Univerzita Hradec Králové
Filozofická fakulta

Bakalářská práce

2019 Ondřej Tomiška

Univerzita Hradec Králové

Filozofická fakulta

Katedra pomocných věd historických a archivnictví

eDokumenty a zákon o kybernetické bezpečnosti

Bakalářská práce

Autor: Ondřej Tomiška

Studijní program: Technická podpora humanitních věd

Forma studia: prezenční

Studijní obor: Počítačová podpora v archivnictví (BPARCHIV)

Vedoucí práce: Ing. Monika Borkovcová, Ph.D.

Hradec Králové, 2019

Prohlášení studenta

Čestně prohlašuji, že tato práce je mým vlastním autorským dílem. Práci jsem vypracoval samostatně a uvedl jsem všechny prameny, literaturu a zdroje, které jsem při vypracování práce použil nebo z nich čerpal.

V Hradci Králové dne 29.04.2019 …….

Tomiška Ondřej

Univerzita Hradec Králové
Filozofická fakulta

Zadání bakalářské práce

Autor:	**Ondřej Tomiška**
Studium:	F16BP0095
Studijní program:	B3928 Technická podpora humanitních věd
Studijní obor:	Počítačová podpora v archivnictví
Název bakalářské práce:	**eDokumenty a zákon o kybernetické bezpečnosti**
Název bakalářské práce AJ:	eDocuments and cyber-security regulation

Cíl, metody, literatura, předpoklady:

Cílem práce je analyzovat současné eDokumenty ve vztahu k Velké novele zákona o kybernetické bezpečnosti (ZKB). S příchodem nových legislativních opatření a nařízení (ZKB, EIDAS, GDPR a dalších) souvisí pokročilý způsob ukládání dat a dokumentů s důrazem na bezpečnostní opatření. Práce se bude zabývat eDokumenty v archivní a spisové službě a veřejné správě, kdy součástí práce je popis eDokumentu, elektronického podpisu, razítka, pečetě a souvisejících pojmů. V praktické části autor provede srovnání současného stavu před účinností jednotlivých legislativních opatření a nařízení a po jejich implementaci do různých informačních systémů a aplikací, které pracují s eDokumenty a daty obecně. Praktická část se bude soustředit na přístup k datům, pravidla bezpečnostní politiky organizace, finanční náročnost, lidské zdroje, zpřístupňování dat veřejnosti a s tím související ochrana dat.

HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. Kybernetická bezpečnost: teorie a praxe. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6. MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6. Národní úřad pro kybernetickou a informační bezpečnost [online]. Brno: Ministerstvo vnitra, 2017 [cit. 2017-11-14]. Dostupné z: https://www.nukib.cz/ Svobodný přístup k informacím: Informatika : služby vytvářející důvěru, elektronická komunikace ; eGovernment : elektronické úkony a konverze dokumentů, informační systémy veřejné správy, kybernetická bezpečnost, základní registry, elektronická identifikace (od ..) : redakční uzávěrka .. Ostrava: Sagit, 2014. ÚZ. ŠPAČEK, David. EGovernment: cíle, trendy a přístupy k jeho hodnocení. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN 978-80-7400-261-8. ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: Anag, 2017. ISBN 978-80-7554-097-3. Zákony: Zákon č. 300/2008 Sb., Zákon o elektronických úkonech a autorizované konverzi dokumentů novelizovaný předpisem 183/2017 Sb. Zákon č. 499/2004 Sb., Zákon o archivnictví a spisové službě a o změně některých zákonů novelizovaný předpisem 205/2017 Sb. Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) novelizovaný předpisem 205/2017 Sb. Zákon č. 104/2017 Sb., Zákon o informačních systémech veřejné správy Zákon č. 298/2016 Sb. Zákon, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a o změně některých zákonů novelizovaný předpisem 183/2017 Sb. směrnice 95/46/ES

Garantující pracoviště:	Katedra pomocných věd historických a archivnictví, Filozofická fakulta
Vedoucí práce:	Ing. Monika Borkovcová, Ph.D.
Oponent:	PhDr. Tomáš Černušák, Ph.D.

Datum zadání závěrečné práce: 14.11.2017

Poděkování

Chtěl bych poděkovat Ing. Monice Borkovcové, Ph.D. za její odborné rady, poskytnuté materiály, a čas stráveným čtením této bakalářské práce.

Anotace

TOMIŠKA, ONDŘEJ. eDokumenty a zákon o kybernetické bezpečnosti. Hradec Králové. Filozofická fakulta, Univerzita Hradec Králové, 2019, 107 str., Bakalářská práce.

Cílem práce je analyzovat současné eDokumenty ve vztahu k Velké novele zákona o kybernetické bezpečnosti (ZKB). S příchodem nových legislativních opatření a nařízení (ZKB, eIDAS, GDPR a dalších) souvisí pokročilý způsob ukládání dat a dokumentů s důrazem na bezpečnostní opatření.

Práce se bude zabývat eDokumenty v archivní a spisové službě a veřejné správě, kdy součástí práce je popis eDokumentu, elektronického podpisu, razítka, pečetě a souvisejících pojmů. V praktické části autor provede srovnání současného stavu před účinností jednotlivých legislativních opatření a nařízení a po jejich implementaci do různých informačních systémů a aplikací, které pracují s eDokumenty a daty obecně.

Klíčová slova:

eDokument, Zákon o kybernetické bezpečnosti, GDPR, eGovernement, eIDAS

Annotation

TOMIŠKA, ONDŘEJ. eDocuments and cyber-security regulation. Hradec Králové. Philosophical Faculty. University of Hradec Králové, 2019, 107 pp., Bahelor Degree Thesis.

Goal of this paper is to analyze current eDocuments in relation to Great amendment of Cybersecurity law (ZKB). With coming of the new legislative measures and regulations (ZKB, eIDAS, GDPR and others) comes advanced processes for data and document storage with emphasis on security measures.

This Bachelor degree thesis will be covering eDocuments in archives, filling services and public administrations. First part of this thesis will be dedicated to describing eDocuments, electronic signatures, stamps, seals and other related terms. Second part will be dedicated towards regulation and legislative measures comparisons and analysis from before and after their implementation into different information systems, apps which handle eDocuments and data in general.

Keywords:

eDocument, Cyber-security regulation, GDPR, eGovernment, eIDAS

Obsah

Seznam zkratek

AES Advanced Encryption Standard

COBIT Control Objective for Information and related Technology

CPU Central Processing Unit

CzechPOINT Podací Ověřovací Informační Národní Terminál

BFU Běžný fyzický uživatel

DES Data Encryption Standard

DMS Document Management System

DPH Daň z přidané hodnoty

DPIA Data Protection Impact Assessment

DPO Data Protection Officer

eID elektronická identifikace

eIDAS elektronická identifikace a důvěryhodnost služeb

eOP elektronický občanský průkaz

EP Elektronický podpis

ERMS Electronic Record Management System

ESSL Elektronický systém spisové služby

ETSI European Telecommunications Standard Institute

EU Evropská Unie

FO Fyzická osoba

GDPR General Data Protection Regulation

HTML Hypertext Markup Language

ICT Information and Communication Technology

ID Identification

IP Internet Protocol

IS Information System

ISDS Informační systém Datových schránek

ISMS Information Security Management System

ISO International Organization for Standardization

ISVS Informační systém veřejné správy

IT Information Technology

ITIL	Information Technology Infrastructure Library
LTV	Long Term Validity
METS	Metadata Encoding and Transmission Standard
MODS	Metadata Object Description Scheme
MS	Microsoft
NBÚ	Národní bezpečnostní úřad
NIS	Network and Information Security
NSESSS	Národní standard elektronického systému spisové služby
NÚKIB	Národní úřad pro kybernetickou bezpečnost
OS	Operating System
OSVČ	Osoba samostatně výdělečně činná
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal Identification Number
PO	Právnická osoba
RAM	Random Access Memory
RC2	Rivest Cipher
RSA	Rivest, Shafir, Adleman Cipher
SQL	Structured Query Language
TDPS	Trusted Document Preserved System
USB	Universal Serial Bus
ÚOOÚ	Úřad pro ochranu osobních údajů
XML	Extensible Markup Language
ZEP	Zaručený elektronický podpis
ZKB	Zákon o kybernetické bezpečnosti

Slovník pojmů

Aktiva – (assets) jsou hodnoty, zdroje či majetek který je potřeba chránit.

