpracování, které je s původním účelem slučitelné.[14]

To vše samozřejmě platí pouze po dobu, po kterou existuje dluh. Jakmile je dluh vymožen, měl by být spis s veškerými údaji zařazen do skartačního řízení a osobní údaje

v databázích po přiměřené době anonymizovány (pokud ovšem dotyčný nadále nevyužívá služeb knihovny).

6.3 Historie výpůjček

Je samozřejmé, že knihovny musí uchovávat záznam o výpůjčkách, které mají jejich uživatelé právě vypůjčené. Stejně jako u identifikačních a kontaktních údajů uživatelů tak činí na základě **plnění smlouvy** a za účelem ochrany knihovního fondu.

Za tímto účelem je legitimní uchovávat historii výpůjček i nějakou dobu po vrácení knihovního dokumentu pro případ, že by provozovatel knihovny zjistil jeho poškození dodatečně. Váha takového **oprávněného zájmu** však s časem klesá.

Vzhledem k tomu, že uživatelé vyžadují zobrazení seznamu výpůjček ve svých profilech a proaktivní informaci o tom, že určitý titul již v minulosti četli, domníváme se, že knihovny mohou za účelem naplnění očekávaného rozsahu poskytovaných služeb uchovávat historii výpůjček po celou dobu registrace, pokud má uživatel zároveň možnost uchování historie odmítnout.

Varianty možných řešení (knihovna může zvolit kterékoliv):

1. Knihovna anonymizuje historii výpůjček po X měsících od ukončení výpůjčky, přičemž zároveň může nabízet uživatelům uchování historie jejich výpůjček na žádost. Právním důvodem pro delší uchování historie je v tomto případě **souhlas** uživatele. Pokud knihovna zvolí tuto variantu, nesmí opomenout požádat o souhlas své stávající uživatele.
2. Knihovna uchovává historii výpůjček po celou dobu existence profilu uživatele s tím, že uživatelům aktivně nabízí možnost, aby mohli požádat o to, aby historie výpůjček delší než X měsíců od ukončení výpůjčky byla bez dalšího průběžně anonymizována
3. Knihovna uchovává historii výpůjček po celou dobu existence profilu uživatele s tím, že uživatelům aktivně nabízí možnost, aby mohli požádat o anonymizaci své historie výpůjček. Anonymizovat nelze historii mladší než X měsíců od ukončení výpůjčky.

Poznámka: Knihovny jsou povinny ke konci roku vykazovat statistiku své činnosti jak svým zřizovatelům, tak i orgánům státu (NIPOS)[15]. Z toho důvodu nelze údaje o výpůjčkách z databáze mazat, nýbrž vždy provádět jejich anonymizaci, ačkoli žadatel samozřejmě v žádosti může užít výrazu „výmaz“ či „smazání“ údajů. Anonymizací zde i jinde v textu je míněn proces, po němž nelze údaje žádným způsobem spojit s konkrétní osobou.

6.3.1 Vyhledávání v katalogu

Pokud knihovna nabízí při vyhledávání v katalogu doporučení na základě historie výpůjček konkrétního uživatele, je vhodné takový nástroj označit a dát uživateli možnost jej nevyužít. Nástroj by neměl filtrováním výsledků omezovat svobodu volby.[16] Bez dalšího ale lze při vyhledávání v katalogu doporučovat knihy například od stejného autora či podobného zaměření.

6.4 Výhody pro skupiny uživatelů

Poskytují-li knihovny výhody uživatelům pouze na základě věku, není třeba kvůli tomu uchovávat další údaje. Jiná je situace, pokud knihovna poskytuje výhody uživatelům, kteří jsou držiteli průkazu ZTP či ZTP/P či studenty, a údaj o tom uchovává. Uživatele

není nutné zatěžovat dalšími administrativními požadavky a předložení dokladu prokazujícího daný stav lze považovat za souhlas se zpracováním tohoto údaje za účelem poskytnutí výhody. Samozřejmé je, že knihovna tento údaj uchovává pouze a jen pro účel poskytnutí výhody.

Poznámka: Vzhledem k tomu, že smyslem existence průkazu ZTP či ZTP/P je získání výhod pro jeho držitele, nikoli uchování údaje o jeho zdravotním stavu, nejde o zpracování „citlivého" údaje.[17]

6.5 Poskytování služeb neregistrovaným uživatelům

Pokud knihovna shromažďuje a po určitou dobu uchovává identifikační a kontaktní údaje uživatelů dalších služeb, např. protože se přihlašují na akci pořádanou knihovnou či protože eviduje uživatele Internetu, činí tak proto, aby mohla službu poskytnout, a tedy z právního důvodu **plnění smlouvy**. Před každým takovým zpracováním je třeba stanovit účel, sbírat jen údaje k tomuto účelu nezbytné a uchovávat je jen po nezbytnou dobu.

6.5.1 Záznamy z akcí pořádaných knihovnou

Pořizování fotografií člověka upravuje především občanský zákoník,[18] což se vztahuje též na pořizování fotografií z kulturních, vzdělávacích a společenských akcí pořádaných knihovnou. Podle této úpravy je možné vyfotografovat či nafilmovat člověka tak, aby bylo možné určit jeho totožnost, vždy jen s jeho svolením. Zároveň je možné takto pořízené snímky šířit obvyklým způsobem (reportáž z akce, nikoli užití na leták či billboard). Svolení nemusí být písemné, může být dáno i mlčky, ale je nezbytné, aby dotyčný o fotografování věděl a nevyloučil ho, resp. měl možnost ho vyloučit. Proto je třeba na pořizování záznamů vždy vhodným způsobem upozornit.

Větší pozornost je třeba věnovat fotografování dětí. Zejména při užití jejich fotografií pro propagaci knihovny je třeba požádat o svolení rodiče. Jde-li o školní akci, pro běžné užití fotografií postačuje, pokud rodiče již dali svolení škole.

Pokud z příležitostně pořízených fotografií nebo záznamů nejsou vytvářeny evidence o fyzických osobách ani nejsou k zobrazeným či zaznamenaným osobám systematicky přiřazovány další osobní údaje, nejde o zpracování ve smyslu Nařízení.

6.6 Marketing služeb knihovny

6.6.1 Přímý marketing

Účelem užití osobních údajů je informování uživatelů o službách a akcích pořádaných knihovnou. Zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z důvodu **oprávněného zájmu**.[19] Podmínkou je, aby knihovna své služby nabízela v rámci rozumného očekávání. To znamená, informovat opravdu jen o svých službách a jen ty osoby, se kterými má knihovna nějaký vztah, tj. buď vlastní uživatele (ne nutně jen registrované) nebo ty, kteří o informace projevili zájem.[20]

Za těchto podmínek není nutné vyžadovat předem souhlas se zasíláním nabídek, je však nezbytné umožnit příjemci, aby se ze zasílání newsletterů mohl snadno odhlásit, a na tuto možnost a způsob odhlášení ho výslovně a srozumitelně upozornit v každé takové zprávě.

A jako vždy při užití osobních údajů z důvodu oprávněného zájmu, je třeba provést balanční test:

- **O jaký oprávněný zájem jde?** Zvýšení návštěvnosti knihovny za pomoci informování uživatelů o službách a akcích knihovnou konaných. Podpora čtenářství a přístupu veřejnosti k informacím. Lepší využití knihovních fondů a informačních zdrojů.
- **Nelze daného účelu dosáhnout jiným způsobem?** Přímý marketing je jedním z nejúčinnějších nástrojů oslovování uživatelů a v tomto smyslu je nenahraditelný.
- **Jaké mohou být důsledky pro subjekt údajů?** Důsledky pro subjekt údajů mohou být jednak pozitivní, neboť se dozví informace, které by ho mohly zajímat, jednak negativní v podobě narušování jeho soukromí.
- **Převažuje oprávněný zájem knihovny nad zájmy subjektů údajů?** Zájem na zvýšení návštěvnosti knihovny převažuje nad individuálním zájmem subjektu údajů, aby nebylo narušováno jeho soukromí, zejména proto, že narušení soukromí je velmi malé a vždy je dána snadná možnost zasílání novinek odmítnout.

6.2.2 Cílený přímý marketing

Za účelem lepšího cílení sdělení může být využíváno některých osobních údajů, což je v přímém marketingu poměrně běžné. Knihovna může použít k zacílení sdělení pouze obecné charakteristiky, jako je věk či pobočka, kterou uživatel navštěvuje. Je například možné poslat pozvánku na akci pro děti pouze rodičům dětí nebo pozvánku na klub pro seniory pouze seniorům.

Naopak jisté riziko může představovat nabízení knih či akcí například podle toho, co konkrétní uživatel dříve četl. Takové profilování nelze dělat bez vědomí uživatele a je třeba mu vždy dát možnost jej odmítnout. Každou takovou funkci je navíc třeba důkladně vážit, zda je v souladu s rozumným očekáváním uživatele, a tedy slučitelná s novým účelem.

6.7 Právo na informace a úkoly knihoven

6.7.1 Bibliografie a katalogy

Knihovny samozřejmě uchovávají základní osobní údaje autorů. Činí-li tak v rozsahu nezbytném pro zpracování bibliografie a poskytování bibliografických a faktografických informací, plní úkol daný jim knihovním zákonem **ve veřejném zájmu**.

6.7.2 Databáze osobností

Složitější je otázka doplňování různých životopisných údajů jednak k autorům, jednak k dalším osobnostem veřejného života. Některé knihovny zpracovávají veřejné databáze regionálních osobností[21]. Obecně je i tato činnost vykonávána v rámci poslání knihoven, jímž je v nejširším slova smyslu zajištění bezbariérového přístupu k informacím a dále pro účely vědeckého či historického výzkumu[22], a tedy **ve veřejném zájmu**.[ ]V tomto případě je však veřejný zájem vymezen jen velmi obecně. O to více je třeba při zpracování údajů o žijících osobách hledat rovnováhu mezi právem konkrétního člověka na soukromí a právem veřejnosti na informace.

Při zpracování každého záznamu je tak třeba zohlednit:

- **Postavení osoby, které se informace týkají** – Nakolik jde o veřejně známou osobu?
- **Charakter informací** – Jde o základní životopisná data nebo o údaje, které by bylo možné považovat za „citlivé“, případně fotografie?
- **Dostupnost informací** – Jde o informace již zveřejněné a veřejně dostupné? Jsou pravděpodobně zveřejněné přímo subjektem údajů nebo alespoň s jeho vědomím?

- **Předvídatelnost užití údajů** – Mohl dotyčný člověk rozumně předpokládat, že by ke zveřejnění jeho údajů v daném kontextu mohlo dojít? (Údaje o autorovi v katalogu knihovny jsou očekávatelné více než údaje o hiphopové tanečnici na stránce regionálních osobností.)
- **Zpřístupnění** – Budou informace zpřístupněny na Internetu všem, pouze přihlášeným uživatelům, nebo budou přístupné pouze v prostorách knihovny?

Pokud je to alespoň trochu možné, měl by provozovatel knihovny dotyčnou osobu informovat[23] o jejím zařazení do databáze a dát jí tak možnost se zpracováním konkrétních údajů nesouhlasit.

6.7.3 Zpřístupňování dokumentů

Zpřístupňování dokumentů je jednou ze základních knihovnických služeb a je zřejmé, že i dokumenty zpřístupňované knihovnou mohou obsahovat osobní údaje žijících osob, zejména pokud jde o periodický tisk.

Za účelem zpřístupňování jsou různé knihovní dokumenty digitalizovány a zpřístupňovány veřejnosti, a to i vzdáleným uživatelům, čímž se stávají přístupnými širšímu okruh osob, a zásah do soukromí těch, jichž se dotýkají, je tak větší. Dohledatelnost záznamů je navíc lepší díky článkovým databázím jako je Databáze českých článků ANL. Větší pozornost tak bude třeba věnovat právům subjektů údajů. Je však nepochybné, že knihovny při zpřístupňování dokumentů i při poskytování faktografických informací a rešerší jednají na základě **veřejného zájmu**, jehož rámec je dán knihovním zákonem.[24]

6.8 Zaměstnanci knihoven

6.8.1 Uchazeči o zaměstnání

Údaje z životopisu uchazeče zpracovává provozovatel knihovny pro účely výběrového řízení a z právního důvodu **plnění smlouvy** (neboť i jednání předcházející uzavření smlouvy lze do tohoto právního důvodu zahrnout). Jakmile však výběrové řízení skončí, neměl by životopisy dále uchovávat, a to ani elektronicky. Pokud si však přeje vytvořit databázi vhodných uchazečů pro případ, že by potřeboval obsadit další pozici, může požádat uchazeče o udělení **souhlasu** s uchováním životopisu pro tento účel. Pokud by naopak považoval za nutné uchovat osobní údaje uchazeče, jehož si zaměstnat z nějakého závažného důvodu nepřeje (blacklist) může tak učinit na základě **oprávněného zájmu**. Vedení takového blacklistu by mělo mít svá pravidla (např. stanovenou dobu uchování) a každý případ musí být dobře odůvodněný.

6.8.2 Zaměstnanci

Většinu osobních údajů zaměstnanců zpracovává provozovatel knihovny za účelem vedení personálně-mzdové agendy a z právního důvodu **plnění právní povinnosti**.[25]Důležitým úkolem provozovatele knihovny je vymezit zpracování osobních údajů zaměstnanců, které provádí a na které právní povinnost nedopadá, což zahrnuje i užití osobních údajů, které provozovatel knihovny shromáždil za účelem plnění právní povinnosti, ale zpracovává je za jiným účelem.

Příkladem takového zpracování může být zveřejnění fotografií zaměstnanců na webu knihovny či uvedení jména na visačkách za účelem podpory komunikace s uživateli, seznamy zaměstnanců ve výroční zprávě, poskytování darů při pracovních výročích a životních jubileích, monitorování zaměstnanců, uchovávání dalších kontaktních údajů. Pro tato zpracování je třeba hledat jiný právní důvod - **souhlas nebo oprávněný zájem**.

6.8.3 Bývalí zaměstnanci

Provozovatel knihovny může uchovávat osobní údaje zaměstnanců i po skončení pracovního poměru. Přiměřenou dobu (doporučuje se 4 roky) tak může činit za účelem své ochrany v případě právního sporu se zaměstnancem, právním důvodem je **oprávněný zájem.** I po uplynutí této doby je nutné po stanovenou dobu uchovávat dokumenty, u kterých to výslovně vyžadují právní předpisy.[26] Je-li knihovna veřejnoprávním původcem dle zákona o archivnictví a spisové službě, vztahuje se na osobní spisy a další dokumenty povinnost uložení po dobu trvání skartační lhůty (viz dále).[27]

Pokud provozovatel knihovny uchovává kontaktní údaje bývalých zaměstnanců ze společenských důvodů, smí tak činit na základě **souhlasu**.

6.9 Spisová služba a skartační lhůty

Většina knihoven je jako veřejnoprávní původce povinna vést spisovou službu[28] a vydat spisový a skartační plán. Skartační plán upravuje skartační lhůty, což je doba, během níž musí být dokumenty uloženy u původce. Vedení spisové služby je **plněním úkolu ve veřejném zájmu**, jeho rámec je stanoven zákonem, ale určení přiměřené délky skartačních lhůt je odpovědností původce – provozovatele knihovny.[29]

Uvedené se týká samozřejmě i dokumentů, které obsahují osobní údaje, jako jsou osobní spisy zaměstnanců, žádosti uživatelů apod. Po dobu skartační lhůty mají být dokumenty uloženy ve spisovně, kam je zamezen přístup nepovolaných osob. Připomínáme, že osobní údaje lze zpracovávat pouze pro vymezený účel. Je-li tedy účelem dalšího uchování pouze umožnění výběru archiválií, nelze údaje po tuto lhůtu užívat jinak, tedy ani do dokumentů nahlížet z jiných důvodů, než je příprava na skartaci.

7 Práva subjektů údajů

7.1 Informování o zpracování osobních údajů

Nařízení klade velký důraz na to, aby informace poskytované subjektům údajů byly úplné, stručné a srozumitelné[30]. Zároveň je toho mnoho, o čem musí provozovatel knihovny své uživatele a zaměstnance aktivně informovat[31]. Splnit informační povinnost správně, a navíc ke každému zpracování, které knihovna provádí, je tedy docela výzva.

Knihovna musí najít vhodný způsob, jak subjekty údajů informovat, aby se k nim to podstatné opravdu dostalo. Pro uživatele může kapitolu o ochraně osobních údajů zařadit do knihovního řádu, ten ale bývá psán spíše formálním způsobem. Zajímavěji jde pojmout sdělení uživatelům na webu knihovny či v informačním letáku. Aby se o těchto informacích uživatelé opravdu dozvěděli, lze je upozornit emailem či plakátkem v knihovně. Odkaz na „podmínky ochrany osobních údajů“ by měli uživatelé vidět, když vyplňují papírovou či elektronickou přihlášku a při každém přihlášení do svého konta. Není ale nutné, aby každý podepsal, že informace opravdu četl.

Zaměstnance menších knihoven může provozovatel knihovny informovat přímo, u těch větších bude vhodnější vyvěsit informace na intranetu. Kromě stávajících zaměstnanců nesmí zapomenout ani na ty, kteří nastoupí později. Ochrana osobních údajů by měla být součástí vstupního školení, a to jak z hlediska nakládání s osobními údaji zaměstnanců, tak z hlediska jejich povinností vzhledem k osobním údajům uživatelů.

Důležitá je také forma sdělení. Sdělení má být pro své adresáty srozumitelné, při informování svých uživatelů proto není vhodné používat právnické termíny z Nařízení a

vlastně ani z této Příručky. Sdělení má být dostatečně konkrétní, obecné fráze nikomu nepomohou. Je ho dobré rozdělit do kapitol, na webu je také možné rozdělit informace do více vrstev, od jednoduchých sdělení k jejich rozvinutí. K některým sdělením navíc Evropská komise slíbila vydat standardizované ikony.