Autentizace – Proces ověření identity.

Autorizace – Proces získávání povolení k operaci.

Big Data – Enormní množství datových souborů, které díky své rozsáhlosti nelze spravovat a zpracovávat běžnými metodami. Ukládají se do datových skladů.

Brute Force – Metoda pro dešifrování obsahu používající „hrubou sílu“. Daný počítač jednoduše zkouší náhodné varianty přístupových údajů, podob hesel aj. Závislá na výpočetním výkonu zařízení.

Cloud computing – Způsob propůjčování výpočetních služeb skrze internet (Cloud) nepřímo jeho uživateli. (Například úložiště dat, výpočetní výkon, Analytické nástroje, Softwarové aplikace, Databázové servery aj.)

Data – Informace v digitální podobě určené k binárnímu zpracování. Jedná se o souhrn informací se společným znakem a vypovídající hodnotou.

Data mining – Proces získávání netriviálních skrytých a potenciálně užitečných informací z dat.

Databáze – Strukturovaný systém uložených informací a dat.

Databázový server – Prvek počítačové sítě a úložiště databází umožňující manipulaci s nimi a jejich poskytování.

Digital Born Documents – eDokumenty vytvořené pomocí textového procesoru.

Digital Surrogates – Převedené analogové dokumenty do digitální podoby.

Document Management System – Aplikační software, sloužící ke správě záznamů. (angl. Document = záznam v českém prostředí)

eGovernment – Elektronický systém veřejné správy se všemi jejími prvky.

Framework – Je sada pravidel, standardů a metod, které se obecně používají jako vzor pro řešení určitého problému. Lze definovat také jako podpůrnou softwarovou strukturu s již předem definovanými pravidly, standardy a metodami.

Hardware – Technické vybavení počítače.

Informační bezpečnostní incident – Narušení bezpečnosti informací, služeb, integrity informačního systému v důsledku kybernetické bezpečnostní události.

Informatika – Věda zabývající se studiem procesů zpracovávajících informace, jejich teoretickými základy, analýzou, návrhem, efektivitou, implementací a aplikacemi, ať už jde o informace uložené ve formě bitů v paměti počítače, nacházející se v dokumentech na internetu nebo zapsané v genech živých organismů.

Informační systém – Systém vzájemně propojených prostředků a procesů, které slouží k ukládání, zpracovávání a poskytování informací.

Integrita – Neměnnost, stálost dat.

Korupce dat – chyby v datech, které se přihodili selháváním či poruchou paměťového média (Například Operační paměť, Pevný disk, SSD)

Kybernetická bezpečnost – Odvětví informatiky zabývající se snižováním bezpečnostního rizika a reagováním na ně pomocí technických, organizačních a jiných prostředků.

Kyberprostor – Virtuální prostředí počítačových sítí (Internet, intranety aj.) dohromady tvořících nehmotný svět.

Metadata – Popisné informace o datech.

Moorův zákon – Pravidlo o růstu výpočetního výkonu vyřčené zakladatelem firmy Intel Moorem. Říká, že průběžně za každé 2 roky se počet tranzistorů na procesoru zdvojnásobí.

Operační paměť – Paměť s náhodným přístupem. Základní komponenta osobního počítače umožňující zápis a čtení informací s relativně vysokou rychlostí. Volatilní.

Procesor – Základní elektronická součástka osobního počítače, která umí vykonávat strojové instrukce pomocí své instrukční sady. Má na starosti výpočetní operace.

Profilování – Metoda získávání informací a vzorců chování dané osoby pomocí jejich osobních údajů a dalších doplňujících informací.

Původce – dle archivního zákona každý, z jehož činnosti dokument vznikl; za dokument vzniklý z činnosti původce se považuje rovněž dokument, který byl původci doručen nebo jinak předán.

Software – Programové vybavení počítače. Dělí se na systémový a aplikační.

Šifrování / kryptografie – Způsoby a metody utajování informací (jak digitální, tak analogové). Dělí se na asymetrické (2 klíče) a symetrické (1 klíč)

Šifrovací algoritmus – Matematické operace sloužící k zašifrování (= utajení) daných dat.

Time to live – Volně přeloženo jako délka života. Označuje životnost. Doba existence a platnosti daných dat. Po vypršení této doby by mělo dojít k jejich vymazání.

USB Token – Zabezpečené paměťové zařízení sloužící k autentizaci vlastníka.

Virtualizace – Označení postupů, technik a prostředků, které umožňují počítači simulovat (vytvářet iluzi) určitého výpočetního prostředí.

XML – Extensible Markup Language. Značkovací jazyk standardizovaný W3C. Umožňuje snadné vytváření konkrétních značkovacích jazyků pro různé účely a různé typy dat. Jazykovou sadou je Unicode. Většina metadatových schémat je psaná v XML.

Úvod

S neustále se rozvíjejícími a finančně dostupnějšími informačními technologiemi se stává eGovernment, jehož základním prvkem je eDokument, stále výkonnějším, užitečnějším a poptávaným prostředníkem ke komunikaci různých subjektů s veřejnou a státní správou. Na druhou stranu tento rozmach přináší nové, chytřejší a výkonnější metody, nesoucí s sebou rostoucí bezpečnostní hrozby založené na různých rizicích jednotlivých metod. Na tuto skutečnost reagují výkonné orgány Evropské Unie a její členské země zavedením nových legislativních opatření. Dochází k zásadním změnám, nejen právního rámce, ale ke komplexní změně v problematice bezpečnosti kyberprostoru, a tedy i eDokumentů, které se v něm pohybují. Nejdůležitějšími opatřeními v posledních dvou letech jsou elektronická identifikace a důvěryhodnost služeb (eIDAS), implementace směrnice NIS do českého práva pomocí Velké a Malé novely Zákona o kybernetické bezpečnosti a nařízení General Data Protection Regulation (GDPR). Platí, že veškerá legislativa zmíněná v textu je platná v době psaní této práce.

Cílem této práce je poskytnout ucelený všeobecný přehled v oblasti těchto nových legislativních opatřeních a dalších prvků eGovernmentu dotýkajících se eDokumentů. Dále provést srovnání procesů před a po aplikaci směrnice NIS do Zákona o kybernetické bezpečnosti s důrazem na přístup k datům, pravidlům bezpečnostní politiky organizace, finanční náročnosti, lidským zdrojům, zpřístupňování dat veřejnosti a v neposlední řadě k ochraně dat.

Práce je rozdělena na teoretickou a praktickou část, kdy teoretická část je zaměřena na jednotlivá nová legislativní opatření (ZKB, eIDAS, GDPR) a prvky českého eGovernmentu (eDokument, Datová schránka, elektronická značka aj.). Praktická část práce je tvořena komparací Zákona o kybernetické bezpečnosti s jeho novelami zavádějícími směrnici NIS.

Základními prameny pro zpracování celé práce byly především samotné zákony, směrnice a nařízení. Nelze také opomenout informační servis poskytovaný Ministerstvem vnitra skrze své obsáhlé webové stránky. Neméně důležitými zdroji byly také webové stránky Národního úřadu pro kybernetickou bezpečnost a Úřadu pro ochranu osobních údajů, které mají velmi dobře strukturovaný, a především

srozumitelný informační servis. Základní literaturu potom tvořili knihy E-government v České republice Právní a technologické aspekty od autorů P. Matese, V. Smejkala. V problematice ochrany digitálních dokumentů bylo pro práci velmi zásadní dílo pana L. Cubra Dlouhodobá ochrana digitálních dokumentů.

Čtenáři by práce měla poskytnout přehled o klíčových prvcích eGovernmentu České republiky a legislativou s tímto přímo související včetně výsledné komparace ZKB.

1. eDokument

Dokumentem se dle zákona o archivnictví a spisové službě č. 499/2004 Sb. rozumí „*…každá písemná, obrazová, zvuková nebo jinak zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena,"*[1] eDokument má tudíž naprosto totožnou právní hodnotu jako analogový dokument, s tím, že musí dodržet veškeré náležitosti, které jej jednoznačně identifikují a zajišťují jeho integritu[2]. V České republice řádně podepsaný a orazítkovaný elektronický dokument nabývá stejné právní účinnosti jako, klasický, analogový dokument.

eDokument (dále také digitální dokument) může vzniknout dvěma způsoby – buď je vytvořen digitalizací analogového dokumentu a následným popsáním (digitalizovaný dokument) anebo je vytvořen elektronicky, pomocí osobního počítače či v případě audiovizuálních dokumentů multimediálními technickými prostředky (elektronický dokument).

1.1. eDokumenty vytvořené digitalizací

Digitalizovaný dokument (*digital surrogates*) je typ reformátovaných dokumentů, které vznikly digitalizací analogových a existuje k nim analogový protějšek.[3] Takovýto digitalizovaný[4] dokument má poté stejná práva jako dokument vytvořený čistě elektronickou cestou, avšak aby byl uznáván zákonem, tak musí být řádně popsán a musí být jasně identifikovatelný (i časově).

---

[1]Zákon č. 499/2004 Sb.: Zákon o archivnictví a spisové službě a o změně některých zákonů. *Zakonyprolidi.cz* [online]. [cit. 2018-07-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-499

[2]Integritou se rozumí neměnnost daného dokumentu = věříme, že během své existence je dokument stále stejný. Nejen jeho obsah ale i metadata a další.

[3]CUBR, Ladislav. *Dlouhodobá ochrana digitálních dokumentů*. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

[4]Výhodou těchto dokumentů je, že analogový protějšek může fungovat jako jakási záloha, kterou lze využít v případě ztráty digitalizovaného dokumentu a vytvořit tak nový, digitální dokument.

1.2. eDokumenty vytvořené technickými prostředky

Výhradně digitální dokumenty *(digital born documents)* jsou takové dokumenty, které byly vytvořené s předpokladem, že už nebudou mít analogové protějšky.[5] Jsou vytvářeny elektronicky, pomocí technických prostředků výpočetní techniky či jiných, multimediálních přístrojů (kamera, fotoaparát, mikrofon).

1.3. Problematika ochrany eDokumentů

Oproti ochraně klasických, analogových dokumentů, která funguje již, v porovnání s ochranou digitálních dokumentů, velmi dlouho a v zásadě efektivně, je ochrana digitálních dokumentů ve státní správě otázkou posledního čtvrt století.

Ochrana eDokumentů přináší, oproti ochraně analogových, několik nových, zásadních problémů a s tím spojených bezpečnostních hrozeb. Jedním z těchto problémů je interpretace eDokumentu.

Veškeré informace z analogového dokumentu si člověk dokáže interpretovat sám, pomocí zraku či sluchu. Tak tomu ale u digitálního dokumentu není, k získání všech informací z eDokumentu potřebuje čtenář vždy interpreta, což je v tomto případě osobní počítač, notebook, chytrý telefon či jiné elektrotechnické zařízení, postavené na bázi PC a pokud se jedná o zvukovou informaci, tak také příslušenství k PC jako jsou sluchátka či reproduktory.

Proto již nestačí chránit fyzický nosič, který v analogovém případě, byl jediným nedělitelným[6] originálem a pokud byla zajištěna jeho ochrana a trvanlivost byl v zásadě bezpečný[7], ale je zapotřebí zohlednit i ostatní riziko spojená s eDokumentem.

---

[5] CUBR, Ladislav. *Dlouhodobá ochrana digitálních dokumentů*. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

[6] Digitální data jsou nezávislá na paměťovém médiu dají se tedy snadno přesouvat, a tak je mnohem těžší zajistit jejich autenticitu.

[7] CUBR, Ladislav. *Dlouhodobá ochrana digitálních dokumentů*. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

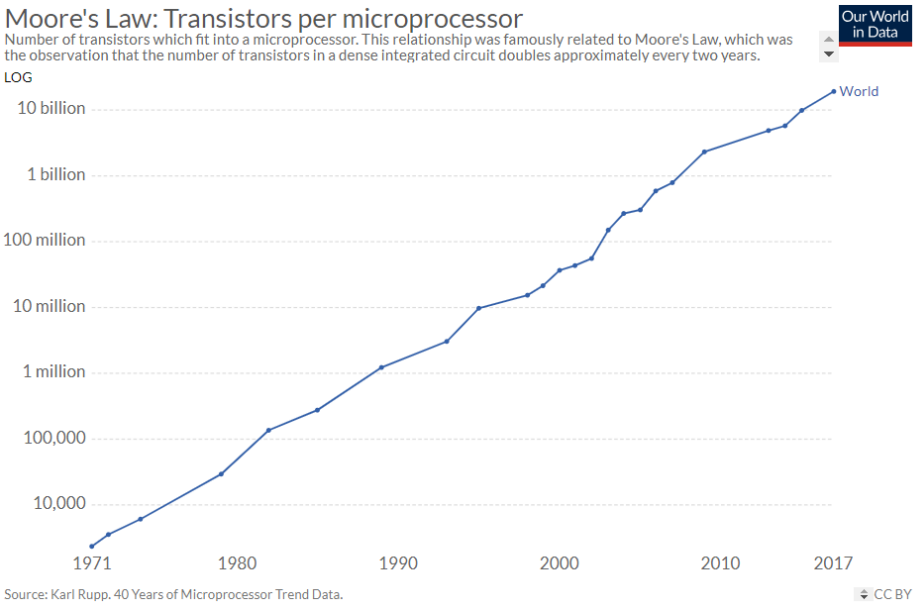
Digitální dokument má tu vlastnost, že fyzický nosič nemusí být jediným nositelem originálu, a tak mu musí být zajištěna ochrana jak fyzická (nosiče), tak softwarová (dat)[8]. To s sebou přináší značnou zátěž jak z pohledu finanční náročnosti, tak z pohledu personálního obsazení.

Finanční náročnost stoupá, oproti analogovým dokumentům, geometrickou řadou, nové technické vybavení, dostatečně chráněná a objemná, vyhovující úložiště dat, softwarové vybavení těchto technických prostředků, softwarové zajištění ochrany, pravosti a autenticity eDokumentů, zajištění dostatečně kvalifikovaného personálu, údržba a instalace všech těchto složitých systémů představují vysokou finanční zátěž.

Vývoj moderních informačních technologií je stále velmi rychlý, a nevypadá to, že by měl zpomalovat. Rozvíjí se jak samotný hardware, tak software. Toto přináší riziko prolomení kryptografických šifer a certifikátů, které jsou pro bezpečné uchování, zajištění integrity a autenticity eDokumentů kritické. S tímto souvisí také problematika přístupu k eDokumentům a jejich čitelnost, jelikož rychlost, s jakou zastarávají jak softwarové, tak hardwarové prostředky je úměrná rychlosti vývoji modernějších HW a SW prostředků.

[8]CUBR, Ladislav. *Dlouhodobá ochrana digitálních dokumentů*. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

Růst výpočetního výkonu lze zjednodušeně shrnout pomocí Moorova zákona[9] , který říká, že za každé 2 roky se počet integrovaných obvodů na procesoru zdvojnásobí.



Obr. 1 – Grafické znázornění Moorova zákona za posledních 46 let[10]

To přináší nejen problém z hlediska kryptografických šifer, ale také z hlediska přístupu k eDokumentu a jeho čitelnosti. Samotný HW a SW zastarává velmi rychle, a tak firmy, které je vyvíjejí jim poskytují časově omezenou podporu. Z hlediska hardware je důležité počítat se zastarávání některých technologií důležitých pro přístup a pro správnou interpretaci eDokumentů. Z hlediska softwaru je zásadní zajistit přístupnost datového formátu daného eDokumentu. Tím se myslí jeho dokumentace a softwarová podpora. Velmi důležitá je v tomto případě možnost konverze do jiného datového formátu, pokud se původní datový formát stane příliš náročným či nemožným na jeho udržování. Tím může být například

[9]V posledních letech toto sice přestává pomalu platit, ale přední firmy ve vývoji výpočetní techniky dokáží tento deficit vykompenzovat v jiných odvětvích. Například vývojem efektivnějších API jako například DirectX 12 nebo Mantle.

[10]ROSER, Max a Hannah RITCHIE. Technological Progress: Moore's Law - exponential increase of the number of transistors on integrated circuits. *Our World In Data* [online]. 2019 [cit. 2019-04-19]. Dostupné z: https://ourworldindata.org/technological-progress

ukončení podpory datového formátu nebo zkrachování firmy vlastnící daný datový formát.

Problematiku ochrany digitálních dokumentů lze rozdělit na tři základní roviny. Jedná se o rovinu technologickou, rovinu informační a rovinu systémovou.