Každému, jehož osobní údaje uchovává, by měl provozovatel knihovny sdělit:

- Kontakt, kam se může ohledně svých osobních údajů obrátit.
- K čemu které osobní údaje knihovna potřebuje.
- Které údaje jsou nezbytné pro uzavření smlouvy. Tato informace může být případně pouze na přihlášce/smlouvě.
- Bližší vysvětlení, proč knihovna uchovává osobní údaje, dělá-li to na základě oprávněného zájmu, např. proč uchovává historii výpůjček.
- Proti kterému zpracování osobních údajů konkrétně může vznést námitku. Jde o ty, které knihovna zpracovává na základě oprávněného nebo veřejného zájmu.
- Kdo další má k osobním údajům přístup. Informaci o tom, že knihovna předává údaje společnosti vymáhající pohledávky, lze uživateli sdělit s předstihem až ve chvíli, kdy je to relevantní.
- Jak dlouho které údaje knihovna uchovává.
- Že má právo zjistit, jaké osobní údaje uchovává knihovna o něm konkrétně; kde je najde, jsou-li přístupné online, např. po přihlášení do čtenářského konta; a kam se obrátit, kdyby chtěl přehled všech zpracovávaných údajů.
- Že tyto údaje může získat i ve strojově čitelné podobě.
- Jak může požádat o opravu osobních údajů, které o něm knihovna zpracovává.
- Jak může požádat o výmaz osobních údajů, za jakých podmínek bude žádosti vyhověno.
- Že může podat stížnost u Úřadu pro ochranu osobních údajů.

Informace by měla být šitá na míru uživatelům konkrétní knihovny. Není tedy možné připravit jednotný vzor, pro inspiraci snad poslouží alespoň příklad.

Příklad informování registrovaných uživatelů

Vzor knihovního řádu malé knihovny a poučení pro uživatele (.docx)
Vzor přihlášky - děti do 15 let (.docx)
Vzor přihlášky dospělí starší 15 let (.docx)

7.2 Právo na přístup a přenositelnost

7.2.1 Právo na přístup

Každý, jehož osobní údaje knihovna zpracovává, má právo vědět, jaké osobní údaje to jsou.[32] Subjekt údajů se může ptát na konkrétní údaje, ale může žádat i seznam veškerých zpracovávaných údajů, tedy nejen těch, které nám sám dal, ale i těch, které později z jeho činnosti vyplynuly. Alespoň první kopii všech údajů navíc musí dostat zdarma a v elektronické formě, pokud nežádá o jiný způsob.

Tento požadavek nemusí být úplně lehké splnit, doporučujeme proto vytvořit si předem postup, alespoň pro případ, kdy o údaje žádá registrovaný uživatel knihovny. Základní údaje by mělo být snadné získat z AKS a v ideálním případě také v on-line čtenářském kontě po přihlášení uživatele:

- identifikační a kontaktní údaje uživatele

- historie výpůjček
- historie načítání průkazu, pokud ji AKS uchovává
- historie přístupu ke čtenářskému kontu přes webové stránky knihovny, pokud je uchovávána
- historie rezervací
- platební historie

Může se ale stát, že bude potřeba dohledat i údaje další, např. o postupu vymáhání jeho pohledávek. K tomu by mohla pomoci správně vedená spisová služba.

Splnit žádost by měl provozovatel knihovny co nejdříve, nejpozději do měsíce. Krom samotných údajů má žadatel právo ještě na některé dodatečné informace[33]. Jde v zásadě o tytéž, které knihovna zveřejňuje v rámci informační povinnosti (viz kapitola 7.1), jen tyto informace konkretizuje vzhledem ke konkrétnímu žadateli.

Před poskytnutím údajů je třeba přiměřeným způsobem ověřit totožnost žadatele. I tady je třeba hledat rovnováhu mezi snahou o vyhovění žádosti a rizikem neoprávněného zveřejnění údajů. Údaje v plném rozsahu je vhodné předat osobně oproti ověření totožnosti, zaslat do vlastních rukou či do datové schránky, a u ostatních je možné postupovat přiměřeně okolnostem.

Ideální je, pokud má k většině údajů uživatel přístup přes své konto, které mu je přístupné po zadání hesla. Typicky se to může týkat e-mailové adresy, telefonního čísla, ale třeba i adresy.[34]

7.2.2 Právo na přenositelnost

Některé osobní údaje má navíc subjekt údajů právo získat elektronicky ve strojově čitelném formátu, tj. takovém, který umožňuje fulltextové vyhledávání. Týká se to údajů, které knihovna zpracovává automatizovaně na základě smlouvy či souhlasu, a zároveň které získala od subjektu údajů, což zahrnuje nejen údaje poskytnuté vědomě, ale též údaje vypozorované na základě používání služby, tj. např. i historii výpůjček.[35]

Smyslem práva na přenositelnost je přenesení osobních údajů z jednoho IT prostředí do jiného. Na žádost subjektu údajů by měl provozovatel knihovny údaje předat přímo jiné knihovně, pokud je to technicky možné. Import takto získaných údajů do jiného systému však v současné době spíše realizovatelný není, na což je vhodné uživatele upozornit. Stejně jako u práva na přístup nesmí provozovatel knihovny zapomenout na přiměřené ověření totožnosti žadatele.

7.3 Přesnost a opravy osobních údajů

Provozovatel knihovny má přijmout rozumná opatření k tomu, aby osobní údaje, které zpracovává, byly přesné a aktualizované. To však nemusí vždy znamenat, že musejí být pravdivé. Pokud subjekt údajů poskytl nepřesné údaje nebo je při změně neaktualizoval, samozřejmě za takovou nepřesnost knihovna neodpovídá. Úkolem provozovatele knihovny je vyjít vstříc těm, kteří žádají opravu svého osobního údaje. Zároveň musí dbát na to, aby chyby nevznikaly jeho nepozorností. Pokud zjistí např. rozpor mezi přihláškou a záznamem v databázi, měl by chybu obratem opravit. Dále by měl označit a nepoužívat osobní údaje, o kterých ví, že jsou nepřesné (např. protože se vrátil dopis s tím, že adresát na adrese nebydlí).

Tip: Umožnit změnu osobních údajů, které není nutné ověřit, přes webový formulář na čtenářském kontě.

7.4 Minimalizace a výmaz osobních údajů

Už od počátku je důležité shromažďovat jen nezbytné osobní údaje. Před každým novým zpracováním musí provozovatel knihovny pečlivě vážit, které osobní údaje k danému účelu opravdu potřebuje.

Příklad: Za účelem poskytování služeb většinou není třeba vědět, do které třídy a školy čtenář chodí.

Jak již bylo řečeno výše, osobní údaje může provozovatel knihovny uchovávat pouze po dobu, po kterou je nezbytně potřebuje pro naplnění stanoveného účelu. Poté je zlikviduje či anonymizuje, aniž by o to subjekt údajů musel žádat.

Poznámka: Povinnost řádného vyřazování dokumentů ve skartačním řízení tím není dotčena, neboť po dobu skartační lhůty jsou osobní údaje uchovávány právě pro tyto účely.

Subjekt osobních údajů má právo žádat o výmaz osobních údajů[36], které o něm knihovna uchovává. Toto právo ale není absolutní. Žádosti musí provozovatel knihovny vyhovět jen v tom rozsahu, ve kterém údaje již nepotřebuje pro účely, kvůli kterým je zpracovával.

Poznámka: Možným způsobem řešení žádostí o výmaz osobních údajů je též anonymizace osobních údajů.

Právo na výmaz se může týkat i osob, které jsou předmětem vyhledávání v databázích vedených knihovnami (Databáze českých článků ANL, Databáze národních autorit apod.). Provozovatel databáze by měl vždy posoudit, zda zájem společnosti, aby uvedená informace byla nalezena při vyhledávání, převáží nad zájmem konkrétního člověka v jeho konkrétní situaci, a vyžádají-li si to okolnosti, pak dotyčného z vyhledávání odstranit přesto, že se jeho jméno oprávněně vyskytuje v původních zdrojích.[37] Uvedené navíc neznamená, že by knihovna měla přestat zpřístupňovat původní zdroje obsahující danou informaci.

O výmazu osobních údajů je třeba informovat též další příjemce, pokud je knihovna některým předala.[38]

7.5 Vyřizování žádostí uživatelů týkajících se jejich osobních údajů

Žadatel vybírá, jak s ním má knihovna při výkonu práv komunikovat. Pokud podá žádost v elektronické formě, odpovědět je třeba, je-li to možné, také elektronicky.

Co nejdříve, ale nejpozději do jednoho měsíce, musí knihovna na podanou žádost zareagovat jedním z těchto způsobů:

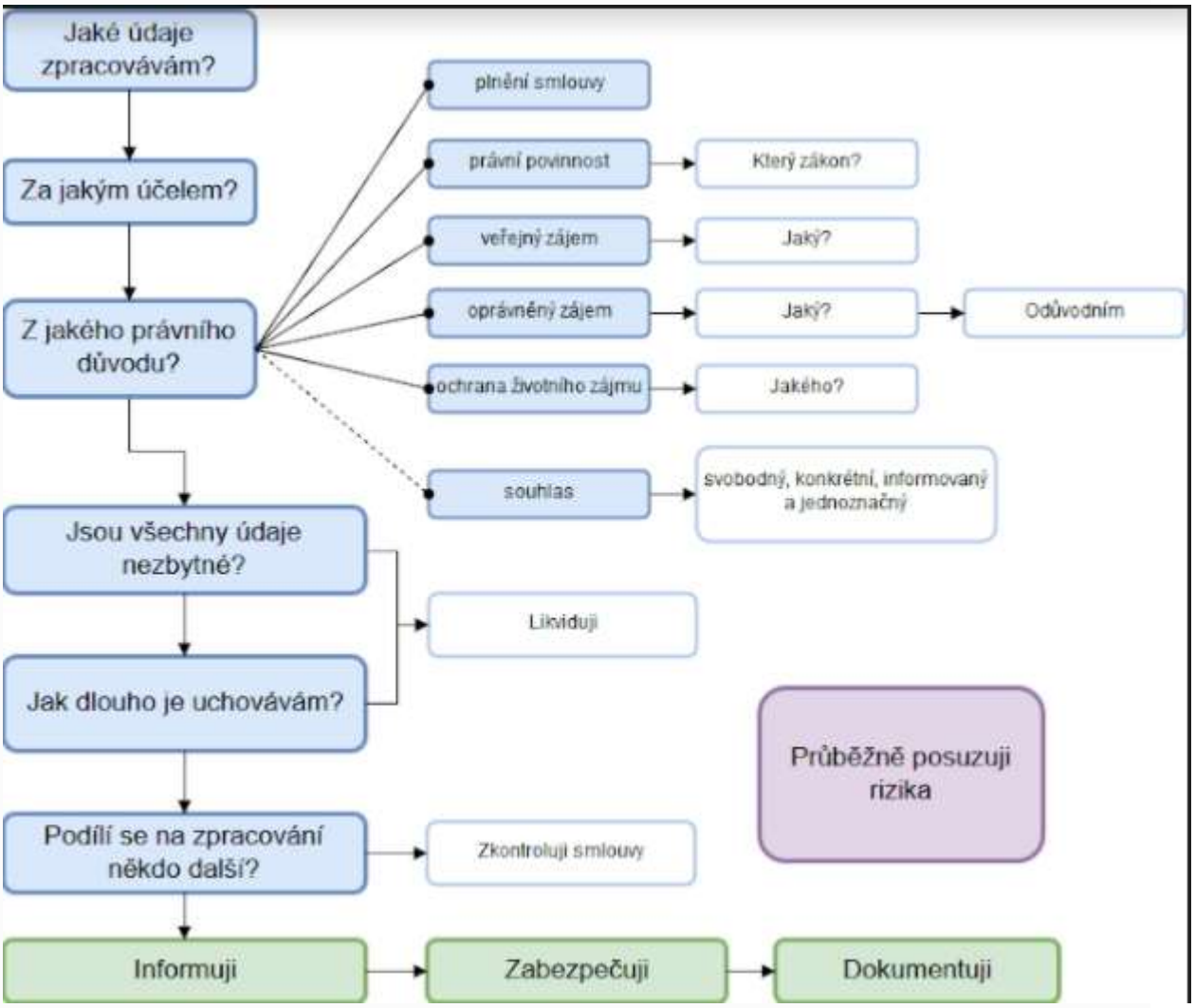
- vyhovět žádosti.
- odmítnout žádost, vysvětlit důvody odmítnutí a informovat žadatele o možnosti podat stížnost k Úřadu pro ochranu osobních údajů a žádat o soudní ochranu.
- pokud je vyřízení žádosti složité, informovat žadatele, že mu bude vyhověno později (maximálně o dva měsíce) a z jakých důvodů.

Na první žádost musí knihovna odpovědět zdarma, pokud však žadatel své žádosti zjevně nedůvodně nebo nepřiměřeně opakuje, může knihovna žádost odmítnout nebo žádat náhradu nákladů.[39]

8 Vnitřní procesy

Jak již bylo řečeno výše, je na provozovateli knihovny, aby doložil, že plní všechny povinnosti, které mu Nařízení ukládá. Je tedy potřeba mít všechny postupy dobře zdokumentované.

Doporučení: Je vhodné shromáždit veškeré obecné dokumenty, které se týkají ochrany osobních údajů, na jednom místě, ať již v šanonu či na zabezpečené intranetové stránce (přehled zpracovávaných údajů, vnitřní směrnice, informace poskytované subjektům údajů, formuláře, smlouvy s dodavateli systémů, doklad o proškolení zaměstnanců, kteří nakládají s osobními údaji, tuto příručku apod.).



8.1 Odpovědný zaměstnanec

Prvním krokem by mělo být určení osoby, která bude v rámci knihovny odpovědná za oblast ochrany osobních údajů. Tedy samozřejmě ne za každý incident, ale za správné nastavení procesů. Může jít o vedoucího či zaměstnance, který bude zvlášť pověřen tímto úkolem.

Někteří provozovatelé knihoven budou navíc povinni jmenovat **pověřence pro ochranu osobních údajů.**[40] Které veřejné subjekty to nakonec budou, bude upravovat zákon o zpracování osobních údajů, který však v době vydání této příručky ještě nebyl přijat. Je pravděpodobné, že povinnost jmenovat pověřence budou mít obce a školy, ale nikoli knihovny, které jsou příspěvkovými organizacemi.

Nařízení upravuje jmenování, postavení a úkoly pověřenců, více je možno nalézt také v Pokynu pracovní skupiny WP29 na úrovni EU.[41]

8.2 Uzavírání smluv se zpracovateli

Jednou z dalších povinností provozovatele knihovny je náležité smluvní zajištění ochrany osobních údajů všude tam, kde do hry vstupuje zpracovatel. V tomto ohledu je třeba dbát již na výběr důvěryhodného zpracovatele, neboť i to je odpovědností provozovatele knihovny. Jak již bylo řečeno výše, zpracovatelem je každý, kdo pro knihovnu jakkoli zpracovává osobní údaje, ne však její vlastní zaměstnanec.

Smlouva mezi provozovatelem knihovny a zpracovatelem musí být uzavřena písemně, což zahrnuje i prostou elektronickou formu. Nařízení nově podrobně vymezuje obsahové náležitosti smlouvy.[42] Téměř určitě tedy bude potřebné uzavřít nové smlouvy nebo dodatky s provozovateli automatizovaných knihovních systémů, poskytují-li software jako službu nebo servis systému, a jsou tedy v postavení zpracovatelů. To se může týkat i krajských a pověřených knihoven, které provozují AKS pro knihovny ve své oblasti. Dle okolností i provozovatelů kamerových systémů, systémů správy zaměstnaneckých dat, ekonomických systémů, systémů spisové služby či osob zabývajících se vymáháním pohledávek pro knihovnu.

Vzor smluvní doložky (příloha - .docx)

8.3 Porušení zabezpečení

Dojde-li k porušení zabezpečení osobních údajů, je to provozovatel knihovny povinen ohlásit Úřadu pro ochranu osobních údajů, a to do 72 hodin od okamžiku, kdy se o něm dozvěděl.[43] Samozřejmě se musí snažit, aby mu něco takového neuniklo a informace o případném incidentu se včas dostala k odpovědnému zaměstnanci.

Není podstatné, zda k porušení zabezpečení došlo v důsledku kybernetického útoku nebo porušením povinností zaměstnance, zda se to stalo záměrně nebo omylem, a zda důsledkem je ztráta osobních údajů nebo jejich neoprávněné vyzrazení, nebo dokonce jen jejich dočasná nedostupnost, např. v případě výpadku proudu. Této povinnosti se zprostí pouze v případě, že je nepravděpodobné, že by toto porušení zabezpečení znamenalo nějakou újmu pro dotčené osoby.

Naopak v případě, kdy by riziko pro subjekty údajů bylo velké, je třeba incident oznámit nejen Úřadu, ale vhodným způsobem i dotčeným lidem, aby mohli podniknout kroky pro svou ochranu.[44] Například v situaci, kdy by unikla hesla, je vhodné všechny upozornit, aby si je změnili i všude tam, kde použili stejné přístupové údaje.

Každé porušení zabezpečení, i takové, které nebylo ohlášeno Úřadu, je třeba zdokumentovat spolu s přijatými opatřeními, která byla přijata ke zmírnění rizik a jejich dopadů.[45]

8.4 Povinnosti zaměstnanců

Provozovatel knihovny odpovídá i za jednání svých zaměstnanců a je jeho povinností zajistit, aby byli se svými povinnostmi seznámeni. Oblast osobních údajů by měla být součástí školení nových zaměstnanců a opakovaně i zaměstnanců stávajících, s důrazem na dodržování všech povinností, které se ochrany osobních údajů týkají.

Lze doporučit i přijetí vnitřních pravidel upravujících povinnosti zaměstnanců, která by měla být dostatečně konkrétní, srozumitelná a zároveň splnitelná. Je vhodné stanovit

základní zásady ochrany osobních údajů, zároveň je ale rozvést do konkrétních povinností konkrétních zaměstnanců.