1.3.1. Technologická rovina

Technologickou rovinou se rozumí dlouhodobé uchování nosiče eDokumentu. Základními problémy s tím spojenými jsou degradace nosičů, technologické selhání a technologická zastaralost[11]. Obecně platí, že v této rovině jsou chráněna paměťová média a jejich přehrávače.

Jednou z metod ochrany proti technologické zastaralosti je emulace. Emulací se rozumí reprodukce chování zastaralých technických prostředků na současných technických prostředcích pomocí virtuálního prostředí.[12].

1.3.2. Informační rovina

Informační rovina v sobě potom zahrnuje ochranu datových formátů. Základními problémy informační roviny je potom zajištění dokumentace formátů, jejich specifikace, licence a robustnost[13]. Robustností se rozumí odolnost vůči korupci dat a životnost formátu, která je dána jeho rozšířeností, podporou vývojáře, dokumentací a dalšími parametry.

[11]CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

[12]GUTTENBRUNNER, Mark; RAUBER, Andreas. Evaluating Emulation and Migration: Birds of a Feather?. In: International Conference on Asian Digital Libraries. Springer Berlin Heidelberg, 2012. p. 158.
poznámka: jedná se o vlastní překlad citovaného díla.

[13]CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

Datovou korupcí se rozumí chyby v datech, které se přihodili selháváním či poruchou paměťového média (Například Operační paměť, Pevný disk, SSD).[14] Výsledkem datové korupce je úplná, nebo v lepším případě částečná ztráta dat či jejich nečitelnost. V případě textových souborů se může jednat například o ztrátu znaků nebo jejich zpřeházení. V horším případě o ztrátu celého souboru, který přestává být čitelný. U obrazového souboru naopak dochází k výskytu chybných informací, a tudíž ke ztrátě originálních obrazových informací.

Obr. 2 – Ukázka korupce obrazových dat[15]

[14]Data corruption. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2019-04-19]. Dostupné z: https://en.wikipedia.org/wiki/Data_corruption

[15]Data loss of image: Data Corruption. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-19]. Dostupné z: https://en.wikipedia.org/wiki/Data_corruption#/media/File:Data_loss_of_image_file.JPG

1.3.3. Systémová rovina

Systémovou rovinou se rozumí ochrana digitálních dokumentů z hlediska jejich organizace a přístupnosti. Základními problémy systémové roviny jsou uspořádání velkého množství eDokumentů do logických struktur, zajištění přístupu k těmto strukturám, a nakonec jejich samotná identifikace v rámci způsobu jejich organizace.[16]

1.4.Metadata

Velmi důležitým aspektem je také popis eDokumentu, konkrétně souvisejících metadat. Metadata představují informace o uložených datech v určitém dokumentu, někdy bývají také označována jako data o datech. eDokument, který není řádně popsán ztrácí mnoho ze své původní hodnoty. Metadata představují informace o uložených datech v určitém dokumentu, někdy bývají také označována jako data o datech. Jedná se o popisy daných dat, které jej blíže specifikují (název, datum vydání, autor, licence aj.).

Podoba a struktura těchto metadat je stanovena několika zásadními metadatovými standardy. Každý tento metadatový standard má potom vlastní manuál, který popisuje jednotlivé popisné prvky pro daný dokument. Jako vzory pro popis eDokumentu slouží potom metadatová schémata. Pro jejich psaní se využívá značkovacího jazyka XML. Popis dokumentu pomocí metadat je nedílnou součástí jakéhokoliv systému pracujícím s eDokumenty, například Document Management System(DMS)[17] nebo eSSL.

Metadata lze rozdělit do několika základních kategorií popisu. První z nich jsou metadata popisná. Tato metadata slouží k popsání obsahu dokumentu. Jedná se například o název, původce, rok vydání, místo vydání. Obecně lze říct, že tyto metadata slouží k identifikaci popisovaného eDokumentu.[18]

---

[16]CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

[17]O EDMS a eSSL více v kapitole Elektronický systém spisové služby.

[18]Metadata: Typy metadat. *Wikisofia* [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/Metadata

Druhou kategorii tvoří metadata administrativní, které, jak už z názvu vypovídá, slouží především ke správě digitálních dokumentů. Jedná se například o informace o vzniku dokumentu, jeho úprav a další podpůrné informace.

Lze je dále dělit na metadata archivační, technická a právní. Archivační metadata obsahují prvky popisu, které jsou důležité z archivního hlediska. Těmi jsou například informace o původci nebo krátké historii dokumentu. Technická metadata potom slouží k upřesnění technické charakteristiky eDokumentu. Jedná se například o velikost souboru, souborový formát, rozlišení, délka videa a další. Metadaty právními se rozumí takové prvky popisu, které upřesňují jeho právní charakteristiku.[19] Jedná se například o licenční ujednání, autorské právo, doba trvání licence a další.

Poslední kategorií metadat jsou metadata strukturální. Taková metadata slouží k popisu vnitřní struktury dokumentu. Poskytují informace o vnitřní organizaci a vyjadřují strukturu digitálního objektu. Může se jednat například o jednotlivé stránky čísel časopisů.[20]

1.4.1. Dublin Core

Nejběžnější metadatový standard pro popisná metadata, který je velmi jednoduchý, modulární a lehce čitelný. Používá 15 popisových prvků, které nejsou povinné[21]. Soubor je potom uložen v HTML či XML souborovém formátu.

Z důvodu oblíbenosti, jednoduchosti a jeho přístupnosti byla vytvořena vyšší verze Dublin Core zvaná Kvalifikovaný Dublin Core, který přináší zpřesnění prvků popisů, aniž by je ale rozšiřovali o nové. K zpřesnění těchto prvků používá tzv.

[19]Metadata. *Wikisofia* [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/Metadata

[20]Metadata. *Wikisofia* [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/Metadata

[21]Dublin Core. Wiki knihovna.cz [online]. 2012 [cit. 2019-04-19]. Dostupné z: http://wiki.knihovna.cz/index.php/Dublin_Core

kvalifikátory, ty lze rozdělit na kvalifikátory, které pomáhají k interpretaci jednotlivých prvků a na kvalifikátory zpřesňující význam jednotlivých prvků.[22]

1.4.2. METS

Metadatový standard METS je definován jako standard pro kódování popisných, administrativních a strukturálních metadat o digitálních objektech.[23]

Metadatový standard, který je využíván v SIP balíčcích k popisu metadat u textových a audio eDokumentů[24]. Nabízí velmi široké využití v paměťových institucích, jelikož je velmi univerzální a všestranný. Svou strukturu definuje v XML formátů.

1.4.3. MODS

Společně s Dublin Core je MODS pravděpodobně nejpoužívanějším metadatovým standardem pro popisná metadata. Stejně jako Dublin Core využívá souborů ve formátu XML. Mezi jeho největší výhodu patří jeho všestrannost Je totiž použitelný při výměně záznamů mezi institucemi, které jej používají[25]. Navíc je konvertibilní se standardem Dublin Core. MODS vyvíjí a udržuje Kongresová Knihovna USA. Obsahuje 20 prvků popisu s možností využívat i podprvky. Největší zastoupení má potom v USA, odkud podchází.

---

[22]Kvalifikovaný Dublin Core: Dublin Core Qualified, DCQ. *KTD - Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*[online]. 2012 [cit. 2019-04-02]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00000/08/000000895.htm

[23]SNÍŽKOVÁ, Martina. METS. *Wikiknihovna.cz* [online]. 2012 [cit. 2019-04-13]. Dostupné z: http://wiki.knihovna.cz/index.php/METS

[24]Standardy pro metadata. NDK Národní digitální knihovna [online]. 2018 [cit. 2019-04-19]. Dostupné z: https://www.ndk.cz/standardy-digitalizace/metadata

[25]BARTOŠEK, Miroslav. Digitální knihovny - teorie a praxe. Národní knihovna: knihovnická revue[online]. Praha: Národní knihovna ČR, 2004. 2004, roč. 15, č. 4 [cit. 2012-04-26], s. 233-254. Dostupný z WWW: < http://eprints.rclis.org/6901/1/DL-Bartosek-final2.pdf>. ISSN 1214-0678

1.4.4. PREMIS

Oproti MODS a Dublin Core se Premis specializuje na metadata archivační a technická. Standard řídí a spravuje PREMIS vydavatelská komise.[26] Standard se skládá z XML schématu, slovníku pojmů a podpůrné dokumentace. PREMIS je tak určen především pro archivy, jelikož je vytvořen s ohledem na OAIS[27].