Vnitropodniková směrnice o ochraně osobních údajů (.docx)

Příklady technických opatření k naplnění souladu s Nařízením

Michal Denár a Pavla Kovářová

V této části se budeme věnovat praktickým stránkám implementace GDPR do prostředí knihoven a to především menších a středně velkých. Text nemá ambice být návodem krok za krokem, ani technickou příručkou pro odborníky na IT. Cílem je doplnit teoretickou část o příklady, které knihovny v souvislosti s Nařízením a informačními technologiemi mohou řešit. Text je určen především managementu knihoven, systémovým knihovníkům a případně i správcům IT systémů jako vodítko k oblastem, jejichž řešením by se v kontextu svých institucí měli zabývat. Předložíme některé praktické příklady, které pomohou pojmenovávat potencionální problematické místa v procesu zpracování osobních údajů a příklady řešení, které mohou přispět ke snížení rizik. Vzhledem k rozsahu této příručky nemůže jít o výčet úplný a aplikovatelný do provozu každé knihovny. Konkrétní řešení je nutné vždy přizpůsobit na míru konkrétní instituci s přihlédnutím k ekonomickým, personálním a technickým podmínkám. S vědomím, že nezanedbatelná část menších knihoven nedisponuje odborníkem na informační technologie, lze vnímat text jako jeden z podnětů, který může pomoci při auditu aktuálního stavu a definici požadavků na případné změny. Konkrétní řešení lze konzultovat například s nadřízenou knihovnou nebo externím dodavatelem.

Prvním krokem k úspěšnému zvládnutí implementace Nařízení je uvědomit si, jaké osobní údaje knihovna využívá, ať už jde o informace o jejích zaměstnancích, uživatelích, příp. spolupracovnících (např. dodavatelé, externisté pracující na dohodu o pracovní činnosti) a dalších lidech (např. lokální osobnosti nebo autoři v databázích spravovaných knihovnou). Dalším krokem je definovat účel zpracování, a zda jsou pro daný účel tyto informace nezbytné, aby bylo zpracováváno co nejmenší množství osobních údajů. Poté následuje vymezení, jak se s informacemi knihovna pracuje a opět zhodnocení, zda není možné zpracování omezit, např. nastavením autorizace, aby k osobním údajům měl přístup skutečně jen ten, kdo nezbytně pro daný účel musí. V opačném případě by bylo složité a ve větších institucích nemožné řídit bezpečnost informací ani určit případného viníka úniků nebo ohrožení bezpečnosti. Přitom v rámci tohoto zpracování je potřeba zvážit, jaká jsou využita bezpečnostní opatření, ať už technická (např. instalace antiviru) nebo fyzická (např. zámek na skříni, kde jsou uloženy pracovní smlouvy). Tato opatření pak nestačí jen zavést, ale je nutné neustále dbát na jejich dodržování (např. důsledným odebíráním klíčů stejně jako přístupových práv od bývalých zaměstnanců, případně jejich omezení po zneužití oprávnění).

To vyžaduje zvážení všech digitálních nástrojů a informačních systémů využívaných pro zpracování osobních údajů. Nejde jen o knihovní systém, kde jsou uloženy záznamy registrovaných uživatelů, ale třeba i o paměťovou kartu, síťové úložiště, poštovního klienta s uloženými e-maily, online dotazník ukládající IP adresu respondenta atd. Ve všech těchto nástrojích je nutné zamyslet se nad využitím bezpečnostních opatření, aby se k informacím dostal jen ten, kdo skutečně má, ale také aby nemohlo dojít k poškození nebo ztrátě informací. V případě, že není možné zajistit soulad s Nařízením, je vhodné daný způsob zpracování opustit a najít alternativu odpovídající požadavkům. Základním (i když ne jediným) opatřením je bezpečná autentizace, pseudonymizace, případně využití šifrování (přenosu i uložených informací). V případě, že jde o online službu

(např. knihovní systém v cloudu), je potřeba myslet na to, že její provozovatel se stává zpracovatelem osobních údajů a je nutné mít s ním vhodně nastavenou smlouvu, aby odpovídala požadavkům Nařízení.

9 Role zaměstnanců při naplňování požadavků GDPR

Při zavádění opatření, která definují chování organizace v oblasti bezpečnosti osobních údajů je klíčová role managementu. Pokud dojde k nepochopení účelu Nařízení nebo dokonce k jeho ignorování ze strany vedení, nebude možné očekávat důsledné vykonávání postupů ze strany podřízených. Nařízení doporučuje zavést opatření za účelem ochrany osobních údajů v oblastech organizačních a technických. Zabezpečení se týká všech osobních údajů bez ohledu na jejich formu a druh zpracování. Týká se tedy jak údajů v elektronické, tak „papírové" podobě. V rámci zavádění opatření do praxe musí být se základními pravidly seznámeni všichni zaměstnanci knihovny. Vedle toho část zaměstnanců, která zpracovává údaje pro konkrétní účel, by se měla podrobněji orientovat v pro ně relevantních oblastech (např. uklízečka a mzdová účetní nemusí být v této oblasti poučeny do stejné míry). Osvěta může mít podobu interních předpisů, se kterými se musí zaměstnanci seznámit. Pravidelně konaná školení v oblasti ochrany osobních údajů přispívají k odstraňování míry nejistoty a jsou důležitým prvkem v řetězci opatření. Účast na nich se dokumentuje prezenční listinou, která se zakládá (doložitelnost provedených opatření).

Při přípravě školení je nutné si uvědomit, proč ho vlastně děláte. Nejde jen o splnění Nařízení, ale především o preventivní opatření, které by mělo mít dopad na reálné chování zaměstnanců. Pokud si tedy objednáte i špičkového lektora – právníka nebo IT specialistu, který přesně zaměstnancům poví, co a jak dělat, ale způsobem, který nepochopí, je efekt školení velmi omezený. Čím cíleněji bude lektor znát prostředí knihovny, ale také pozice a potřeby zaměstnanců, tím lépe může nastavit jeho obsah. Plánování a správné zadání je tedy faktor, který by rozhodně neměl být zanedbáván. V rámci tohoto zadání je možné využít interní předpisy knihovny a výsledky analýz, které údaje, jakým způsobem (včetně využívaných informačních systémů a elektronických nástrojů) a za jakým účelem jsou zpracovávány. Možné je udělat plošné školení s představením základních bezpečnostních opatření v oblasti chování i technických prostředků, pro určité zaměstnance, kteří ale pracují se specifickými údaji, je ale vhodné udělat samostatné školení, kterým nemusí procházet ti, kterých se daná oblast netýká. V rámci školení by měli být zaměstnanci seznámeni nejen s tím, co dělat a co ne, ale také proč jsou tato pravidla stanovena a jaké jsou postihy za jejich nedodržení, protože v opačném případě je pravděpodobné, že budou hledat pohodlnější a méně bezpečné postupy.

V rámci obecného školení by zaměstnanci měli být seznámeni například s následujícími tématy (vždy je ale nutné zvážit potřeby konkrétní instituce):

- Kdo má práva nakládat s jakými osobními údaji. Jedná se o oblast autorizace (kdo má k čemu přístup), což povede k tomu, že bude možné při požadavku odkázat uživatele na jiného zaměstnance, který má přehled o dané oblasti (např. kdo řeší odstranění údajů ze systému na žádost uživatele, ale i kdo má klíče od kartotéky s registračními formuláři uživatelů). Součástí toho je také informace, komu hlásit podezření nebo zjištění bezpečnostního incidentu.
- Správné nakládání s přístupovými údaji, tedy jak má vypadat uživatelské jméno a heslo, jaká nastavení jsou využívána v určitém systému pro podporu silného hesla a jak bezpečně heslo používat (nezapisovat si ho, pravidelně ho měnit atd.).

- Jaká technická opatření a související chování jsou stanoveny na počítačích pro uživatele a zaměstnance (automatické odhlašování, automatické mazání záznamů činnosti na počítači, antivirová ochrana atd.).
- Jaká jsou pravidla pro využívání hardwaru, zejména mobilních zařízení, ale např. i paměťových médií (např. zákaz ukládání nezaheslovaných souborů na flash disk, který může zaměstnanec ztratit).
- Jak ověřit totožnost kolegy a subjektu údajů, co je sociální inženýrství a jakými postupy ho lze rozeznat.
- Jak bezpečně komunikovat, především e-mailem, ale také v jiných využívaných nástrojích (např. sociálních sítích). S tím souvisí i požadavek na mlčenlivost v oblasti osobních údajů.
- Jaké údaje jsou zaznamenávány při použití počítače, internetu a informačních systémů a jak omezit dostupnost těchto záznamů pro neoprávněné osoby (např. využití anonymního okna v prohlížeči).
- Jaké systémy a online aplikace je možné využívat a jakým způsobem, pokud by měly být zpracovávány osobní údaje (např. aby zaměstnanec nevyužil pěkný nový nástroj pro přihlašování účastníků na seminář s uvedením kontaktních informací, kdy ale nebude zajištěna smlouva s tímto zpracovatelem – seznam využitelných nástrojů může být dostupný v intranetu a nový nástroj lze doporučit, ale využitelný je až po zajištění souladu s Nařízením). Na to navazuje i poučení o omezení stahování souborů a instalování programů (instalace by měla být omezena a podléhat schválení IT odporníkem).
- Postup šifrování zvolený v knihovně z hlediska uživatele, který by ho měl využívat (jak zaheslovat soubor, jak poslat šifrovaný e-mail apod.).
- Čeho si všímat při použití IT (např. ikony znázorňující bezpečné připojení, důkladné čtení upozornění a chybových hlášek).
- Jak postupovat pro bezpečné zničení záznamů s osobními údaji (papírová i elektronická skartace, mazání úložišť a paměťových médií, předání odpovědnému pracovníkovi apod.) a kdo je za ně zodpovědný.

Některé bezpečnostní incidenty se mohou dít výhradně v elektronickém prostředí, pak budou pravděpodobně pro většinu zaměstnanců probíhat skrytě. Nicméně je třeba si uvědomit, že každá anomálie v provozu systémů či jejich výpadky mohou (ale nemusí) být průvodním jevem porušení zabezpečení a vzniku rizikové situace pro bezpečnost osobních údajů. Vnitřní předpisy a směrnice musí být jasným vodítkem pro zaměstnance, jaké situace zasluhují jejich pozornost a reakci.

9.1 Rizika při zpracování osobních údajů v knihovnách

Pro snazší orientaci při definici rizik jsme vybrali ty, které se budou týkat pravděpodobně většiny středních a menších knihoven. V prostředním sloupci jsou uvedeny příklady (ne vyčerpávající seznam) opatření týkající se informačních systémů (některé jsou rozvedeny v dalším textu) a pravém sloupci jsou uvedeny související články nařízení.

Riziko	Příklad opatření	Příklady tematicky souvisejících

		článků Nařízení
neoprávněný přístup k údajům	systém uživatelských práv omezující přístup k OÚ silná hesla šifrovaná komunikace zamknutí obrazovky při odchodu od PC informace poskytnout jen osobám, kterých se týkají (ověření identity)	čl. 5, 1., c) čl. 5, 1., f) čl. 12, 6. čl. 32, 1.
neoprávněné zpracování údajů	automatická anonymizace/vymazání po uplynutí stanovené lhůty uchovávání souhlasu v systému, pokud je podmínkou užití odstranění OÚ při obnově ze záloh odstranění OÚ z vyřazené IT techniky a médií dokumentace přijatých bezpečnostních opatření	čl. 5, 1. čl. 7 čl. 17, 1. čl. 17, 2. čl. 24, 1. čl. 32, 1.
ztráta dat	plán záloh záložní zdroje energie péče o hardware	čl. 5, 1., f) čl. 32, 1.
nedostupnost dat	záložní internetová konektivita off-line řešení výpůjčního	čl. 5, 1., f) čl. 15, 1. čl. 20, 1. čl. 32, 1.

	protokolu ochrana proti malware na každé stanici obsluhy existence plánu obnovy v případě selhání HW zveřejnění seznamu zpracovávaných údajů (strojově čitelné)	
neaktuální a nesprávné údaje	proaktivní dotazování uživatele na aktuálnost dat při přihlášení do systému kontrola správného formátu kontaktních údajů (e-mail, telefonní číslo) kontrola logů neúspěšné komunikace a zadání požadavku na vyžádání si aktuálního kontaktního údaje při dalším kontaktu	čl. 5, 1., d) čl. 5, 1., f) čl. 16 čl. 32, 1.

V následujících kapitolách se problematice zabezpečení na úrovni systémů budeme věnovat podrobněji.

10 Opatření ke snížení lidských chyb při komunikaci

I pokud jsou osobní údaje uloženy na pevném počítači nebo v zabezpečené službě, často je potřeba je sdílet nebo jinak s nimi nakládat v rámci elektronické komunikace, a to mezi zaměstnanci (např. předat DPČ na personální oddělení od zaměstnance, který smlouvu s externím zaměstnancem domlouvá) nebo i směrem k subjektu údajů, kterému Nařízení rozšiřuje možnosti v tomto směru – ať už jde o přehled zpracovávaných osobních údajů nebo jejich aktualizaci, kdy Nařízení preferuje právě elektronickou komunikaci.

Aby byla zajištěna bezpečnost osobních údajů, je nutné mít jistotu, že komunikace probíhá výhradně mezi těmi, kdo mají k údajům oprávněný přístup. Znamená to důkladně ověřit totožnost člověka, kterému budou informace sděleny. Toto ověření v elektronickém prostředí obvykle znamená přihlášení do systému (např. k e-mailu). V případě telefonního kontaktu, ale třeba i e-mailu, který není veden jako ten, který patří

žádoucí osobě, je potřeba využít jiných postupů, např. dotazem na informace, které by měl znát jen tento člověk. Je potřeba ale myslet na to, že některé informace jsou známé nejen jemu, takže pokud se zeptáte na adresu a datum narození, určitě to není něco, co by prokázalo totožnost, protože tyto informace zná řada lidí. Vhodné je mít pro podobné účely bezpečnostní klíč, podobně jako to můžete znát z bankovnictví, kde při telefonickém kontaktu chce operátor slyšet číslice na konkrétních místech bezpečnostního klíče.

V případě, že bylo ověření totožnosti v pořádku, je potřeba myslet na bezpečnost samotné komunikace. Velmi jednoduchým řešením, které ale často není využíváno, je využití skrytých kopií při zasílání hromadných zpráv. Po zpřísnění ochrany vlivem Nařízení bude e-mailová adresa také osobním údajem, proto využívání skrytých kopií bude představovat důležité bezpečnostní opatření. Stejně jako u jiných způsobů komunikace je nutné myslet na uložení a přenos a ideálně šifrování obou těchto postupů (podrobněji v 10.1). Přehled forem šifrování e-mailů a srovnání různých nástrojů je možné najít v různých článcích[46]. V případě posílání příloh, kde jsou uvedeny osobní údaje, je pak vhodné tyto přílohy opět šifrovat a heslo poslat jiným komunikačním kanálem (např. sdělit telefonem). V případě využití e-mailových schránek, které nejsou spravovány institucí (typicky freemalů, jako např. Gmail), je nutné myslet na to, že provozovatel služby zpracovává zasílané e-maily, je tedy zpracovatelem podle Nařízení, pokud jsou obsahem e-mailu osobní údaje (viz 12.5).

Ověření totožnosti by ale nemělo být omezováno na přímý kontakt s určitým člověkem. Opět z online bankovnictví (ale i jiných služeb) jsou poměrně dobře známé phishingové útoky. Stejný princip ale je možné využít i při útoku na zaměstnance knihovny, který při podlehnutí poskytne své přístupové údaje neoprávněné osobě. Podstata phishingu spočívá v tom, že přihlašovací údaje jsou sděleny podvodníkovi. Ten nejčastěji využívá podvrženou stránku, jejíž vytvoření je velmi snadné (jednoduše je zkopírován zdrojový kód stránky zobrazitelný v prohlížeči a upraven v cíli, kam jsou odesílány přihlašovací údaje). Typický postup phishingového útoku i základní možnosti jeho rozpoznání jsou popsány v článku od bezpečnostního týmu Masarykovy univerzity[47]. Phishing ale může mít třeba také formu jednoduché žádosti v e-mailu z podvržené adresy, který vyžaduje (většinou s odkazem na bezpečnostní incident) ověření přihlašovacích údajů. Základním krokem je důkladná kontrola adresy (URL i e-mailu), kdy je často využíváno podobnosti znaků a ověřování požadavku na zadání přihlašovacích údajů (např. pokud e-mail vyžaduje činnost v systému, měla by být adresa zadána ručně, ne využit odkaz uvedený v e-mailu, nebo by měl být požadavek ověřen přes kontakt z oficiálního zdroje, ne uvedeného v žádosti).

10.1 Zabezpečení obsahu e-mailové komunikace

E-mail je nejběžnějším komunikačním kanálem, kterým jsou přenášeny osobní údaje. Jeho zabezpečení se však často nevěnuje dostatečná pozornost. Jeho bezpečnost lze zvýšit šifrováním samotného přenosu za pomocí protokolu SSL nebo TLS. Nutným předpokladem však je, že tyto technologie umí použít nejen poštovní server odesílatele, ale i příjemce. Jedině podpora na obou stranách může být zárukou, že obsah komunikace zůstane nečitelným jiným osobám. Často není problém zajistit šifrování na straně odesílatele, ale nikdy dopředu nevíme, je-li chráněn i cílový server.

V případech, kdy tedy chceme e-mailem posílat citlivé údaje, je nutné zjistit si toto předem nebo raději přistoupit k zašifrování celé zprávy. K tomu je ovšem potřeba znát veřejný klíč příjemce, který slouží k zašifrování zprávy. Příjemce musí mít aktuální

certifikát nainstalovaný na svém zařízení a znát heslo, jinak nebude schopen zprávu přečíst. Certifikáty vystavují komerční autority za poplatek nebo je možné využít otevřená řešení zdarma jako je například OpenPGP[48]. Pokud není možné zajistit bezpečný přenos, je vhodnější volit jiné komunikační kanály, například datovou schránku. Je nutné provést analýzu stavu a i s ohledem na četnost zasílání e-mailů s osobními údaji zvolit odpovídající řešení. Následně pak stanovit pravidla pro používání a zabezpečení komunikace.