[26]PREMIS. PREMIS Preservation Metadata Maintenance Activity [online]. 2018 [cit. 2019-04-19]. Dostupné z: https://www.loc.gov/standards/premis/

[27]Open Archive Information System je referenční model fungování archivu

2. Informační bezpečnost

Bezpečnost eDokumentu lze rozdělit do dvou kategorií. Prvním z nich je zabezpečení samotného eDokumentu (pomocí elektronického podpisu a dalších prvků[28]). Druhou je potom zabezpečení samotné instituce, která s nimi pracuje.

2.1.Šifrování

Základním prvkem veškeré bezpečnosti v kyberprostoru je právě šifrování. V dnešní době dokáže i téměř jakýkoliv amatér vysledovat téměř jakýkoliv nešifrovaný obsah v prostředí internetu pomocí jednoduchých programů volně dostupných ke stažení na internetu[29]. Samotné šifrování lze potom definovat jako proces, při kterém dochází k utajení dané informace, která je dostupná pouze za pomocí šifrovacího klíče.[30]

Existují dva základní způsoby šifrování. Asymetrické a symetrické, kdy symetrické je snáze prolomitelné a využívá pouze jeden klíč. Nejběžnějšími symetrickými šiframi jsou potom AES, DES, RC2. Největší nevýhodou tohoto typu šifrování je potom fakt, že jelikož existuje pouze jeden klíč, kterým lze obsah dešifrovat, takže si jej musí obě strany nějakým způsobem vyměnit.

Druhým, více používaným, způsobem je asymetrické šifrování, které funguje na bázi dvou klíčů – veřejného a soukromého. Nejběžnější používanou šifrou je potom RSA. Dá se říct, že elektronický podpis, razítko aj. mohou fungovat relativně bezproblémově pouze pomocí asymetrického šifrování. Oproti symetrické šifře má jednu nevýhodu a tou je rychlost šifrování a dešifrování, která, jelikož se jedná o složitější metodu, je mnohem pomalejší. Zároveň ale trvá mnohem déle ji prolomit pomocí Brute Force, pro variantu 512 b a výše je to takřka nemožné.

Asymetrické šifrování funguje tak, že každá osoba v komunikaci má jeden veřejný a jeden soukromý klíč. Pokud chce BFU1 poslat zprávu BFU2, využije

[28]Popsaných v kapitole o eIDAS.

[29]Jako například WireShark, MS Network Monitor, Ethereal.

[30]Šifrování dat. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2017 [cit. 2019-04-19]. Dostupné z: https://cs.wikipedia.org/wiki/%C5%A0ifrov%C3%A1n%C3%AD_dat

k zašifrování zprávy veřejný klíč BFU2, který je volně dostupný. Takovouto zprávu lze potom odšifrovat jedině soukromým klíčem BFU2. Toto využívá například elektronický podpis s jedním zásadním rozdílem. V případě elektronického podpisu musí vždy existovat třetí strana, která garantuje vlastníka daného klíče, v tomto případě el. podpisu. Její integrita je potom zajištěna pomocí hashe, což je matematický výpočet vytvořený z daného eDokumentu, který při jeho jakékoliv úpravě změní i sám sebe[31], a tudíž není totožný s tím původním hashem. V tomto případě se tedy nejedná o nezměněný eDokument.

2.2.Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací z anglického označení Information Security Management Systém (ISMS) představuje systém, který se stará, jak je z názvu patrno, o správu informační bezpečnosti[32]. V podstatě se zaměřují na několik základních pilířů, které mají zajišťovat, co možná nejvíce bezpečný systém. Skládá se jak z technických opatření, tak různých bezpečnostních pravidel a organizační struktury.

Mezi tyto pilíře patří analýza aktiv[33] a jejich ochrana, kdy aktivum je definováno velmi obecně jako něco mající pro instituci či organizaci hodnotu, kterou je potřeba zabezpečit. Může se jednat o velmi širokou škálu věcí, různá fyzická média či servery, know how, utajované informace, dílčí data či databáze a jiné[34]. Z počátku se vždy počítá s analýzou těchto aktiv, kdy se nejprve zjistí, co je potřeba ochránit, potom se vytvoří prioritní seznam, jelikož tyto aktiva nemají stejnou hodnotu a tudíž důležitost.

[31]Podoba hashe je pevně vázána na podobu eDokumentu.

[32]ISMS. WikiSofia [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/ISMS

[33]Z tohoto pohledu je možná vhodnější anglický termín – (information) assets, což v překladu znamená (informační) zdroje či hodnoty.

[34]Tento výčet není nijak definován, aktiva jsou jednoduše věci, které v systému je potřeba chránit, takže umožňují značnou flexibilitu. Mezi nimi lze zařadit také eDokumenty.

Dalším pilířem je potom analýza rizik, které mohou ohrozit daný systém a pokud tato rizika překročí akceptovatelnou úroveň[35], tak vzniká reakce v podobě protiopatření jako například změna šifrovacího algoritmu, úpravy vnitřní bezpečnostní politiky, změna různých zařízení aj.

Celé si to lze představit jako cyklus, kdy se nejprve kompletně zanalyzují aktiva, potom daná rizika, která když překročí snesitelnou úroveň a stanou se z nich hrozby, jsou potlačována protiopatřeními.

Obr. 3 – životní cyklus kybernetické bezpečnosti[36]

2.3.ISO 27000, 27001, 27002

Z právního hlediska v České republice existuje rodina norem ISO 27000 zabývající se systémy řízení informační bezpečnosti, kdy především první tři jsou velmi důležité. Jsou jimi ISO 27000, 27001, 27002. ISO 27000 funguje jako slovník technických pojmů.

ISO 27002 je velmi obsáhlou normou, která přímo definuje velmi přesně jednotlivá bezpečnostní opatření, obsahuje více než 114 strukturovaných doporučení, ve kterých je více než 5000 bezpečnostních opatření, které podporují

[35]Každé odhalené riziko pro daná aktiva má určitou úroveň, dokdy je stále relativně v bezpečí a vytváření nových protiopatření se jednoduše nevyplácí.

[36]ZÁKLADNÍ POJMY. *KYBEZ Platforma kybernetické bezpečnosti* [online]. 2018 [cit. 2019-02-12]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

dosahování podnikatelských cílů.[37] Norma ISO 27001, která nezabíhá do přímých technickobezpečnostních opatření, definuje způsob, jakým se tato opatření zavádí. Zjednodušeně lze říci, že ISO 27002 poskytuje stavební kámen systému, zatímco ISO 27001 poskytuje příručku, jak tento systém postavit.

2.4. COBIT a ITIL

Další věc, o které je potřeba se zmínit s ohledem na ISO 27001 je metodika COBIT a Framework ITIL. Je potřeba zdůraznit, že COBIT a ITIL si jsou navzájem kompatibilní, je tedy optimální, aby byli oba používány společně. Zmíněné ISO normy v předešlé kapitole jsou zaměřeny čistě na informační bezpečnost, zatímco COBIT a ITIL mají širší zaměření, přesto spolu ale velmi úzce souvisí a koexistují.

Hlavním cílem COBITu je plně řídit celou informatiku dané společnosti. Jedná se o souhrn metod, poznatků, procesů a politik pro řízení celého systému.[38] Je tedy mnohem obecněji založený, jelikož se stará o co nejširší část informatiky.

Tuto obecnost lze například vypozorovat *„…v oblasti popisu procesů přichází pouze s výčtem vstupů, výstupů, rolí a aktivit, avšak jedná se jen o jejich pojmenování a podrobnější popis toho, co je tím myšleno, většinou schází.“*[39]

Na druhou stranu ITIL je zaměřen pouze na IT management, a tak sice nemá tak široký záběr jako COBIT, ale zato tento framework obsahuje mnohem hlubší informační základ (definice, procesy, způsoby implementace aj.), kterým COBIT nedisponuje.

---

[37]ISMS: normy ISO 27001 a ISO 27002. *RiskAnalysisConsultants* [online]. 2018, 2018 [cit. 2019-02-12]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799

[38]HOUŠKA a KUNC. COBIT: Co je to COBIT?. Underground ÚAI [online]. [cit. 2019-04-19]. Dostupné z: http://www.uai.tode.cz/stud_mat/Management_IS/Cobit.pdf

[39]Vztah ITIL® a CobiT. *BESTPRACTICE.CZ: IT Management Knowledge Base* [online]. [cit. 2019-02-12]. Dostupné z: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Vztah-ITIL-a-dalsich-pristupu/Vztah-ITIL-a-CobiT.alej

3. Elektronická identifikace a služby vytvářející důvěru (eIDAS)

Pro fungující systém masivní důvěryhodné elektronické komunikace je potřeba zajistit 3 základní věci, a to:

- jednoznačnou identifikaci účastníka komunikace,
- důvěryhodnost samotného obsahu komunikace,
- prostředí a prostředky nutné ke komunikaci.

Především o první dva body se právě snaží nařízení EU eIDAS (č. 910/2014).

Při použití IT terminologie by bylo možné připodobnit toto nařízení eIDAS masivnímu frameworku či sadě standardů, dle kterého se mají členské státy řídit, aby byl zajištěn digitální trh a jednotný systém důvěryhodné elektronické komunikace. Oběh důvěryhodných eDokumentů by měl být tedy možný mezi všemi členskými zeměmi Evropské Unie bez jakýchkoliv obstrukcí. Soustředí se především na dvě základní oblasti působení, a to elektronickou identifikaci a služby vytvářející důvěru.

Do českého prostředí je toto nařízení zavedeno pomocí zákona č.297/2016 Sb., č. 298/2016 Sb. a č.250/2017 Sb. Pozici garanta a dohlížitele zastupuje Ministerstvo vnitra.[40]

3.1. Elektronická identifikace

Oblast nařízení Evropské Unie eIDAS zavádí elektronickou identifikaci občanů pomocí elektronického občanského průkazu (eOP v aj. eID).

Tyto občanské průkazy mohou komunikovat s úřady přes Portál veřejné správy.

Nový eOP funguje také jako nosič kvalifikovaných certifikátů, tudíž odpadá potřeba USB Tokenů a jiných zařízení. Tyto elektronické občanské průkazy v sobě mají zabudován čip, který obsahuje certifikát, kterým se její nositel při komunikaci s úřady jednoznačně identifikuje. Správu těchto certifikátů má na starosti Národní identitní autorita a její systém.

[40]EIDAS, ELEKTRONICKÝ PODPIS. *Ministerstvo vnitra České republiky* [online]. Praha: Odbor eGovernmentu, 2016 [cit. 2018-07-24]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx

S novými eOP přichází také řada problémů. Ke každému eOP je nutné spolu s eOP vlastnit až 6 přístupových klíčů, pokud chce občan využívat všechny funkce eOP. Nutnost vlastnit 6 klíčů a samotnou eOP samo o sobě představuje potenciálně vysoké bezpečnostní riziko, zároveň potom značně snižuje atraktivitu[41] takového občanského průkazu. Při vydání nového občanského průkazu je dnes tato eOP standardem a o starší „verzi“ si zažádat nelze. Naštěstí pro mnohé si lze alespoň tyto funkce deaktivovat, po deaktivaci je už ale nelze obnovit, v takovém případě musí občan zažádat o nový eOP.

Naopak výhody plynoucí z tohoto nového OP jsou zřejmé, elektronický občanských průkaz umožňuje nositelům komunikaci s úřady prakticky odkudkoliv, vzhledem k možnostem dnešního datového připojení. Zkrácení čekacích lhůt by se mělo tak stát minulostí a pro současné mladší generace naší společnosti v tomto digitálním věku by se tento způsob komunikace měl stát také preferovaným.

3.2. Služby vytvářející důvěru

Tato oblast nařízení Evropské Unie eIDAS má za úkol právně ošetřit a zavést prostředky zajišťující integritu, autentičnost a původ eDokumentů a s nimi spojenými službami vytvářejících důvěru.

Nařízení EU 910/2014 (eIDAS) je definuje jako zpravidla placené[42] služby, které vytvářejí / kontrolují / uchovávají prostředky potřebné k zajištění důvěry eDokumentu. (Elektronický podpis, elektronické časové razítko, elektronická pečeť, certifikát aj.).

Služby vytvářející důvěru mají za úkol zajistit důvěryhodnost eDokumentů, což naplňují pomocí výše zmíněných prostředků, které jsou rozebrány v následujících kapitolách, a s nimi spojenými kvalifikovanými certifikáty. Tyto služby platí napříč členskými zeměmi Evropské Unie.

[41]Na samotných stránkách eIdentity autoři uznávají, že tyto klíče mohou být matoucí.

[42]V oficiálním znění (bod 16 článek 3) je definice, až s podivem, na to, že se jedná o právní dokument, uvedena takto obecně.

3.2.1. Elektronický podpis

Elektronickým podpisem se rozumí data v elektronické podobě, připojená nebo logicky spojená s datovou zprávou, která mohou být použita k identifikaci podepisující osoby ve vztahu k datové zprávě a představují její souhlas s informacemi, v datové zprávě obsaženými.[43] Jedná se o obdobu klasického podpisu, připojuje se k eDokumentu a vyjadřuje souhlas s jeho obsahem a je základním kamenem oběhu dokumentů v eGovernmentu. Umožňuje jednoznačně spojit vlastníka podpisu s eDokumentem, kterou zároveň dokáže identifikovat. Zajišťuje také tzv. neporušenou integritu (neměnnost). V legislativě České republiky je ošetřen zákonem č. 297/2016 Sb.

V České republice jsou zákonem zakotvené 3 varianty elektronického podpisu:

- zaručený elektronický podpis (ZEP,
- kvalifikovaný elektronický podpis[44] (KEP),
- „běžný“ elektronický podpis (EP).

Každá tato varianta elektronického podpisu nabývá různých právních hodnot. Kvalifikovaný elektronický podpis je takový elektronický podpis, který poskytuje eDokumentu stejnou právní účinnost, jakou nabízí analogový dokument. Umožňuje jednoznačně identifikovat danou osobu. Kvalifikovaný certifikát, na kterém je tento typ podpisu založen je garantován tzv. certifikační autoritou[45], která garantuje informace obsažené v certifikátu. Tyto certifikační autority mají hierarchickou strukturu a platí po celé Evropské Unii díky nařízení eIDAS, které si klade za cíl

[43]MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.

[44]Zde je často zmatek v názvosloví. Často se uvádí místo kvalifikovaného elektronického podpisu pojem uznávaný elektronický podpis. V oficiálním dokumentu eIDAS se nikde pojem uznávaný elektronický podpis nevyskytuje, správným pojmem je kvalifikovaný elektronický podpis. Uznávaný elektronický podpis je zaveden pouze v České legislativě, kde je akceptován v situacích, kdy by se mělo využívat kvalifikovaného elektronického podpisu.

[45]V České republice poskytují kvalifikované certifikáty celkem tři certifikační autority – První certifikační autorita, Česká pošta a eIdentity

unifikovat systém eDokumentů ve státních správách, a tak umožnit průběh eDokumentů mezi všemi členskými zeměmi Evropské Unie.

Zaručený elektronický podpis je totožným s kvalifikovaným elektronickým podpisem, s tím zásadním rozdílem, že neobsahuje kvalifikovaný certifikát. Lze jej definovat jako digitální data, která podepisující osoba vytváří svým privátním klíčem a zajišťuje jimi integritu a nepopiratelnost původu podepsaných dat.[46]

Kvalifikovaný certifikát slouží dokumentům jako záruka pravosti elektronického podpisu a certifikační autority. Obsahují jméno, příjmení a bydliště osoby, či pokud se jedná o právnickou osobu, tak název a sídlo firmy, data pro certifikování podpisu, unikátní číslo (ID) kvalifikovaného certifikátu, identifikátor vydávající certifikační autority, dobu, v které certifikát platí. Další osobní údaje lze doplnit jen se souhlasem osoby vlastnící kvalifikovaný elektronický podpis. Certifikační autorita, v nařízení zvaná kvalifikovaný poskytovatel služeb, garantuje a zajišťuje pravost a bezpečí všech svých certifikátů, a pokud dojde k jakémukoliv narušení bezpečnosti kteréhokoliv certifikátu, tak se takový certifikát stává neplatným. Zároveň nositel podpisu má za povinnost tento elektronický podpis chránit a dodržovat základní bezpečnostní opatření.[47]

Pokud by došlo ke ztrátě, tak to musí vlastník co nejdříve nahlásit příslušné certifikační autoritě. Všechny elektronicky podepsané dokumenty po té době jsou zneplatněny a elektronický podpis je vyřazen ze seznamu platných elektronických podpisů. Certifikační autorita tedy přestává garantovat platnost daného certifikátu a ruší jej.