10.2 Končí e-maily z knihovny „ve spamu“?

Pokud chceme e-mail v knihovně používat k informování uživatelů, měl by to být spolehlivý kanál. Často zprávy odcházejí přímo z informačních systémů a mohou využívat různé poštovní servery. To může přinášet komplikace, protože při nedodržení určitých pravidel mohou být takové zprávy cílovými servery považované za nevyžádanou poštu. Může se pak stávat, že je adresát nikdy nepřečte, protože skončí ve složce spam, místo v doručené poště. Doporučuje se nastavit tzv. SPF (Sender Policy Framework) DKIM (DomainKeys Identified Mail), DMARC (Domain based Message Authentication) záznamy u DNS domény. Správným nastavením lze úspěšnost doručení výrazně zvýšit. Na ověření správnosti nastavení lze použít online nástroje[49].

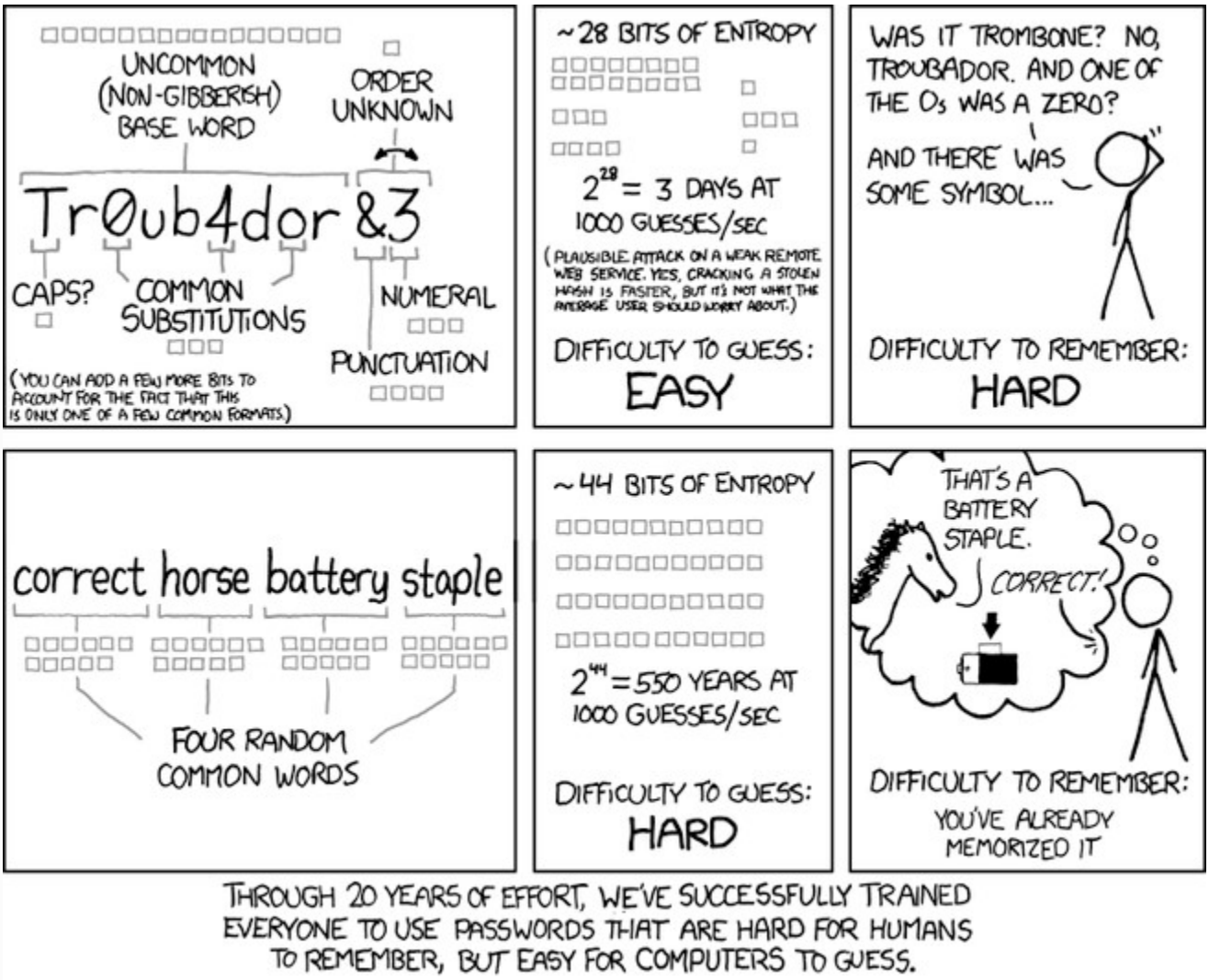
11 Autentizace a autorizace

11.1 Pravidla pro tvorbu a používání hesel

Každý z nás používá hesla pro přístup na různé webové stránky i do množství systémů. Ke zneužití či odcizení hesel dochází velmi často[50]. Za relativně bezpečná se považují hesla o délce minimálně osmi, ale spíše dvanácti znaků složená z malých a velkých písmen, číslic a speciálních znaků. Taková hesla si však většina z nás obtížně pamatuje. Proto spíše volíme hesla nebezpečně krátká a jednoduchá (jména, e-maily atp.) nebo shodná a totožná pro několik stránek. Existuje množství postupů, jak vytvořit heslo pro nás snáze zapamatovatelné a zároveň bezpečné. Lze si představit například takovýto scénář: uživatel si vybere oblíbený krátký citát nebo pasáž z oblíbené knihy. Text zapíše například tak, že třetí slovo začne verzálkou, písmena „o“ nahradí číslicí nula a před poslední slovo vloží emotikon smajlíka. Tímto způsobem si lze poměrně snadno zapamatovat i delší hesla. Kvalitní heslo by mělo splňovat tyto podmínky:

- nebude snadno odhadnutelné: nepožívejte jména dětí, domácích mazlíčků, data narození atp.
- vytvořte heslo co nejdelší s využitím co nejvíce kombinací různých typů znaků
- vyvarujte se často používaným slovům a jejich kombinacím, ideální jsou neexistující slova
- pro každý web nebo službu vytvořte unikátní heslo

Tip: Pokud si chcete otestovat kvalitu svého hesla, můžete využít některou z online aplikací, kdy zadáte typově stejné heslo (není doporučeno zadat skutečně využívané heslo, můžete třeba využít posunutí o určitý počet znaků na klávesnici). Jedna z mála, která zkouší heslo prolomit je dostupná na webu CSIRT týmu Masarykovy univerzity na *https://security.ics.muni.cz/apps/passwords/*

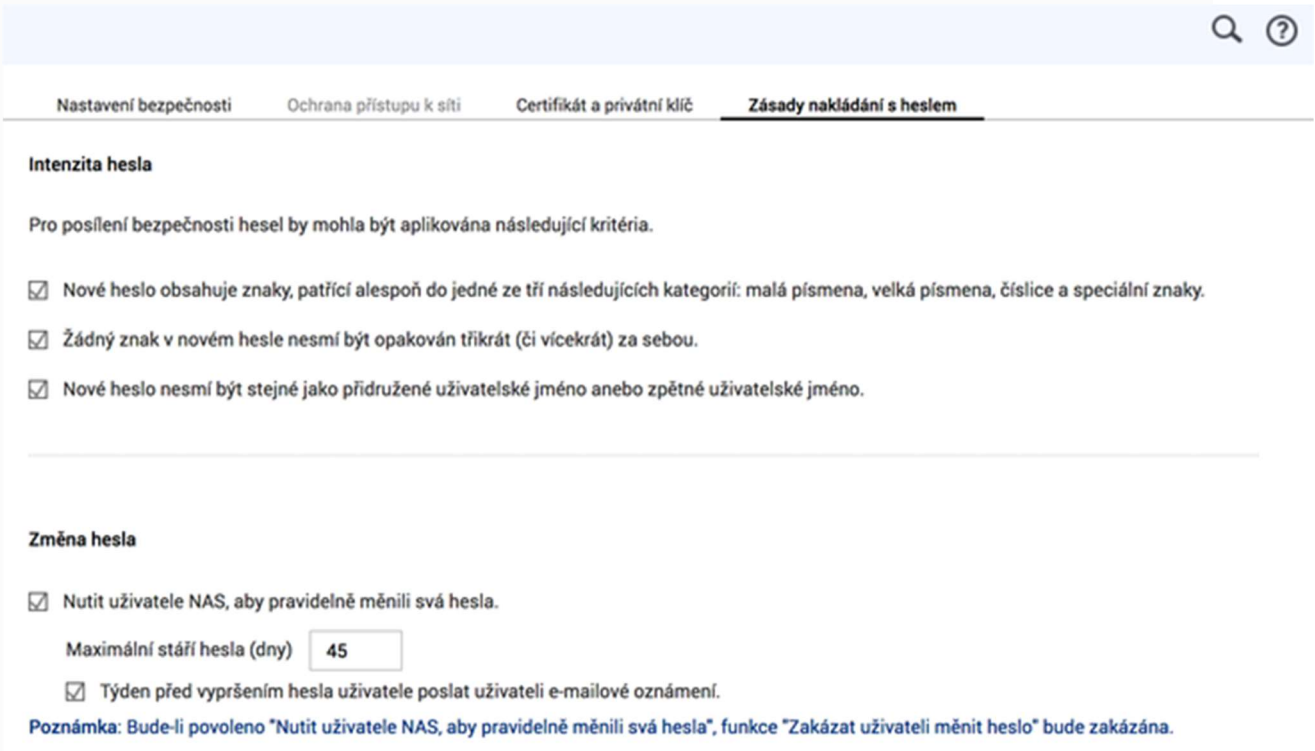


Obrázek 1: Grafický návod, jak vytvořit kvalitní heslo.
Zdroj: https://xkcd.com/936/Vydáno pod licencí Creative Commons Attribution-NonCommercial 2.5 License

Lze také využít některou z mnoha aplikací, které si mohou hesla pamatovat za nás. Aplikace si každé heslo uloží a při přihlašování je vyplní do formuláře. Většina z takových aplikací nabízí také generátor silných hesel, takže si s jejich vymýšlením nemusíte lámat hlavu. Nicméně takový komfort přináší i riziko. Všechna hesla uložená v takové aplikaci jsou často zabezpečena jen jedním hlavním heslem. Pokud by došlo k jeho prozrazení nebo prolomení ochrany aplikace, útočník získá ne jeden přístup, ale všechny. Škody pak mohou být značné. Proto je lze doporučit disciplinovaným uživatelům, kteří si uvědomují možná rizika a dodržují pravidla bezpečného chování v digitálním prostoru. Za bezpečné nelze považovat ani ukládání hesel prohlížečem. Pokud není nastaveno hlavní heslo, jsou všechny uložené přihlašovací údaje dostupné nezašifrované podobě. Ukládání by rozhodně nemělo být prováděno na sdílených počítačích.

Pravidla pro tvorbu a používání hesel by měla být součástí interních předpisů o ochraně osobní údajů. Případně ji mohou definovat a kontrolovat systémy samotné. Často lze definovat minimální délku hesla i povinný výskyt určitých typů znaků. Pokud jsou pravidla navržena s rozumem, pomohou uživatelům a zároveň nedovolí zvolit nebezpečné heslo. Je však nutné vycházet uživatelům vstříc a pravidla vždy nastavit s

ohledem na to, aby bylo možné si vzniklá hesla skutečně zapamatovat a jejich zadávání nezpůsobovalo utrpení. Pak se totiž často stává, že bezpečné heslo skončí nalepené na monitoru a celá snaha o vysokou úroveň zabezpečení vyjde zcela naprázdno.



Obrázek 2: Příklad řešení pravidel pro tvorbu hesel rozhraní zařízení

11.2 Dvoufázové ověření při přihlašování

Bezpečnost přihlašování může být zvýšena zavedením tzv. dvoufázového ověření. Tento způsob získává na oblibě nejen u koncových uživatelů, ale především u správců systémů a serverů. Další stupeň ověření snižuje riziko ohrožení zabezpečení dat v případě prozrazení hesel. Řešení spočívá v přidání dalšího jednorázového kódu spolu s uživatelským jménem a heslem. Takový kód může být generovaný například aplikací na mobilním telefonu[51] či zaslán na registrovaný e-mail nebo telefonní číslo jako SMS. Případně je vytvořen technickým zařízením (např. v USB). Tento druh bezpečnostního opatření můžete znát například z internetového bankovnictví. Výhodou je, že ani případná znalost přihlašovacího jména a hesla nedovolí neoprávněné osobě přístup do systému. Nevýhodou je nutnost mít při sobě zařízení, které slouží k druhé fázi ověření. V případě, že je to mobilní telefon, tak se při jeho nenadálé nefunkčnosti či dokonce ztrátě proces přihlášení komplikuje. Zařízení do USB fungují většinou tak, že na vyžádání uživatele vygenerují jednorázové heslo, které je při přihlášení systémem online ověřeno. Oproti telefonu není tedy nutné kód opisovat, ale je vyžadováno funkční připojení k internetu. Je to tedy řešení vhodné výhradně pro online systémy. V případě ztráty nebo poškození zařízení se již při aktivaci vygeneruje set jednorázových hesel, která lze využít pro přihlášení.

Obrázek 3: Ukázka použití USB tokenu při dvoufázové autentifikaci

11.3 Systém uživatelských oprávnění

Přístup a rozsah možného zpracování osobních údajů je vhodné v informačních systémech řídit. Jedním z nástrojů k tomu určených jsou uživatelská oprávnění. Například knihovnice, která má na starosti akviziční proces a katalogizaci nutně ke své činnosti nepotřebuje přistupovat k osobním údajům čtenářů. Správce systému tedy udělí každému jen taková práva, která odpovídají rozsahu vykonávaných činností. Podobně je to například s právem spouštět skripty nebo výstupy z databáze, které obsahují osobní údaje. K takovým nástrojům by měl mít přístup jen ten, kdo je k tomu kompetentní a je poučený o tom, jak s údaji nakládat. V malých knihovnách, kde často „všichni dělají vše“, lze systém uživatelských oprávnění částečně nahradit interním předpisem, který upraví chování uživatelů při práci s osobními údaji.

11.4 Fyzické zabezpečení

Bylo by chybou domnívat se, že ochrana osobních údajů musí být nutně spojena s investicí do IT či jiných sofistikovaných řešení. Zabezpečení může zvýšit v některých případech pouhé přesunutí monitoru nebo připevnění zábrany, která ztíží přístup veřejnosti za obslužný pult. V prostředí typické městské knihovny lze uvažovat o fyzickém zabezpečení v podobě zdí, zámků a dveří. Rozšířením mohou být pak různé přístupové systémy na bázi čipových karet, turnikety nebo přepážky. Některé větší knihovny mívají u vstupu recepční pult, který lze také považovat za fyzickou bariéru. Vhodnou kombinací univerzálních a speciálních klíčů lze dobře rozdělit prostory na

zóny tak, aby do některých částí měl přístup pouze omezený okruh osob. Počítačové skříně a prvky síťové infrastruktury jsou často vybaveny zámky, aby bylo možné ztížit přístup nepovolaných osob k nim nebo jejich částem.

Mimo provozní dobu knihovny je vhodné využít elektronického zabezpečení prostor knihovny s napojením na centrální pult nebo alespoň se zajištěním přenosu informace o porušení zabezpečení nebo havárií v hlídaném prostoru odpovědným osobám, například telefonicky nebo SMS zprávou.

12 Ochrana kontaktních bodů

12.1 Zaměstnanecké stanice a desktopové aplikace

Rizikem pro zabezpečení osobních údajů jsou lidé a jejich chování v digitálním prostředí. V souvislosti s využíváním informačních technologií by tedy neměla být opomíjena osvěta a vzdělávání (viz 9). Poučený a disciplinovaný knihovník je předpokladem k zajištění funkčnosti systémů a bezpečnosti informací v nich uložených. Samozřejmostí musí být schopnost rozeznat podezřelou přílohu e-mailu, či obezřetnost při instalaci aplikací do počítače.

Ochrana stolních počítačů spočívá především v omezení přístupu nepovolaných osob k aplikacím na nich instalovaných a datům v nich uložených. Ve služebních počítačích mohou být uloženy informace, které jsou osobními údaji. Ty je nutné ochránit v první řadě proti přístupu neoprávněných osob (viz 11). To platí o stanici umístěné ve veřejně přístupné půjčovně, stejně tak o počítači v kanceláři. Rozdílná budou přijatá opatření, která budou odpovídat míře rizika.

Nejčastěji používaným prvkem ochrany proti neoprávněnému přístupu jsou přihlašovací údaje a hesla, která chrání sdílené nebo osobní účty oprávněných uživatelů (viz 11.1). Do informačních systémů musí uživatelé vstupovat svým uživatelským jménem, aby bylo možné zpětně rozlišit, kdo a kdy vykonával transakce nebo měnil údaje. Použitá hesla musí být dostatečně silná a musí zůstat v tajnosti. Jejich tvorba a použití podléhají politice tvorby hesel, která je součástí širší bezpečnostní politiky organizace. Samozřejmostí by mělo být odhlášení uživatele při vzdálení se od počítače (lze podpořit automatickým odhlášením po určité době nečinnosti, ne delší než 10 minut). To nebude činit problémy v neveřejných kancelářích, ale může být problematické zajistit jej na služebních počítačích ve veřejných prostorách, kdy obsluha často opouští své místo při vyřizování požadavků návštěvníků. Je třeba zajistit, aby v takovém čase nikdo nepovolaný nemohl číst z monitoru osobní údaje jiných osob. Neustálé zamykání profilu a následné zadávání hesla při odblokování může být pro obsluhu nepříjemné. A ve svých důsledcích může vést k nedůslednosti. Je tedy dobré kombinovat různá opatření, aby byla ochrana účinná. Moderní operační systémy nabízejí další autentifikační metody (viz 11.2), většinou založeny na biometrických údajích (dvoufázové ověření, otisk prstu, rozpoznání obličeje, sken oční duhovky atp.) nebo na technických řešeních (certifikáty, smart-karty nebo tokeny). Zvolte takové, které je ekonomicky a logisticky vhodné pro konkrétní počítač a informace v něm uložené. Tyto zabezpečovací metody se dají využít i na serverech v aplikacích nebo informačních systémech.