Kvalifikovaný elektronický podpis má dnes využití v mnoha složkách státní správy, především pro právnické, ale i fyzické osoby.

Mezi nejčastější využití elektronického podpisu patří situace, kdy dojde k:

- využití datové schránky,
- podepisování různých dokumentů,

[46]Zaručený elektronický podpis. *První certifikační autorita* [online]. [cit. 2018-07-20]. Dostupné z: http://www.ica.cz/Zaruceny-a-uznavany-ep

[47]Neohlášená ztráta či nedbalé zacházení může být klasifikována jako přestupek.

- podávání daňového přiznání z přidané hodnoty či příjmu[48],
- komunikaci se státní a veřejnou správou nebo zdravotními pojišťovnami.

Obecně platí, že elektronický podpis má využití všude, kde je dnes nutný vlastnoruční podpis.[49]

Vlastnění elektronického podpisu ale nese i jisté povinnosti. Nositel má povinnost se seznámit se správným zacházením s elektronickým podpisem a nese za něj zodpovědnost. V případě, že elektronický podpis předá jiné osobě či jej neodevzdá k evidenci se může dopustit i přestupku a finanční pokuty. Přestupky dle zákona o službách vytvářejících důvěru pro elektronické transakce projednává ministerstvo vnitra.

Základním rizikem všech variant elektronického podpisu je stav, kdy v okamžiku podepsání dokumentu elektronickým podpisem tento obsahuje i časové razítko, kdy byl dokument podepsán, a to ze systémového času uživatelského operačního systému. Tento čas si ale téměř každý, kdo má alespoň nějaké základní znalosti práce s informačními technologiemi, může nastavit dle potřeby, a tak časové razítko nemusí nést odpovídající časový údaj. To může být problém například při podepisování závislých elektronických dokumentech.

Dalším rizikem, souvisejícím s elektronickými podpisy a se kterým je nutno počítat, je nutnost důvěřovat certifikační autoritě a jejím kvalifikovaným certifikátům. Certifikační autority jsou strukturované hierarchicky, a tak platí, že pokud by došlo ke ztrátě důvěry některé z certifikačních autorit, které jsou v žebříčku na vysokých pozicích, mohlo by dojít k vysokým škodám, nejen ve státním, ale i v soukromém sektoru.

---

[48]BÍLÝ, Radek. Elektronický podpis – k čemu je dobrý a jak jej získat?. Portál.pohoda [online]. 2016 [cit. 2019-04-19]. Dostupné z: https://portal.pohoda.cz/pro-podnikatele/uz-podnikam/elektronicky-podpis-%E2%80%93-k-cemu-je-dobry-a-jak-jej-zi/

[49]MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.

Příkladem tohoto je kauza Nizozemské certifikační autority DigiNotar, kdy se neznámému útočníkovi podařilo zcizit přes 500 podvodných certifikátů. Reakce certifikační autority DigiNotar byla bohužel velmi pomalá. Některé vystavené falešné certifikáty měli platnost až měsíc a půl.

*„Reakce napadené autority ale nebyla zdaleka tak rychlá a důsledná, jako v případě COMODO: DigiNotar revokoval podvodně vydané certifikáty až s určitým zpožděním. Na jeden z nich dokonce nějak „pozapomněl", resp. ani nezaregistroval, že byl vydán. Shodou okolností či náhod šlo právě o SSL certifikát, vystavený na *.google.com, a to již 10. července 2011. Na jeho existenci se přišlo až 29. srpna 2011, a revokován byl téhož dne v 19:09."*[50]

DigiNotar nakonec ztratila důvěru a již se nedokázala z kauzy vzpamatovat. Nakonec došlo také k jejímu krachu.

3.2.1.1. ETSI standardy

Podobu elektronického podpisu, jeho umístění a další údaje definuje ve svých standardech organizace ETSI[51]. „*ETSI je uznávaná jako oficiální standardizační organizace Evropskou komisí. V oblasti elektronických podpisů tedy připravila standardy, které požadavky Evropské komise splňují."*[52]

Dnes se u nás v zásadě uplatňují tři základní standardy[53]. Prvním z nich je CAdES, který je velmi všestranným, protože umožňuje podepsání jakéhokoliv typu digitálních dat. Právě díky tomu je u nás využíván v systému Datových schránek. Jeho všestrannost ovšem nespočívá pouze v jeho umění podepsat jakýkoliv typ digitálních dat, ale také ve formě samotných dat a podpisu k nim připojeným. Tento

[50]Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. Lupa.cz [online]. 2011 [cit. 2019-04-19]. Dostupné z: https://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/

[51]Standardy jsou důležité z hlediska archivace, kdy všechny tři umožňují tzv. LTV – Long Term Validity, což lze volně přeložit jako dlouhodobou dobu platnosti.

[52]Normy ETSI: Vznik standardů. *EARCHIVACE.CZ* [online]. 2014 [cit. 2019-03-19]. Dostupné z: http://www.earchivace.cz/legislativa-a-normy/aplikace-norem-pro-elektronickou-archivaci/

[53]Všechny jsou samozřejmě v souladu s eIDAS

standard umožňuje určitou flexibilitu. Definuje totiž způsob zpracování podpisu a principy jeho fungování, ale nijak nedefinuje způsob, jakým mají být tyto informace podpisu uchovány (jestli uvnitř, kolem, nebo vedle samotného eDokumentu.[54]

Druhým standardem je potom XAdES, který je oproti obecnému CAdESu zaměřen na dokumenty formátu XML, ovšem podporuje ale i další formáty.

Posledním ze standardů je potom PAdES, který umožňuje elektronický podpis pouze PDF dokumentů, a i když je přesně zaměřen a přesně definuje podobu a umístění elektronického podpisu, tak se jedná v mnohých ohledech spíše o výhodu než nevýhodu především z ohledu bezpečnosti.

3.2.2. Časové razítko

Mezi základní metadata elektronického dokumentu patří také časové razítko, což je, společně s kvalifikovaným elektronickým podpisem, základní prvek informace o eDokumentu. Časové razítko slouží k zaznamenání času vytvoření daného eDokumentu, kdežto elektronický podpis jen určuje čas podepsání. Poskytuje tedy dokumentu časový údaj jeho vzniku.

Připojuje se k dokumentům jako důkaz, že v daném čase a v dané podobě existovaly. Spojení nezpochybnitelného časového údaje a konkrétních dat je nutné pro účely jejich zpětného ověření. Často bývá kombinováno právě s elektronickým podpisem.[55]

Znovu, jako u elektronického podpisu, existuje varianta časového razítka zvaná kvalifikované časové razítko, které nabízí navíc garanci pravosti časového záznamu. Tyto kvalifikovaná časová razítka poskytují certifikační autority, které pomocí certifikátů, obdobný princip jako u elektronických podpisů, umožňují zajistit pravost těchto časových razítek.

---

[54]Normy ETSI: Vznik standardů. *EARCHIVACE.CZ* [online]. 2014 [cit. 2019-03-19]. Dostupné z: http://www.earchivace.cz/legislativa-a-normy/aplikace-norem-pro-elektronickou-archivaci/

[55] Elektronická časová razítka. *První certifikační autorita* [online]. [cit. 2018-07-21]. Dostupné z: http://www.ica.cz/elektronicka-casova-razitka

Elektronická časová razítka jsou důležitá také z hlediska dlouhodobého ukládání dat, protože zajišťují, že se dokument od „orazítkování“ nezměnil a je mu tedy zaručena právní účinnost po celou dobu jeho platnosti.

Využití elektronických časových razítek je vcelku široké, nalezneme využití jak ve službách elektronické státní správy a justice, ale i v soukromých sférách.

Elektronická časová razítka jsou funkční v mnohých službách, např. I.CA Secom, Adobe Acrobat, Adobe LiveCycle, JSignPDF, podepsatPdf (TOPSPIN), LongTermValidator, informační systém datových schránek (ISDS), systémy elektronického bankovnictví, spisové služby, e-fakturace, e-podatelny, důvěryhodná úložiště (archívy), v různých bankovních řešení, IS v oblasti justice a advokacie atd.[56]

Jedním z problémů časových razítek je fakt, že není zcela jisté, jak dlouho elektronický dokument existoval před aplikací otisku časového razítka. Mezi dobou, kdy byl elektronický dokument „orazítkován“ a jeho vznikem je vždy nějaká drobná prodleva.