V posledních letech se rozšiřují útoky za pomocí tzv. malware. Škodlivý kód zavlečený do systému umožňuje převzít útočníkovi kontrolu nad systémem, získat uložené informace nebo zneužít zařízení k dalším činnostem. Častým kanálem pro distribuci škodlivého kódu je e-mail. Nákaza často bývá maskovaná jako příloha. Tváří se jako

běžný soubor tabulkového nebo textového editoru, případně jako zdánlivě neškodný odkaz zaslaný známým skrze sociální síť. Opět tedy hraje klíčovou roli člověk, který se rozhoduje, zda infikovanou přílohu otevře. K ochraně přispívá dále používání pouze podporovaných a aktualizovaných operačních systémů, kvalitní antivirové a antispywarové ochrany.

Že malware může představovat skutečný problém i pro knihovny, lze ilustrovat na jednom zdokumentovaném typu útoku. V roce 2017 byl zaznamenán nárůst hackerských útoků[52] skrze protokol Remote Desktop Protocol (RDP), který se využívá ke vzdálenému přístupu k serverům s operačními systémy společnosti Microsoft. Protože některé knihovny využívají tohoto protokolu k připojení tzv. vzdálené plochy, existuje reálné riziko pro jejich systémy a data. Útok spočívá v prolomení slabého hesla ke vzdálené ploše a následnému ovládnutí serveru, které často končí zneužitím stroje k dalším hackerským aktivitám, případně umístěním ransomware. Ten zašifruje soubory na discích, včetně síťových a požaduje za obnovení dat zaplacení výkupného. Obnovení činnosti systémů a záchrana dat bývá ztížena zašifrováním záloh umístěných na discích serveru nebo k němu připojených. Pokud by k takovému incidentu došlo v knihovně, byl by její provoz paralyzován po dobu desítek hodin nebo dokonce dní. Ochranou proti takovému útoku jsou silná hesla a nastavení na straně serveru[53].

Tip: Stále používáte Windows XP? Víte, že to již není podporovaný operační systém a není tedy bezpečný? Na této stránce se dozvíte, kdy skončí podpora různých verzí Microsoft Windows. *Více na http://bit.ly/podpora-windows*

Pokud preventivní opatření selžou a útok se zdaří, lze spoléhat jen na obnovu systému a dat z nenapadené zálohy. Zálohování klíčových systémů a dat by tedy měla být věnována odpovídající pozornost (viz 13).

12.1.1 Specifika zabezpečení mobilních zařízení zaměstnanců

Význam mobilních zařízení v institucích roste a tím rostou i bezpečnostní rizika. Na rozdíl od stabilně uložených zařízení je výrazně vyšší riziko ztráty celého zařízení, případně neoprávněného přístupu k němu a tím i k údajům v nich uložených (nebo přes ně vzdáleně dostupných). Výrobci notebooků, tabletů a mobilních telefonů nabízejí paletu pomůcek, které pomáhají zařízení i jejich obsah ochránit. Je však nutné zvážit, jsou-li dostatečně účinné. Sebedokonalejší ochrana může selhat, pokud si uživatel zjednoduší život až příliš. Například čtyřmístný zámek telefonu nebo jednoduché zamykací gesto lze poměrně snadno odhalit například podle mastných stop na displeji. Doporučuje se kód minimálně šesti, lépe osmimístný. Zařízení dnes často také obsahují čidla, která umožňují ochranu za použití biometrických údajů. Ta poskytují vyšší úroveň zabezpečení, nicméně jsou známy případy jejich překonání.

Chytré telefony s operačními systémy Google Android i Apple iOS umožňují aktivaci služby „najdi telefon/tablet“. Ta v případě ztráty zařízení umožní, pokud je zapnuté a připojené k internetu, na dálku vykonávat různé akce a vidět polohu zařízení na mapě. Lze například napsat vzkaz pro případného nálezce na displej, spustit hlasité zvonění nebo případně i vymazat veškerá data. Aktuální verze operačních systémů chytrých telefonů a tabletů mají automaticky aktivované šifrování souborového systému. Při ztrátě zařízení by tedy nemělo být možné získat soubory a informace bez znalosti kódu, pokud je dostatečně silný. Šifrování disku lze aktivovat i u přenosných počítačů. Pokud zařízení není vybaveno SSD diskem, může se aktivace šifrování projevit pomalejším přístupem k uloženým souborům a vede tedy ke zpomalení běhu samotného operačního systému a aplikací.

K použití mobilních zařízení k ukládání nebo přístupu k citlivým osobním údajům by mělo být přistupováno jako k rizikovému. Pokud je takové použití nevyhnutelné, je nutné věnovat maximální péči zaškolení uživatele a nastavení co nejvyšší úrovně zabezpečení. Organizace by měla zahrnout pravidla provozu mobilních zařízení a jejich zabezpečení do interní směrnice, včetně postupu při jejich ztrátě.

12.2 Počítače určené pro veřejnost

Knihovny v rámci svých služeb standardně provozují veřejně přístupné počítače. Registrovaní čtenáři i anonymní návštěvníci z nich mohou přistupovat do svých e-mailových schránek, tisknout své dokumenty, skenovat nebo stahovat soubory. Při takových činnostech mohu ukládat na disky soubory, které obsahují osobní údaje, někdy i velmi citlivé povahy. Lidé, kteří s počítači pracují, mají různou úroveň počítačové gramotnosti a někteří si nemusí do důsledků uvědomovat míru nebezpečí, která plynou z využívání veřejných stanic. Často před opuštěním počítače své soubory neodstraní a ty pak mohou zůstat přístupné dalším uživatelům. Prohlížením webu může docházet k vytváření historie, uživatelé mohou ukládat svoje přihlašovací údaje nebo se zapomínají odhlašovat ze svých účtů internetových služeb. Knihovna musí osobní údaje svých uživatelů chránit a platí to i v tomto případě. Pouhé upozornění, že uživatelé mají své soubory mazat, není dostatečné.

Možná řešení spočívají ve využití funkce anonymního prohlížení internetu v prohlížečích v kombinaci s automatickým mazáním souborů uložených při sezení. Existují aplikace, které jsou přímo určené pro provoz na veřejných stanicích a nabízejí komplexní nástroje k zajištění bezpečnosti systému a dat uživatelů. Ochrana často funguje tak, že po skočení seance je systém navrácen do stavu před ní. Nevýhodou takových řešení je vysoká cena. Alternativně lze využít možností omezení uživatelů, které nabízí přímo operační systém, doplněné o automatizované odstranění souborů přidaných uživatelem.

12.3 Tiskárny, skenery a reprografická technika

Knihovny nabízejí veřejnosti služby v oblasti tisku a kopírování. Často se tedy stává, že dochází ke zpracování dokumentů, které obsahují osobní údaje, v některých případech i osobní údaje zvláštní kategorie. Je nutné zavést taková opatření, aby nedocházelo k přístupu neoprávněných osob v průběhu zpracování i po něm. Například na veřejných počítačích mohou zůstávat uložené naskenované dokumenty uživatelů. Je nutné zajistit, aby před dalším použitím takových počítačů došlo k bezpečnému vymazání všech uživatelem uložených souborů. K tomu lze využít buď na míru napsaných skriptů, ale i specializovaných aplikací[54]. Obezřetně by mělo být nakládáno také s nepovedenými výtisky dokumentů s osobními údaji. Ty je nejvhodnější před subjektem údajů skartovat nebo mu je předat, aby mohl jejich zničení provést sám.

Při kopírování nebo tisku citlivých dokumentů by měl mít k zařízení přístup jen k tomu určený pracovník, který by měl za všech okolností dodržovat bezpečnost při nakládání s osobními údaji. Moderní tiskárny a kopírovací stroje běžně obsahují paměťová média. Měli bychom zajistit, aby na nich nezůstávalo uložené nic, co obsahuje osobní údaje. Pokud je to možné, preferovaným uložištěm by mělo být výhradně to ve vlastnictví zákazníka služby. Tak budeme mít jistotu, že dokumenty si odnese s sebou a nezůstanou na zařízení knihovny.

12.4 Webové stránky a jiné online aplikace na vlastních serverech

Stejně jako systémy na počítačích v lokálních sítích se zabezpečují i webové stránky a podobné online aplikace (např. OPAC). Základem bezpečnosti je použití silných hesel a

odstupňovaná přístupová práva pro uživatele. U stránek přístupných přes veřejnou síť však do hry vstupuje další úroveň, kdy je nutné monitorovat a případně eliminovat pokusy o proniknutí nepovolaných osob do systémů či databází, které mohou přijít odkudkoli. Politika síťové komunikace a zabezpečení sítě definuje parametry a způsoby ochrany vnitřní sítě organizace.

Stejně jako u operačních systémů je zapotřebí udržovat systém aktualizovaný. Opravy reagují na zjištěná bezpečnostní rizika, pokud nejsou aplikovány, hrozí riziko převzetí kontroly útočníkem nad systémem a ohrožení dat. Kvalitní systémy pro správu obsahu (označované také jako Content Management System) se snaží o proaktivní přístup. V případě, že si knihovna platí externí podporu takových systémů, musí mít smluvně ošetřené podmínky a dodavatelem garantovaná opatření k zajištění bezpečnosti a zajištění provozu. Poměrně často knihovny provozují i CMS systémy s otevřeným zdrojovým kódem a podporu zajišťuje zaměstnanec. Je na zvážení každé instituce, jaké řešení využije s ohledem na důležitost daného systému, personální zajištění nebo na ekonomické možnosti.

Tip: GDPR a oblíbené systémy pro správu obsahu (CMS):

Wordpress
Projekt GDPRWP
GDPR a WordPress

Drupal
GDPR project
Příspěvěk o GDPR na Drupalogy

Joomla
Stránka týmu GDPR
Blokové schéma práce s osobními údaji v Joomla

Jelikož jsou útoky různých robotů na webové systémy velmi časté, lze využít i tzv. webových firewallů, které monitorují nestandardní chování uživatelů na stránkách a automaticky filtrují pokusy aplikovat metody, které používají hackeři k získání kontroly či údajů z databází. Umí také blokovat IP adresy, ze kterých přicházejí takové požadavky nebo se z nich někdo pokouší opakovaně neúspěšně přihlašovat do administračního rozhraní. Samozřejmostí je aktualizace webového serveru a jeho součástí, jako jsou PHP, databázový systém apod. Součástí řešení by mělo být také zabezpečení komunikace protokolem SSL (Secure Sockets Layer), kterému se blíže věnuje kapitola 12.6.

Tip: Chcete zjistit, jak bezpečné jsou vaše webové stránky nebo katalog? Nechejte si je otestovat zdarma Skenerem webu, které provozuje sdružení CZ.NIC. *Více na https://www.skenerwebu.cz*

12.5 Specifika aplikací dodávaných formou služby

Trendem posledních let je přechod z desktopových aplikací, které fungují na lokálních počítačích nebo ve vnitřních sítích, do prostředí tzv. cloudu. Taková řešení přinášejí často úsporu investic, které představuje nákup hardware a zajištění jeho provozu. Pronájmem celé aplikace přesune knihovna značnou část starostí se samotným během serveru na dodavatele. Z pohledu GDPR se takový dodavatel stává zpracovatelem osobních údajů. Je tedy nutné, abychom smluvně ošetřili zabezpečení osobních údajů a zálohování dat, ale dodavatel musí definovat i okruh osob, které mohou mít přístup ke zpracovávaným údajům, a deklarovat způsoby zabezpečení včetně mlčenlivosti dotčených zaměstnanců. Běžnou součástí smlouvy jsou lhůty, za kterých jsou řešeny

výpadky či havárie a smluvní pokuty za jejich nedodržení. Instituce při použití řešení dodaného formou služby (dále jen SaaS) zůstává odpovědná jako správce osobních údajů za jejich bezpečnost a dostupnost. Musí tedy smluvně řešit situace, procesy a vztahy, které v případě běhu aplikace na vlastních serverech řeší interními předpisy. Tento způsob provozu informačního systému může být zajímavý pro menší knihovny, které nedisponují IT specialisty a část agendy outsourcují právě poskytovatelům SaaS, kteří jsou schopni zajistit nejen bezpečnostní dohled, ale i řešení havarijních stavů. Otázkou však zůstává, jak vybrat spolehlivého a důvěryhodného poskytovatele takové služby.

Existuje množství kritérií, které je možné aplikovat při výběru dodavatele SaaS řešení. Z povahy věci by se instituce měla zaměřit na ty, které jsou schopny zajistit odpovídající míru bezpečnosti. Dodavatel by měl být schopen transparentně, a ještě před začátkem smluvního vztahu doložit soulad s GDPR a jakým způsobem zajišťuje ochranu osobních údajů v souladu s Nařízením. Dále jakými způsoby a opatřeními je zajištěna bezpečnost systémů samotných, ale i bezpečnost organizační a personální. V praxi to znamená také, že dodavatel by měl mít vypracovanou komplexní bezpečnostní strategii, která je naplněna souborem procesních opatření. Vše je pravidelně kontrolováno a v případě zjištění nedostatků nebo dokonce incidentů je bezodkladně zajištěna náprava formou revize nastavení procesů a aktualizace metodik, interních nařízení a směrnic. Mělo by být zjevné, že nejde jen o „fráze na papíře“, nýbrž o skutečně prováděné činnosti. Vodítkem mohou být zkušenosti dalších knihoven, které již zvolené řešení provozují a mohou poskytnout cenné informace z běžného provozu i krizových situací.

Obliba používání online nástrojů je značná. Využívají se online formuláře, kooperativní nástroje, plánovače schůzek atp. Pokud jsou do takových nástrojů ukládány osobní údaje, musí mít knihovna smluvně ošetřeno jejich zpracování. Podle dostupných výkladů[55] tato smlouva nemusí být písemná, přesto může být problém ji získat. Lze předpokládat, že nemožné to bude u služeb zdarma (případně u tzv. freemium). Poměrně nejednoznačná situace je u cloudových služeb společnosti Google. Společnost sice deklarovala dopředu soulad s Nařízením[56], ale jen pro služby v rámci placeného balíku G-Suite (knihovny jej mohou získat zdarma[57]). Nicméně v současné době není jasné, jak bude řešena případná smlouva o zpracování a jaké nástroje Google skutečně nabídne například pro výmaz údajů či jejich anonymizaci. Je tedy nutné sledovat situaci a podle ní zvážit další využívání jejich online nástrojů. Například Microsoft veřejně deklaroval soulad s Nařízením u Office 365[58] a to i v oblasti smluvní. Doporučujeme si ověřit aktuální situaci a zajistit případné zpracovatelské smlouvy včas. U služeb, kam se nezadávají osobní údaje, se nic nemění.

12.5.1 Portál Knihovny.cz - Moravská zemská knihovna v Brně jako zpracovatel dat

Portál knihovny.cz se od jiných knihovnických portálů liší tím, že jeho prostřednictvím se mohou uživatelé dostat i ke službám knihoven, které jsou do portálu zapojeny a tedy i ke svým uživatelským údajům. Z tohoto důvodu osobní údaje daného uživatele procházejí skrze servery a síť Moravské zemské knihovny v Brně, která portál Knihovny.cz provozuje.

Na druhou stranu MZK jako provozovatel portálu potřebuje pro jeho provoz dlouhodobě uchovávat jen velmi malou část údajů. Osobní údaje každého uživatele se do MZK přenášejí nejdříve ve chvíli, kdy se uživatel na portál poprvé přihlásí. Velkou většinu osobních údajů přitom portál jen zobrazuje uživateli, nebo je využívá pro další činnosti na základě požadavků uživatele (např. zrušení rezervace, úhrada poplatku apod.).

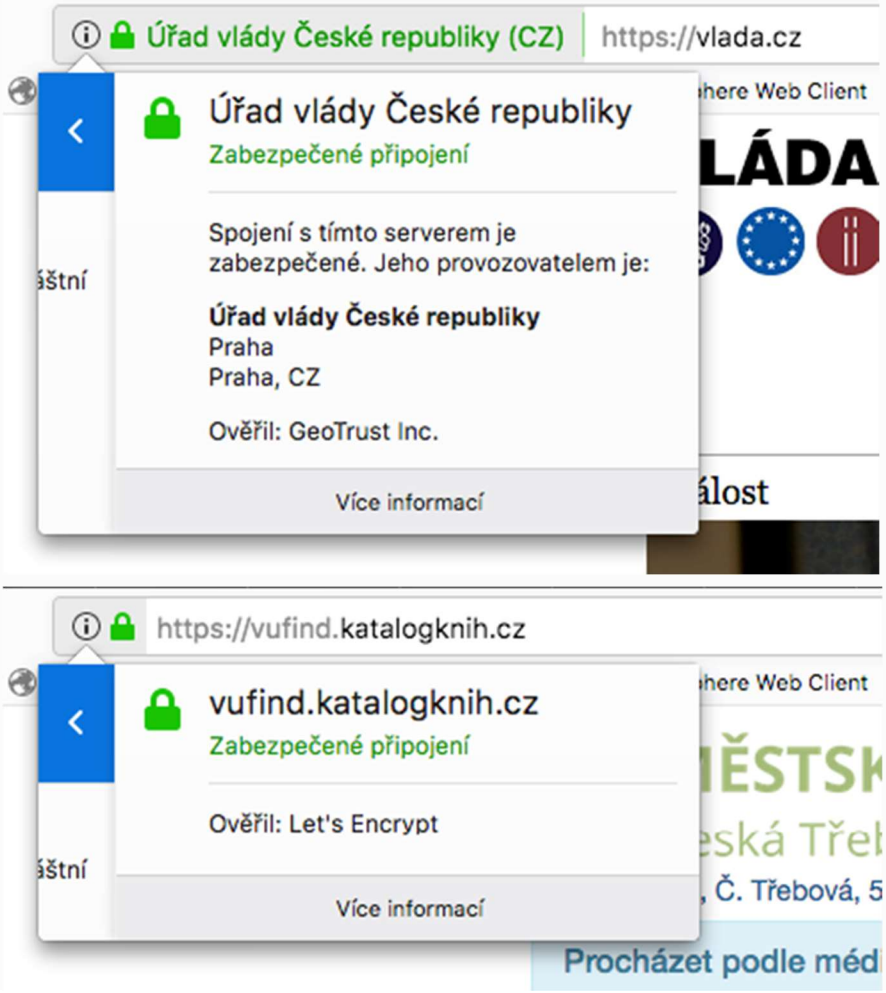
Jedinými údaji, které si portál dlouhodobě uchovává, jsou jednoznačné identifikátory uživatele v knihovních systémech knihoven, zapojených do portálu. Tyto údaje jsou nezbytné k identifikaci uživatele při dalším přihlášení a k propojení účtů uživatele v jednotlivých institucích. Všechny tyto údaje může uživatel kdykoli z portálu smazat tím, že rozpojí navzájem sloučené účty a smaže je z portálu. Údaje o chování uživatelů, které se v rámci portálu archivují, jsou uchovávány v pseudonymizované podobě tak, že je není možné ztotožnit se skutečnými osobami.

Vzhledem k tomu, že MZK osobní údaje sama nearchivuje, je z hlediska bezpečnosti klíčové odpovídající zabezpečení komunikačních kanálů mezi portálem Knihovny.cz a jednotlivými knihovními systémy v zapojených knihovnách a samozřejmě i zabezpečení fyzických a virtuálních serverů na kterých je portál provozován.

MZK připravuje v době psaní tohoto textu zpracovatelskou smlouvu, kterou bude uzavírat s knihovnami zapojenými do portálu.

12.6 Zabezpečení přenosu dat ve veřejné síti internet

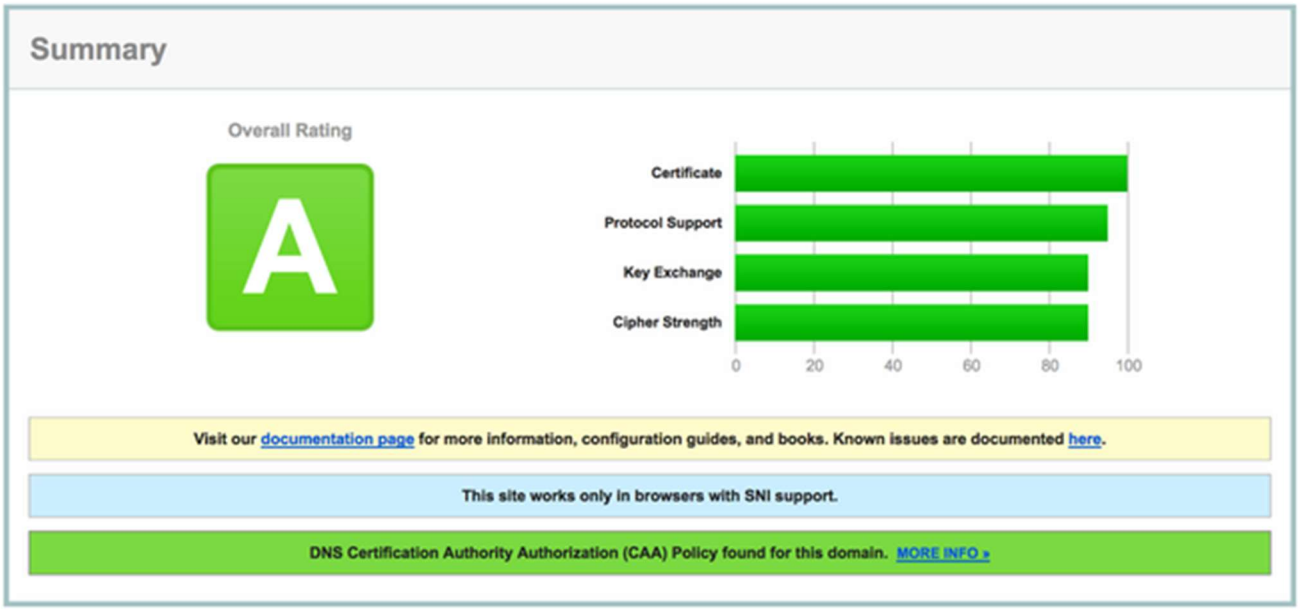
Nařízení neukládá povinně zavádět šifrování jako prostředek k ochraně osobních údajů. Nicméně zavedení SSL jako nástroje k zabezpečení komunikace mezi online aplikací a uživatelem je obecně vnímáno jako standard. Přesto nezanedbatelná část katalogů a webových stránek knihoven tuto ochranu komunikace dosud nenabízí. To je zásadní problém především tam, kde uživatelé zadávají hesla a další citlivé informace, protože jejich přenos po síti probíhá v čitelné podobě a útočník je může získat a zneužít.



Obrázek 4: Dva příklady certifikátů pro SSL zabezpečení komunikace. Horní je komerční s uvedením vlastníka domény (zelený adresní řádek), druhý certifikátem zdarma od Let's Encrypt (bez uvedení vlastníka domény).

Certifikát lze pořídit od komerčních autorit, knihovny zapojené do infrastruktury Cesnet mohou získat certifikáty DigiCert zdarma. Ostatní knihovny mohou využít například řešení Let's Encrypt[59], které umožňuje vystavovat a automaticky obnovovat SSL důvěryhodné certifikáty zdarma. Tvůrce řešení, nezisková společnost Internet Security Research Group, se rozhodla podpořit používání šifrované komunikace na internetu. Vyvinula tedy technické řešení, které od konce roku 2015 poskytuje pod značkou Let's Encrypt. Náklady na zprovoznění jsou spojené převážně s prvotní instalací na server. Služba je nová a logicky se objevují dětské nemoci v podobě nalezených bezpečnostních rizik[60], které se však vývojáři snaží rychle řešit. Každopádně certifikáty od Let's Encrypt se těší značné oblibě a jsou využívanou alternativou ke komerčním certifikátům. Řešení nabízí zdarma nebo za mírný poplatek jako součást svých služeb většina kvalitních webhostingových společností v ČR. Zavedení bezpečné komunikace v prostředí knihovních katalogů, ale i webových stránek by tedy neměl představovat pro knihovny problém a mělo by jít o standard ve všech systémech, kde se pracuje s osobními údaji.

Pokud webová aplikace zabezpečenou komunikaci již používá, je na místě prověřit její kvalitu. Lze využít některé z mnoha služeb k tomu určených[61]. Výsledky testu umožní zhodnotit funkčnost a kvalitu zvoleného řešení, zelený zámeček v adresním řádku prohlížeče nemusí být nutně důkazem, že komunikace je skutečně zabezpečená na potřebné úrovni.



Obrázek 5: Příklad úspěšného výsledku testování SSL certifikátu

Tip: Víte, co znamenají různě barevné zámečky v adresním řádku prohlížeče?

Spojení se serverem je zabezpečené certifikátem SSL. Obsah	*Pokud považujete provozovatele za důvěryhodného,*

	komunikace by měl být chráněný proti odposlechu a změně.	*můžete zadávat bez větších obav své osobní údaje.*
	*Spojení se serverem je zabezpečené certifikátem SSL, ale části webu zabezpečené nejsou. Často se jedná o obrázky či jiný obsah z externích zdrojů. Případně byla uživatelem povolena výjimka z pravidel zabezpečení. Minimálně část komunikace se serverem nemusí být chráněna.*	*Zjistěte si více informací o serveru a jeho provozovateli a případně jej upozorněte na problém se zabezpečením. Raději nezadávejte citlivé osobní údaje.*
	*Spojení se serverem není zabezpečeno.*	*Zde rozhodně nezadávejte žádné osobní údaje ani hesla.*

Doporučení ÚKR: Webové stránky knihoven – přechod na protokol HTTPS (.pdf)

12.6.1 Bezdrátové sítě (wi-fi)

Vzhledem k zamýšlené cílové skupině tohoto textu a rozsahu se příliš nevěnujeme síťové infrastruktuře. Protože však knihovny velmi často nabízejí přístup k internetu přes wi-fi, považujeme za přínosné se věnovat krátce alespoň problematice bezdrátového připojení. Jako důsledek nepříliš obezřetné politiky výrobců bezdrátových síťových směrovačů (routerů) jsou jejich zařízení bezpečnostním rizikem. Problémem je především to, že výrobci nevydávají dostatečně rychle bezpečnostní aktualizace, které reagují na objevené bezpečnostní problémy. Navíc instalace nových verzí jejich softwaru vyžaduje aktivní účast uživatele, který většinou není proaktivně informován o

dostupnosti bezpečnostní aktualizace a nutnosti ji provést. Kvůli tomu jsou směrovače poměrně často zranitelné, čehož lze zneužít k průnikům do sítě či odposlouchávání komunikace uživatelů. Bezdrátové sítě, které nebezpečné zařízení využívají, mohou být tedy potenciálně značně rizikové[62]. Řešením je náhrada nebezpečných zařízení za kvalitnější (aktuálně investice okolo 6500 Kč), která umožňují automatické nebo asistované aktualizace[63]. Klíčovým faktorem pro výběr je rychlost, s jakou jsou výrobci schopni reagovat na vznik bezpečnostních problémů a vydání opravného balíčku.

Pokud má být síť bezpečná pro provozovatele i uživatele, musí být také správně nakonfigurovaná. V tomto ohledu je důležité oddělení veřejně přístupné bezdrátové sítě od sítě LAN, na které jsou umístěny klíčové interní systémy. Moderní bezdrátové routery střední třídy umožňují vytvoření tzv. sítí pro hosty, které dovolují uživatelům přistupovat do internetu, nikoli však do vnitřní sítě instituce. Samozřejmostí by mělo být použití silných hesel pro vstup do administrace a omezení přístupu do ní například jen pro vybrané IP adresy lokální sítě.

Služební bezdrátové sítě je vhodné zabezpečit nejen dostatečně silným heslem a komunikaci zašifrovat (např. protokol WPA2), ale nejlépe i omezit skupinu připojitelných zařízení podle jejich jednoznačných síťových identifikátorů (MAC adresa). Případně využít dalších možností pro zabezpečení přístup do sítě, například protokolem 802.1x. Kvalitní routery disponují nástroji na monitorování a analýzu síťového provozu, které umožní detekovat pokusy o průnik do vnitřní sítě a informovat o nich správce.

12.7 Údaje ve vyřazených IT zařízeních a na paměťových médiích

Skartace papírových dokumentů v knihovnách probíhá naprosto běžně a má svá pravidla daná skartačním řádem. Na tomto místě tedy není nutné ji zvlášť rozebírat. Někdy se může zapomínat na skartaci informací uložených v elektronických zařízeních. Jak již bylo zmíněno, veškerá výpočetní a komunikační technika v praxi také často obsahuje informace, které lze považovat za osobní údaje. Stejné je to s paměťovými médii. Když tato zařízení přestanou být provozu schopná nebo morálně zastarají, dochází k jejich vyřazení a předávají se k likvidaci nebo recyklaci. Než se tak stane, mělo by vždy dojít k bezpečnému vymazání všech údajů. K tomu, aby tato operace byla nevratná a vedla skutečně k definitivnímu odstranění, nestačí běžné „vyhození do koše“ a často ani zformátování média pomocí nástrojů v operačním systému. Pokud chcete mít jistotu, je vhodné sáhnout ke specializovaným aplikacím určeným k vyčištění datových médií[64]. V případě, že je například pevný disk nefunkční a není tedy možné jeho připojení a provedení jeho vyčištění, přikročit k fyzické likvidaci v takovém rozsahu, aby nemohlo dojít k opětovnému přečtení dat z média. Podobný postup je vhodný i pro jednorázově zapisovatelná média jako jsou CD a DVD, poradí si s nimi některé druhy skartovacích strojů. Fyzická likvidace a následná recyklace je vhodná také pro flash disky a paměťové karty všech typů.

13 Zajištění dostupnosti dat a ochrana proti jejich ztrátě a zničení

13.1 Proaktivní opatření

Pravděpodobně nemusíme diskutovat o tom, že nejlepší prevencí před havárií IT zařízení je jejich pravidelná kontrola a obnova. Ekonomická situace některých knihoven však často neumožňuje obnovu počítačů po doporučovaných cca pěti letech, ale stanice a servery slouží často až do momentu selhání. Podobná situace je i u součástí síťové infrastruktury. V tomto ohledu může být řešením již zmíněný přechod na dodávání

systémů formou služby. Před výběrem řešení by vždy mělo dojít k analýze ekonomické stránky i souvisejících rizik.

S klesající cenou výkonných serverů s podporou virtualizace se toto řešení stává dostupné a zajímavé i pro středně velké knihovny. Místo několika fyzických serverů umožní provoz stejného počtu virtuálních, pouze na jednom z nich. Konsolidace je ekonomicky zajímavá, protože cena výkonného serveru je často nižší než provoz a obnova několika méně výkonných. Tento přístup přináší také nové možnosti při zálohování (celé servery) a často také zjednodušení řešení případných havarijních stavů na úrovni jednotlivých virtuálních serverů. Pokud ovšem dojde k havárii fyzického serveru, na kterém běží několik virtuálních, řešíme najednou výpadek více systémů. Vždy je nutné zvážit potřeby instituce.

Řešením může být pronájem celých virtuálních serverů, u kterých přeneseme odpovědnost za jejich funkčnost na provozovatele platformy. Při využití cloudových řešení se stává pro chod kritickou položkou konektivita. Naštěstí ceny za kvalitní a rychlé připojení k síti internet jsou poměrně dostupné a je tak možné pořídit záložní připojení. To může být v porovnání s kapacitou primárního spojení pomalejší, ale v případě jejího výpadku mohou zůstat klíčové systémy funkční, byť odezva bude delší.

13.2 Plán obnovy systémů po havárii či výpadku (též crash plan)

Ve velkých organizacích existují množství bezpečnostních agend, které se věnují také řešení krizových stavů v souvislosti s IT. Menší knihovny nezřídka takové krizové plány vytvořeny nemají a spoléhají často jen na dodavatele svých systémů, že v případě krize zasáhnou. Je užitečné zpracovat si alespoň plán obnovy klíčových systémů (knihovní systém), případně si jej vyžádat od dodavatele. Jde vlastně o předem připravený a otestovaný postup, který je nejvhodnější použít při řešení konkrétního typu havárie nebo po výpadku. Pokud dojde k nějaké nepředvídatelné situaci, je takový návod neocenitelným pomocníkem a dokáže čas výpadku výrazně zkrátit. Když takový plán neexistuje, dochází ke zdržení kvůli zjišťováním informací a zkoušením, často „naslepo“.

13.3 Plán záloh

Zálohování je klíčovou činností při ochraně proti ztrátě dat. Máme-li jako správci osobních údajů zajistit jejich důvěrnost, dostupnost a aktuálnost, musíme se připravit na situace, které si nepřejeme, ale mohou neočekávaně nastat. Čím lépe připraveni budeme, tím menší škody nastanou. Může dojít k technickému selhání serveru nebo paměťových médií. Tato selhání mohou mít původ v zařízeních samotných nebo jsou důsledkem živelných událostí či neopatrnosti obsluhy nebo samotných koncových uživatelů. Bez ohledu na to, jak vzniknou, vždy způsobí problémy a často paralyzují provoz celé instituce. I s ohledem na nařízení GDPR je v zájmu instituce co nejrychlejší znovuobnovení funkčnosti a hlavně opětovné získání plného přístupu k uloženým informacím v plném rozsahu.

Plán záloh je dokument, který by měl obsahovat informace o tom, jak často se zálohy provádějí, kam se ukládají a kdo k nim má přístup. Tento dokument by měl zpracovat správce systému v součinnosti s jeho výrobcem nebo dodavatelem.

Protože zálohy logicky obsahují osobní údaje, je velmi vhodné ochránit je před zneužitím, například šifrováním. K uložištím pak můžeme zřídit přístupy jen vybraným jednotlivcům. Záloha by měla být ukládána ideálně mimo toto úložiště. V menších knihovnách se k ukládání záloh poměrně často využívají síťová úložiště (NAS), ale konkrétní řešení záleží na konkrétním prostředí, potřebách a finančních možnostech.

Případně je možné využít služeb nějakého externího subjektu a ukládat zálohy i mimo budovu knihovny. Tím můžeme ochránit data například v případě požáru či jiné živelné události. Pokud dochází k ukládání záloh k externím subjektům, je nutné analyzovat stávající smlouvy a případně je rozšířit, aby bylo vyhověno požadavkům GDPR.

Zálohování musí probíhat tak často, aby při výpadku nebo havárii nedošlo ke ztrátě dat. V některých systémech se data mění velmi málo, v knihovním systému naopak proběhne velké množství transakcí i v průběhu jediného dne. Vždy je tedy nutné provést analýzu a jejím základě určit odpovídající četnost záloh. Například u zmíněného knihovního systému nebude mít valného smyslu udržovat zálohy staré více než několik dní, protože neobsahují aktuální údaje. Ze zálohy musíme být schopni obnovit všechny údaje, které systém obsahoval před havárií nebo výpadkem systému. Při obnově dat musí dojít ke kontrole, neobsahují-li údaje, které již nemáme právo zpracovávat.

14 Jak zajistit naplnění povinnosti přenositelnosti dat v systémech

Nařízení dává každému subjektu zpracování možnost požádat správce o vydání osobních údajů, které správci poskytl na základě smlouvy nebo souhlasu, případně jejichž zpracování se provádí automatizovaně. Klíčem k úspěšnému naplnění této povinnosti je dokonalá znalost rozsahu údajů a jejich umístění v jednotlivých systémech instituce. Pravděpodobně se totiž nebudou nacházet pouze na jednom místě. Musíme tedy mít předem zpracovanou jakousi mapu, která nám pomůže vybrat systémy, kde budeme přítomnost údajů ověřovat.

Nařízení uvádí, že správce musí údaje předat ve strojově zpracovatelném formátu, přesný formát ale nestanoví. Můžeme uvažovat o běžně používaných formátech, které nejsou zatíženy licenčními podmínkami a nenutí uživatele k otevření použít konkrétní nástroj. Lze tedy uvažovat o CSV, XML, JSON a podobných. Zvolené kódování by mělo být opět zvoleno nediskriminačně, což nejlépe splňuje UTF-8, které by nemělo činit problémy v žádném z běžně používaných operačních systémů a aplikacích pro práci s uvedenými formáty. Rozsah údajů, kterých se týká přenositelnost, je upřesněný v kapitole 7.2.2., měl by obsahovat především přímo poskytnuté údaje (jméno, adresa, e-mail…), ale i údaje vypozorované, tedy i historii výpůjček.

Vzhledem k povaze údajů bude pravděpodobně nejvhodnější volit osobní předání uživateli po ověření jeho totožnosti uložením na jeho paměťové médium. Případně lze uvažovat i o odeslání zašifrovaného souboru na ověřený e-mail nebo datovou schránku.

14.1 Pomocné nástroje pro zajištění aktuálnosti a správnosti údajů

Nařízení klade důraz i na to, aby správce i zpracovatelé věnovali pozornost aktuálnosti a správnosti údajů. Toto lze dosáhnout vhodným nastavením procesů, ale existují i způsoby, jak s úspěchem zapojit technologii. Například kontrolu aktuálnosti kontaktních údajů bude knihovna vykonávat častěji než při prodlužování registrace. Doplněním může pak být proaktivní výzva k odsouhlasení aktuálnosti údajů po přihlášení uživatele do jeho konta. Dalším účinným nástrojem v boji za aktuální údaje je analýza neúspěšné elektronické komunikace. Z ní lze získat informace o tom, na jaký e-mail nebo telefonní číslo se nepodařilo zprávu doručit. K odpovídajícímu kontaktu lze připojit poznámku, která bude instruovat obsluhu, aby o této skutečnosti uživatele informovala a získala funkční telefonní číslo nebo e-mail. Podobně lze zobrazit upozornění přímo v kontě a vyzvat k zadání aktuálního kontaktu.

Chyby vznikají již při zadávání do systémů, jejich počet lze snížit například implementací validátoru pole pro telefonní čísla nebo e-mailové adresy. Přímo při zadávání je zadaný

údaj zkontrolovaný na správný formát: telefonní číslo musí mít 9 číslic, první tři číslice musí být z určené série. E-mailová adresa musí obsahovat znak "@“ a tečku, za kterou následuje kód domény.

14.2 Odvolatelnost souhlasu a informační systémy

Důraz na institut odvolatelnosti souhlasu v praxi může přinést nové požadavky na systémy. Příkladem může být schopnost systému zaznamenávat souhlasy i jejich odvolání. A to pokud je změna na žádost subjektu provedena knihovnou nebo subjektem samotným, například v rozhraní osobního konta. Na úrovni rozhraní budou souhlasy většinou reprezentovány zaškrtávacími poli. Souhlas a jeho případné odvolání se pak bude ukládat do logovacího souboru systému. Ten by měl obsahovat časové razítko, identifikaci původce změny, identifikaci subjektu a nové nastavení souhlasu. Protože souhlas musí být svobodný, jednoznačný a informovaný pro každý účel zpracování, měl by být formulář doplněn vysvětlením, co jednotlivé volby v praxi znamenají pro uživatele. Souhlas musí být vždy výsledkem akce uživatele (ne tedy předvyplněný).

Knihovní systém by měl být schopen evidovat udělení souhlasu. Pokud to neumožňuje, musí být zaznamenán jinak, například na přihlášce. Změny mohou být prováděny knihovníky při návštěvě nebo lze nabídnout tuto možnost přímo v kontě uživatele. Každý si může nastavení kdykoli změnit, podle svých aktuálních potřeb.

V teoretické části této příručky (kapitola 6.3.) jsou uvedeny tři možné varianty přístupu k historii výpůjček. Knihovní systém by pak měl nabízet odpovídající technické řešení pro případy odvolání souhlasu, pokud jsou uchovány na jeho základě.

1. Knihovna anonymizuje historii výpůjček po X měsících od ukončení výpůjčky, přičemž zároveň může nabízet uživatelům uchování historie jejich výpůjček na žádost. Právním důvodem pro delší uchování historie je v tomto případě **souhlas** uživatele. Pokud knihovna zvolí tuto variantu, nesmí opomenout požádat o souhlas své stávající uživatele.
   V této variantě knihovní systém umí automaticky anonymizovat všechny výpůjčky po uplynutí X měsíců po vrácení výpůjčky u čtenářů, kteří nedali souhlas s uchováním historie. Ostatním ji uchovává. Při odvolání souhlasu dojde k jednorázové anonymizaci záznamů ukončených výpůjček, které jsou starší než X měsíců.
2. Knihovna uchovává historii výpůjček po celou dobu existence profilu uživatele s tím, že uživatelům aktivně nabízí možnost požádat o to, aby historie výpůjček starší než X měsíců od ukončení výpůjčky byla bez dalšího průběžně anonymizována.
   V této variantě knihovní systém umí automaticky anonymizovat všechny výpůjčky po uplynutí X měsíců po vrácení výpůjčky u čtenářů, kteří o to požádají. Ostatním ji uchovává. U čtenářů, kteří požádají o anonymizaci, dojde k jejímu jednorázovému provedení a každý další záznam, u kterého uplyne X měsíců od vrácení, dojde již k anonymizaci automaticky.
3. Knihovna uchovává historii výpůjček po celou dobu existence profilu uživatele s tím, že uživatelům aktivně nabízí možnost požádat o anonymizaci své historie výpůjček. Anonymizovat nelze historii mladší než X měsíců od ukončení výpůjčky.
   V této variantě knihovní systém umí automaticky anonymizovat všechny výpůjčky po uplynutí X měsíců po vrácení výpůjčky u čtenářů, kteří o to

požádají. Ostatním ji uchovává. U čtenářů, kteří požádají o anonymizaci, dojde k jejímu jednorázovému provedení.

Knihovny zvolí jeden ze způsobů, nikoli kombinaci. Knihovní systém musí umožnit volbu individuálně každému z uživatelů: například neuchovávat historii výpůjček. Dále by měl disponovat nástrojem pro provedení jednorázové anonymizace výpůjček, pokud to varianta vyžaduje.

14.3 Problematika mazání údajů v informačních systémech a databázích

Nařízení uvádí množství situací, kdy hovoří o povinnosti správce vymazat údaje po uplynutí doby jejich zpracování. V systémech a databázích lze provádět bez rizika přímé mazání jen ve velmi specifických případech. Knihovní systémy uchovávají množství vzájemně provázaných transakčních údajů, které slouží také jako podklad pro statistiky a výkaznictví. Z důvodu zachování konzistence databáze i možnosti získat statistické informace z historických dat není možné údaje přímo mazat. V praxi tedy bude aplikována anonymizace. Tzn., že dojde v záznamu k nahrazení osobních údajů jinými údaji, které znemožní zpětnou identifikaci konkrétní osoby. Zároveň zůstane zachována možnost plnit případné povinnosti v oblasti vykazování výkonů či vytváření statistik.

Tip: Soulad s GDPR u knihovních systémů

Aleph
ARL
Clavius a Tritius
Evergreen
Koha
KP-Sys

[1] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

[2] TKDIV: „Právnická osoba poskytující svým jménem knihovnické a informační služby v dané knihovně. Je-li knihovna právním subjektem, pak sama je provozovatelem knihovny, nemá-li knihovna právní subjektivitu (pokud např. je součástí organizace nebo je organizační složkou územně samosprávného celku nebo státu), pak provozovatelem je příslušný právní subjekt."

[3] Pokyn WP29 k posouzení vlivu na ochranu osobních údajů…

[4] § 31 Zákon č. 89/2012 Sb. Občanský zákoník

Nezletilí

§ 31

Má se za to, že každý nezletilý, který nenabyl plné svéprávnosti, je způsobilý k právním jednáním co do povahy přiměřeným rozumové a volní vyspělosti nezletilých jeho věku.

[5] Čl. 5 odst. 1, písm. b) Nařízení

[6] Bod 45 odůvodnění Nařízení

[7] Čl. 7 Nařízení

[8] § 4 ods. 5 knihovního zákona 257/2001 Sb.

ZÁKON ze dne 29. června 2001 o knihovnách a podmínkách provozování veřejných

knihovnických a informačních služeb (knihovní zákon)

(5) Provozovatel knihovny je oprávněn požadovat úhradu nákladů vynaložených na administrativní úkony spojené s evidencí uživatelů knihovny.

[9] Bod 47 odůvodnění Nařízení
[10] § 84 a násl. občanského zákoníku

Podoba a soukromí

§ 84

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.

[11] Bod 51 Nařízení a Čl. 9 Nařízení
[12] § 13c zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů

HLAVA III

RODNÁ ČÍSLA

§ 13

(1) V informačním systému je rodné číslo identifikátorem fyzické osoby, která splňuje podmínky pro jeho přidělení podle tohoto zákona (dále jen "fyzická osoba").

(2) Rodné číslo určuje ministerstvo.

(3) Rodné číslo je desetimístné číslo, které je dělitelné jedenácti beze zbytku. První dvojčíslí vyjadřuje poslední dvě číslice roku narození, druhé dvojčíslí vyjadřuje měsíc narození, u žen zvýšené o 50, třetí dvojčíslí vyjadřuje den narození. Čtyřmístná koncovka je rozlišujícím znakem fyzických osob narozených v tomtéž kalendářním dnu.

(4) Rodná čísla přidělená fyzickým osobám narozeným před 1. lednem 1954 mají stejnou strukturu jako rodná čísla uvedená v odstavci 3, jsou však devítimístná s třímístnou koncovkou a nesplňují podmínku dělitelnosti jedenácti.

(5) V případě, že jsou výdejovými místy rodných čísel (dále jen "výdejové místo") pro daný kalendářní den v příslušném kalendářním roce vyčerpána veškerá určená rodná čísla, určí ministerstvo pro tento den novou, dodatečnou sestavu rodných čísel, pro niž platí, že rodné číslo je desetimístné číslo, které je dělitelné jedenácti beze zbytku. První dvojčíslí vyjadřuje poslední dvě číslice roku narození, druhé dvojčíslí vyjadřuje měsíc narození, u mužů zvýšené o 20, u žen zvýšené o 70, třetí dvojčíslí vyjadřuje den narození. Čtyřmístná koncovka je rozlišujícím znakem fyzických osob narozených v tomtéž kalendářním dnu.

(6) Totéž rodné číslo nesmí být přiděleno více fyzickým osobám.

(7) Fyzická osoba je nositelem nejvýše jednoho rodného čísla.

(8) Rodným číslem podle tohoto zákona se rozumí také rodné číslo přidělené na území Slovenské republiky před 1. lednem 1993. Toto rodné číslo musí splňovat definici rodného čísla uvedenou v odstavcích 3 a 4 a současně musí splňovat podmínku uvedenou v odstavci 6.

(9) Rodné číslo je oprávněna užívat nebo rozhodovat o jeho využívání v mezích stanovených zákonem (dále jen "nakládat s rodným číslem") výlučně fyzická osoba, které bylo rodné číslo přiděleno (dále jen "nositel rodného čísla"), nebo její zákonný zástupce; jinak lze rodné číslo využívat jen v případech stanovených v § 13c tohoto zákona.

[13] § 18 knihovního zákona 257/2001 Sb.

§ 18

Ochrana knihovního fondu

Provozovatel knihovny je povinen zajistit

a) umístění knihovního fondu v podmínkách vhodných pro poskytování veřejných knihovnických a informačních služeb,

b) ochranu knihovního fondu před odcizením a poškozením, zejména ochránit jej před nepříznivými vlivy prostředí,

c) restaurování knihovních dokumentů, popř. jejich převedení na jiný druh nosiče, je-li to třeba k jejich trvalému uchování.

[14] Bod 50 odůvodnění a čl. 6 odst. 4 Nařízení

[15] Zákon č. 89/1995 Sb. o státní statistické službě. Dostupné z:https://www.zakonyprolidi.cz/cs/1995-89

[16] WP29: „Může tím být podkopána jeho svoboda volby, třeba u produktů nebo služeb jako knihy, hudba nebo pravidelné zasílání zpráv.“ Vodítka k automatizovanému individuálnímu rozhodování a profilování podle Nařízení 2016/679

[17] Čl. 9 Nařízení

[18] § 84 a násl. občanského zákoníku č. 89/2012 Sb.

Podoba a soukromí

§ 84

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.

§ 85

(1) Rozšiřovat podobu člověka je možné jen s jeho svolením.

(2) Svolí-li někdo k zobrazení své podoby za okolností, z nichž je zřejmé, že bude šířeno, platí, že svoluje i k jeho rozmnožování a rozšiřování obvyklým způsobem, jak je mohl vzhledem k okolnostem rozumně předpokládat.

§ 86

Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.

§ 87

(1) Kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se člověka nebo jeho projevů osobní povahy, může svolení odvolat, třebaže je udělil na určitou dobu.

(2) Bylo-li svolení udělené na určitou dobu odvoláno, aniž to odůvodňuje podstatná změna okolností nebo jiný rozumný důvod, nahradí odvolávající škodu z toho vzniklou osobě, které svolení udělil.

§ 88

(1) Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.

(2) Svolení není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.

§ 89

Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.

§ 90

Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka.

[19] Bod 47 odůvodnění Nařízení

[20] Konkrétněji bude přímý marketing pravděpodobně upraven novým nařízením zvaným ePrivacy, zatím v čl. 16 návrhu.

[21] Např. § 11 odst. 2 písm. b) knihovního zákona 257/2001 Sb.

§ 11

Krajská knihovna

(2) Krajská knihovna je součástí systému knihoven vykonávající koordinační, odborné, informační, vzdělávací, analytické, výzkumné, metodické a poradenské činnosti, v jejichž rámci též

[22] Čl. 89 odst. 2 Nařízení

[23] Č. 14 Nařízení

[24] § 4 knihovního zákona 257/2001 Sb.

§ 4

Veřejné knihovnické a informační služby

(1) Veřejné knihovnické a informační služby spočívají

a) ve zpřístupňování knihovních dokumentů z knihovního fondu knihovny nebo prostřednictvím meziknihovních služeb z knihovního fondu jiné knihovny,

b) v poskytování ústních bibliografických, referenčních a faktografických informací a rešerší,

c) ve zprostředkování informací z vnějších informačních zdrojů, zejména informací ze státní správy a samosprávy,

d) v umožnění přístupu k informacím na internetu, ke kterým má knihovna bezplatný přístup.

(2) Veřejné knihovnické a informační služby, uvedené v odstavci 1, je provozovatel knihovny povinen poskytovat bezplatně, s výjimkou

a) zpřístupňování knihovních dokumentů z knihovního fondu knihovny, které mají povahu rozmnoženin zvukového či zvukově obrazového záznamu,[2)1]

b) zpřístupňování knihovních dokumentů z knihovních fondů jiných knihoven zprostředkováním jejich rozmnoženin v rámci meziknihovních reprografických služeb,

c) zpřístupňování knihovních dokumentů z knihovních fondů knihoven v rámci mezinárodních meziknihovních služeb.

(3) Provozovatel knihovny může poskytovat další služby spočívající zejména

a) v umožnění přístupu k placeným informacím na internetu,

b) v kulturní, výchovné a vzdělávací činnosti,

c) ve vydávání tematických publikací,

d) v poskytování reprografických služeb,

e) v poskytování písemných bibliografických, referenčních a faktografických informací a rešerší.

(4) Provozovatel knihovny je oprávněn požadovat za poskytování knihovnických a informačních služeb, uvedených v odstavci 2 písm. a) až c), a dalších služeb úhradu skutečně vynaložených nákladů.

(5) Provozovatel knihovny je oprávněn požadovat úhradu nákladů vynaložených na administrativní úkony spojené s evidencí uživatelů knihovny.

(6) Provozovatel knihovny je povinen zajistit rovný přístup všem k veřejným knihovnickým a informačním službám a dalším službám poskytovaným knihovnou.

(7) Provozovatel knihovny vydá knihovní řád, v němž stanoví podrobnosti poskytování knihovnických a informačních služeb.

[25] Stanovisko ÚOOÚ https://www.uoou.cz/zamestnavatel-jako-spravce-osobnich-udaju/d-6171

[26] Např. § 35a zákona č. 582/1991 Sb. o organizaci a provádění sociálního zabezpečení, § 150 Zákoníku práce

§ 35a zákona č. 582/1991 Sb. o organizaci a provádění sociálního zabezpečení

ÚKOLY ZAMĚSTNAVATELŮ V SOCIÁLNÍM ZABEZPEČENÍ

HLAVA DRUHÁ

ÚKOLY ZAMĚSTNAVATELŮ PŘI PROVÁDĚNÍ DŮCHODOVÉHO POJIŠTĚNÍ

§ 35a

Povinnost zaměstnavatelů vést záznamy a podávat hlášení pro účely důchodového

pojištění

(1) Zaměstnavatelem se pro účely důchodového pojištění rozumí právnická nebo fyzická osoba, která zaměstnává jiné fyzické osoby nebo k níž jsou fyzické osoby ve vztahu, který zakládá účast na důchodovém pojištění. Za zaměstnavatele se považují též organizační složky státu, v nichž jsou zařazeny fyzické osoby v pracovním poměru nebo činěny na základě dohody o pracovní činnosti nebo dohody o provedení práce, služební úřady, v nichž jsou státní zaměstnanci podle zákona o státní službě[3a]) zařazeni k výkonu státní služby, věznice, v nichž vykonává trest odnětí svobody odsouzený zařazený do práce, ústavy pro výkon zabezpečovací detence, v nichž vykonávají zabezpečovací detenci osoby zařazené do práce, a příslušné útvary, složky nebo jiné organizační části bezpečnostních sborů nebo ozbrojených sil České republiky, které vyplácejí příslušníkům bezpečnostních sborů služební příjem nebo vojákům z povolání služební plat nebo služné u ostatních vojáků vykonávajících vojenskou činnou službu (dále jen "útvar"). Za zaměstnavatele se považuje dále organizační složka právnické osoby, která má sídlo ve státě, s nímž Česká republika neuzavřela mezinárodní smlouvu o sociálním zabezpečení, pokud je tato složka zapsána v obchodním rejstříku a tato právnická osoba zaměstnává vedoucí zaměstnance této organizační složky, pokud tito zaměstnanci mají místo výkonu práce trvale v České republice.

(2) Zaměstnavatelé jsou povinni vést potřebné záznamy o skutečnostech rozhodných pro nárok na dávky důchodového pojištění, jejich výši a výplatu a předkládat je příslušným orgánům sociálního zabezpečení.

(3) Změny ve skutečnostech rozhodných pro nárok na dávku a jeho trvání a pro výši a výplatu dávky jsou zaměstnavatelé povinni písemně hlásit, není-li určeno jinak, do osmi dnů. Na výzvu orgánů sociálního zabezpečení jsou zaměstnavatelé povinni podat hlášení a předložit záznamy ve lhůtě určené tímto orgánem, a není-li lhůta určena, do osmi dnů od doručení výzvy.

(4) Zaměstnavatelé jsou povinni uschovávat

a) stejnopisy evidenčních listů (§ 38 odst. 5 věta první) vyhotovených v kalendářním roce, kterého se týkají, nebo v bezprostředně následujícím kalendářním roce po dobu 3 kalendářních roků po roce, kterého se týkají, a stejnopisy ostatních evidenčních listů po dobu 3 kalendářních roků po roce, ve kterém byly vyhotoveny,

b) záznamy o skutečnostech vedených v evidenci podle § 37 odst. 1 písm. h) po dobu 6 kalendářních roků následujících po měsíci, kterého se záznam týká, vždy však po dobu 3 kalendářních roků následujících po měsíci, v němž bylo dlužné pojistné za tento měsíc zaplaceno,

c) záznamy o skutečnostech vedených v evidenci podle § 37 odst. 1, pokud jde o poživatele starobního nebo invalidního důchodu, po dobu 10 kalendářních roků po roce, kterého se týkají,

d) mzdové listy[71a]) nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění, včetně údajů uvedených v § 37 odst. 2 a 3, po dobu 30 kalendářních roků následujících po roce, kterého se týkají, a jde-li o mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění vedené pro poživatele starobního důchodu, po dobu 10 kalendářních roků následujících po roce, kterého se týkají,

pokud zvláštní právní předpis nestanoví pro záznamy, které mají charakter účetních záznamů, delší uschovací dobu; za záznamy o těchto skutečnostech se vždy považují doklady o druhu, vzniku a skončení pracovního vztahu, záznamy o pracovních úrazech a o

nemocech z povolání a záznamy o evidenci pracovní doby[71b]) včetně doby pracovního volna bez náhrady příjmu.

(5) Zaniká-li zaměstnavatel bez právního nástupce před uplynutím dob uvedených v odstavci 4, je povinen zajistit úschovu záznamů a dalších dokladů uvedených v odstavci 4 (dále jen „doklady zaměstnavatele“) do uplynutí těchto dob a bez zbytečného odkladu písemně oznámit okresní správě sociálního zabezpečení, kde jsou doklady zaměstnavatele uloženy.

(6) Jsou-li doklady zaměstnavatele po zaměstnavateli zaniklém bez právního nástupce uloženy ve spisovně nebo správním archivu podle zákona upravujícího archivnictví a spisovou službu, v provozovně, ve které se vykonává činnost na základě státního povolení k provozování živnosti vedení spisovny[78]), nebo v archivu, jsou zřizovatel spisovny, zřizovatel správního archivu, podnikatel, kterému bylo uděleno státní povolení k provozování živnosti vedení spisovny, archiv nebo jeho zřizovatel (dále jen „držitel dokladů“) povinni na výzvu orgánu sociálního zabezpečení pořídit výpis, opis nebo kopii dokladů zaměstnavatele pro účely provádění důchodového pojištění a nejpozději do 30 dnů ode dne doručení této výzvy je orgánu sociálního zabezpečení zaslat. Držitel dokladů na žádost orgánu sociálního zabezpečení potvrdí shodu jím pořízeného opisu nebo kopie dokladu zaměstnavatele s dokladem zaměstnavatele uloženým u držitele dokladů. Držitel dokladů má právo na úhradu nákladů spojených s pořízením výpisu, opisu nebo kopie dokladů zaměstnavatele, s jejich zasláním orgánu sociálního zabezpečení a s potvrzením shody jím pořízeného opisu nebo kopie dokladu zaměstnavatele s dokladem zaměstnavatele uloženým u držitele dokladů; výši nákladů je držitel dokladů na výzvu orgánu sociálního zabezpečení povinen prokázat. Právo na úhradu těchto nákladů nemá veřejný archiv v případech, ve kterých nemá právo na úhradu nákladů na pořízení výpisu, opisu nebo kopie archiválie podle zákona upravujícího archivnictví a spisovou službu[79]).

(7) Zaniká-li bez právního nástupce držitel dokladů, u kterého jsou uloženy doklady zaměstnavatele po zaměstnavateli zaniklém bez právního nástupce, před uplynutím dob uvedených v odstavci 4, je tento držitel dokladů povinen bez zbytečného odkladu písemně oznámit příslušné okresní správě sociálního zabezpečení skutečnosti týkající se jeho zániku a dále na vlastní náklady zajistit uložení dokladů zaměstnavatele u jiného držitele dokladů do uplynutí těchto dob a písemně oznámit příslušné okresní správě sociálního zabezpečení, kde jsou doklady zaměstnavatele uloženy. Příslušné okresní správy sociálního zabezpečení poskytují držitelům dokladů na jejich žádost potřebnou součinnost zejména při určení dokladů zaměstnavatele, jejichž další uložení je třeba zajistit.

(8) Zůstanou-li v majetkové podstatě[80]) zanikajícího držitele dokladů finanční prostředky, použijí se na úhradu nákladů na uložení dokladů zaměstnavatele u jiného držitele dokladů vybraného ve spolupráci s příslušným státním oblastním archivem. V případě neexistence takových finančních prostředků se provede uložení podle odstavce 7 u jiného držitele dokladů na náklady ministerstva.

(9) Prováděcí právní předpis stanoví, co se rozumí odůvodněnými náklady a stanoví maximální výši úhrady nákladů uvedených v odstavci 6 a nákladů na uložení podle odstavce 8, které je držitel dokladů oprávněn požadovat.

§ 150 Zákoníku práce ***č. 262/2006 Sb***

§ 150

Zaměstnavatel eviduje údaje, jimiž jsou jméno, popřípadě jména a příjmení, adresa, jde-li o fyzickou osobu, název a sídlo, jde-li o právnickou osobu, a písemnosti týkající se prováděných srážek ze mzdy, a to po stejnou dobu jako ostatní údaje a doklady týkající se

mzdy nebo platu[56])

[27] § 68 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

§ 68

Ukládání dokumentů

(1) Všechny vyřízené spisy a jiné dokumenty určeného původce jsou po dobu trvání skartační lhůty uloženy ve spisovně. Dokumenty mohou být uloženy též ve správním archivu, pokud jej určený původce zřídil. Dokumenty se ukládají podle spisového a skartačního plánu, a to zpravidla ihned po jejich vyřízení, pokud povaha věci nevyžaduje, aby zpracovatel měl vyřízený dokument déle; tato skutečnost se poznamenává v evidenci podle § 64 odst. 3.

(2) Pro nahlížení do dokumentů uložených ve spisovně nebo ve správním archivu správního orgánu nebo soudu platí obecná ustanovení o nahlížení do spisů v řízení před správním orgánem nebo soudem; to neplatí, jestliže dokumenty před uložením ve spisovně nebo ve správním archivu byly veřejně přístupné. Nahlížení do dokumentů obsahujících utajované informace, poskytování jejich opisů, výpisů a kopií se řídí zvláštním právním předpisem.2)

(3) V případě zániku určeného původce převezme spisovnu nebo správní archiv jeho právní nástupce, zřizovatel nebo ten, na něhož přechází působnost zaniklého určeného původce; je-li právních nástupců více a nedojde-li mezi nimi k dohodě, rozhodne o převzetí spisovny nebo správního archivu příslušný správní úřad na úseku archivnictví a výkonu spisové služby dohlížející na provádění skartačního řízení. Určený původce informuje před svým zánikem příslušný archiv o opatřeních, která v souvislosti se zánikem učinil ve vztahu ke spisovně nebo správnímu archivu.

(4) Budova, v níž je umístěna spisovna nebo správní archiv, musí splňovat tyto podmínky:

a) prostory pro ukládání dokumentů nesmí být ohroženy povodněmi,

b) musí pro ni být zpracována požární dokumentace a musí být vybavena ručními hasicími přístroji; v prostorách pro ukládání dokumentů musí být umístěny pouze práškové hasicí přístroje,

c) prostory pro ukládání dokumentů musí být zabezpečeny proti škodlivému působení přírodních vlivů a jevů vyvolaných činností člověka, a to zejména proti průniku vody, páry, dešťové a splaškové kanalizace, nebezpečných chemických a biologických látek nebo působení fyzikálních jevů a proti nadměrné prašnosti, které by mohly vést k poškození nebo zničení dokumentů,

d) prostory pro ukládání dokumentů musí být vybaveny regály pro ukládání dokumentů,

e) prostory pro ukládání dokumentů musí být zajištěny proti vstupu nepovolané osoby.

[28] § 63 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů

§ 63

(1) Spisovou službu vykonávají

a) veřejnoprávní původci uvedení v § 3 odst. 1 písm. a) až e), i) a k) až m),

b) kraje,

c) hlavní město Praha,

d) obce s pověřeným obecním úřadem a obce se stavebním nebo matričním úřadem,

e) městská část nebo městský obvod územně členěného statutárního města a městská část hlavního města Prahy, na něž byla statutem přenesena alespoň část působnosti obce s pověřeným obecním úřadem nebo působnosti obce se stavebním nebo matričním úřadem,

(dále jen „určení původci“).

(2) Obce neuvedené v odstavci 1, školy a veřejnoprávní původci uvedení v § 3 odst. 1 písm. g) a h) vykonávají spisovou službu v rozsahu ustanovení § 64, § 65, § 66, § 67, § 68 odst. 1 až 3, § 68a a 69a.

(3) Veřejnoprávní původci uvedení v § 3 odst. 1 písm. a) až d), i), k) a m), kraje a hlavní město Praha vykonávají spisovou službu v elektronické podobě v elektronických systémech spisové služby; vyžaduje-li to zvláštní povaha jejich působnosti, mohou vykonávat spisovou službu v listinné podobě nebo v elektronických systémech spisové služby odpovídajících požadavkům podle odstavce 4. Veřejnoprávní původci uvedení v § 3 odst. 1 písm. e), g), h), j) a l) a obce vykonávají spisovou službu v elektronické podobě v elektronických systémech spisové služby nebo v listinné podobě.

(4) Pokud veřejnoprávní původci uvedení v odstavci 3 větě první, jejichž zvláštní povaha působnosti umožňuje výkon spisové služby v listinné podobě nebo v elektronické podobě v elektronických systémech spisové služby, vykonávají spisovou službu v elektronické podobě v elektronickém systému spisové služby, který je součástí informačního systému pro nakládání s utajovanými informacemi34), musí tento elektronický systém spisové služby splňovat požadavky stanovené národním standardem pro elektronické systémy spisové služby (dále jen „národní standard“), s výjimkou těch požadavků, jejichž užití vylučuje splnění podmínek certifikace informačního systému pro nakládání s utajovanými informacemi35), nebo jejichž užití vylučuje zvláštní povaha působnosti těchto původců; elektronické systémy spisové služby i v těchto případech musí umožňovat plnění povinností původce podle § 65 odst. 5 a výběr archiválií.

[29] MV ČR, Ochrana osobních údajů při výkonu spisové služby, zejména v informačních systémech spravujících dokumenty u veřejnoprávních původců: http://www.mvcr.cz/clanek/metodicka-podpora-a-konzultace.aspx

[30] WP29: Pokyny k transparentnosti podle Nařízení 2016/679 (AJ)

[31] Čl. 12, 13 , 14 Nařízení

[32] Čl. 15 Nařízení

[33] Čl. 15, odst. 1 Nařízení

[34] Bod 63 odůvodnění Nařízení

[35] Pokyn WP29 k přenositelnosti

[36] Čl. 17 Nařízení

[37] Viz např. rozsudek SDEU ve věci C 131/12 Google Spain SL, Google Inc. proti Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González http://eur-lex.europa.eu/legal-

content/CS/TXT/HTML/?uri=CELEX:62012CJ0131&from=CS, http://www.privacy-regulation.eu/cs/38.htm

[38] Čl. 19 Nařízení

[39] Čl. 12 Nařízení

[40] Čl. 37-39 Nařízení

[41] WP29: Pokyny týkající se pověřenců pro ochranu osobních údajů

[42] Čl. 28 Nařízení

[43] Čl. 33 Nařízení

[44] Čl. 34 Nařízení

[45] WP29: Vodítka k ohlašování případů porušení zabezpečení osobních údajů podle Nařízení 2016/679

[46] STROM, David. Zabezpečte si e-maily pomocí šifrování. ComputerWorld [online]. 11.07. 2016 [cit. 2018-01-18]. Dostupné z: http://computerworld.cz/securityworld/zabezpecte-si-e-maily-pomoci-sifrovani-53179

[47] Viz https://security.ics.muni.cz/17-Phishing-is-v-ohrozeni

Alternativně https://web.archive.org/web/20170701043037/https://security.ics.muni.cz/17-Phishing-is-v-ohrozeni

Podrobněji viz https://security.ics.muni.cz/20-Uzivatel-na-hacku-kdyz-se-podvodnikum-zadari

Alternativně https://web.archive.org/web/20170701061442/https://security.ics.muni.cz//20-Uzivatel-na-hacku-kdyz-se-podvodnikum-zadari

[48] Email Encryption. *OpenPGP* [online]. OpenPGP, 27. 09. 2017 [cit. 2018-01-03]. Dostupné z: https://www.openpgp.org/software/

[49] SPF Records. *MXtoolbox* [online]. MXTOOLBOX, 2017 [cit. 2018-01-15]. Dostupné z: https://mxtoolbox.com/spf.aspx

[50] V úniku z Mallu je přes tři čtvrtě milionu jmen, hesel a telefonních čísel v čitelné podobě. *Lupa* [online]. Praha: Internet Info, 29. 8. 2017 [cit. 2017-12-29]. Dostupné z: https://www.lupa.cz/clanky/v-uniku-z-mallu-je-pres-tri-ctvrte-milionu-jmen-hesel-a-telefonnich-cisel-v-citelne-podobe/

[51] *FreeOTP: Two-Factor Authentication* [online]. Red Hat, 2017 [cit. 2017-12-30]. Dostupné z: https://freeotp.github.io/

[52] Analýza napadení ransomware: stačí otevřený port RDP a slabé heslo. In: Root.cz: Informace nejen ze světa Linuxu [online]. Praha: Internet Info, 2017, 28. 6. 2017 [cit. 2018-01-19]. Dostupné z: https://www.root.cz/clanky/analyza-napadeni-ransomware-staci-otevreny-port-rdp-a-slabe-heslo/

[53] Viz například https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/securing-remote-desktop-rdp-system

[54] Features. *BleachBit* [online]. BleachBit, 2017 [cit. 2018-01-12]. Dostupné z: https://www.bleachbit.org/features

[55] K obsahu smluv viz např. VESELÝ, Zdeněk. Chybějící zpracovatelské smlouvy. Dlouhodobý prohřešek firem má napravit GDPR. *Podnikatel.cz* [online]. 3. 1. 2018 [cit.

2018-01-18]. Dostupné z: https://www.podnikatel.cz/clanky/chybejici-zpracovatelske-smlouvy-dlouhodoby-prohresek-firem-ma-napravit-gdpr/

[56] Viz zde: https://www.blog.google/topics/google-cloud/google-cloud-our-commitment-general-data-protection-regulation-gdpr/; popis ochrany dat zde: https://www.cleverity.cz/g-suite-zabezpeceni-gdpr/

[57] Viz zde: https://www.techsoup.cz/node/71633

[58] Viz například zde: https://www.autocont.cz/aktuality/openspace/gdpr-microsoftnebo https://enterprise.microsoft.com/cs-cz/articles/roles/it-leader/gdpr-jste-jiz-pripraveni-na-posledni-chvili-nevyresite/

[59] About Let's Encrypt. In: *Let's Encrypt* [online]. San Francisco: Internet Security Research Group, 2015 [cit. 2017-12-30]. Dostupné z: https://letsencrypt.org/about/

[60] CALETKA, Ondřej. Let's Encrypt zablokoval nebezpečnou validaci pomocí self-signed certifikátu. In: *Root.cz* [online]. Praha: Internet Info, 2018, 10. 1. 2018 [cit. 2018-01-19]. Dostupné z: https://www.root.cz/clanky/let-s-encrypt-zablokoval-nebezpecnou-validaci-pomoci-self-signed-certifikatu

[61] *SSL Server Test* [online]. Qualys, 2017 [cit. 2017-12-30]. Dostupné z: https://www.ssllabs.com/ssltest/index.html

[62] Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat. *Root.cz* [online]. Praha: Internet Info, 2017, 17. 10. 2017 [cit. 2017-12-29]. Dostupné z: https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/

[63] Více než jen router: Open-source centrum Vašeho domova. *Turris Omnia* [online]. Praha: NIC. CZ, 2017 [cit. 2017-12-29]. Dostupné z: https://omnia.turris.cz/cs/

[64] FISHER, Tim. 41 Free Data Destruction Software Programs: Completely Free Disk Wipe and Hard Drive Eraser Software Utilities. In: *Lifewire* [online]. Lifeware, 29. 12. 2017 [cit. 2018-01-01]. Dostupné z: https://www.lifewire.com/free-data-destruction-software-programs-2626174

Nahoru