Okamžik vytvoření eDokumentu není nutně tím časovým bodem, kdy je na něj naneseno časové razítko. Toto může být riziko také z právního hlediska, kdy definice v zákoně není úplně výkladově jasná.

Problém by měla ale vyřešit jednoduchá úprava definice elektronického časového razítka v zákoně, popřípadě vést záznam reálného času podpisu dokumentu a čas vzniku dokumentu se zaznamenanou prodlevou, což sice odstraní tento problém z právnické stránky, ale z pohledu zabezpečení se stále jedná o možné využitelné bezpečnostní riziko. Toto riziko je téměř nemožné odstranit se stávajícími technickými prostředky, prodleva mezi těmito časy zůstává tedy možným rizikem a měla by se minimálně vést evidence obou těchto časů.

[56]Elektronická časová razítka. *První certifikační autorita* [online]. [cit. 2018-07-23]. Dostupné z: http://www.ica.cz/elektronicka-casova-razitka

Určitým řešením by mohla být změna definice. *„Možná by bylo přesnější použít definici jinou, právnicky přesnější, tj. typu: data existovala v okamžiku vytvoření vzorku (hash) dokumentu a jeho doručení k poskytovateli.“*[57]

3.2.3. Elektronická značka

Elektronická značka je dalším z ochranných prvků elektronického dokumentu. Technologicky se jedná o elektronický podpis, avšak rozdíl mezi elektronickým podpisem a značkou je především v právním charakteru obou pojmů.

Využívá se především ve strojově vytvářených dokumentech a může jej využít jak fyzická, tak právnická osoba. Jelikož její využití nevyžaduje fyzickou osobu, tak je možné ji přiložit k eDokumentům automatizovaným způsobem, a tím pádem zrychlit jejich oběh.

Elektronická značka je čistě záležitost legislativy České republiky, kdežto například elektronická pečeť je nařízení eIDAS z Evropské Unie, kterým by se měli řídit všechny členské země. Mezi hlavní rozdíly těchto dvou způsobů podepsání dokumentu je jejich použití a platnost. Státy mimo Českou republiku neuznávají elektronickou značku, jako validní formu podepsání dokumentu, kdežto alespoň od států Evropské Unie je vyžadováno, aby byla elektronická pečeť uznávaným způsobem podepsání dokumentu. Členské země Evropské Unie mají rozdílný způsob a rychlost zavádění nařízení Evropské Unie eIDAS, a tak není její využití v současné době všude stejně garantováno.

Elektronickou značku může použít jak fyzická, tak právnická osoba na jakýkoliv typ dokumentu, kdežto elektronickou pečeť může použít pouze právnická osoba a pouze na své vlastní dokumenty.

Připojení elektronické pečeti není projevem vůle, ale spíše označení původu. Právnická osoba připojující pečeť tedy říká, že je původcem daného eDokumentu opatřeného touto pečetí. Z tohoto důvodu je zřejmé, že ji nelze připojovat

[57]MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.

k eDokumentům, které nejsou ve vlastnictví dané právnické osoby.[58] Elektronickou značkou naopak lze podepsat i takový dokument, který není vytvořen podepisujícím. Dle právní definice je elektronická značka projevem vůle podepisovatele, kdežto elektronická pečeť je důkazem o původci dokumentu.

3.2.4. Elektronická pečeť

Jak již bylo výše naznačeno dalším zástupcem Novějším prostředkem nařízení Evropské Unie eIDAS je elektronická pečeť, kterou lze použít ve všech členských zemích Evropské Unie. Je určena pouze pro právnické osoby. Nevyjadřuje souhlas osoby s obsahem dokumentu, ale spíše vůli jej označit, proto se také nazývá pečeť, funguje jako poznávací znak dané firmy.

eDokument či písemnost jsou po opatření elektronické pečetě považovány jako označené danou společností. Značně zrychlují oběh dokumentů firem a jiných společností, jsou běžně používány při strojově vytvářených eDokumentech, které nemusí nutně vyžadovat podepsání kvalifikovaným elektronickým podpisem.

Má také své varianty, kdy nejvyšší úroveň představuje elektronická pečeť opatřená kvalifikovaným certifikátem.

Získání elektronické pečetě je podmíněno vlastněním platného kvalifikovaného certifikátu pro elektronický podpis nebo komerčního osobního certifikátu. Musí se zároveň jednat o právnickou osobu.[59]

Po technické stránce je elektronická pečeť vlastně to samé, co elektronický podpis, s tím rozdílem, že nabývá jiných právních hodnot, zmíněných v předchozím odstavci.

Stejně jako elektronický podpis má několik variant s různou úrovní právní působnosti. Hlavní využití pečetě je ve strojovém vytváření elektronických

---

[58]EIDAS: Elektronické značky a pečetě a rekviem za datovou zprávu. *Lupa.cz* [online]. [cit. 2018-07-22]. Dostupné z: https://www.lupa.cz/clanky/eidas-elektronicke-znacky-a-pecete-a-rekviem-za-datovou-zpravu/

[59]Vydání certifikátu pro elektronickou pečeť. *PostSignum* [online]. [cit. 2018-07-21]. Dostupné z: http://www.postsignum.cz/vydani_prvotniho_certifikatu_pro_elektronickou_pecet.html

dokumentů, kde není stanovena zákonem nutnost použít elektronický podpis. Mezi základní úrovně elektronické pečetě patří běžná elektronická pečeť, která nenabývá žádné právní hodnoty, poté kvalifikovaná elektronická pečeť, která k vydání potřebuje kvalifikovaný certifikát certifikační autority, a tak jasně dokáže určit právnickou osobu.

3.2.5. Srovnání elektronické pečetě a elektronické značky

V následující tabulce je provedeno základní srovnání elektronické značky a elektronické pečetě. Zásadní rozdíl tkví v tom, že elektronická pečeť je právně ošetřena z hlediska použití, kdežto elektronická značka není. Navíc byla elektronický značka zavedena ještě před akceptováním nařízení eIDAS z Evropské Unie.[60]

parametry	elektronická značka	elektronická pečeť
význam	souhlas s dokumentem	vyjádření vlastnictví
použití	fyzická i právnická osoba	právnická osoba
působnost	pouze Česká republika	členské země Evropské Unie
podepisovatelné	všechny edokumenty	pouze vlastní edokumenty

Obr. 4 – porovnání elektronické značky a pečeteˇ[61]

3.2.6. Certifikát

Certifikát obecně představuje datový soubor, který zajišťuje pravost elektronických podpisů, časových razítek, elektronických pečetí a elektronických značek[62]. Vydávají jej certifikační autority, které je zároveň spravují a evidují. Umožňuje tvorbu kvalifikovaných elektronických podpisů a dalších prvků popisu

[60]Proto i její zavedení bylo, v porovnání s dalšími členskými zeměmi Evropské Unie, vcelku rychlé a svižné.

[61]Zdroj: vlastní zpracování

[62]Kvalifikovaný certifikát pro elektronický podpis. I. Certification Authority: První certifikační autorita [online]. [cit. 2019-04-19]. Dostupné z: https://www.ica.cz/kvalifikovany-certifikat-pro-epodpis

dokumentu. eDokumenty tak nabývají právní hodnoty a lze je stavět na stejnou úroveň jako analogové dokumenty.

Systém podepisování eDokumentů pomocí certifikátem zajištěného elektronického podpisu probíhá pomocí šifer asymetrické kryptografie, konkrétně podle šifrovacího algoritmu RSA[63]. Výhodou této šifry je, že v případě prolomení současné varianty RSA, lze jen navýšit počet bitů, a tak velmi zásadně zvýšit její důvěryhodnost.

Princip elektronického podpisu je takový, že nejprve je vytvořený dokument opatřen tzv. hashem (otiskem). Otisk zajišťuje neměnnost dokumentu, protože při změně daného dokumentu se vždy změní i jeho hash. Poté je takto připravený dokument zašifrován soukromým klíčem autora, tomuto se říká digitální podpis. Pro odšifrování elektronicky podepsaného dokumentu s otiskem se nejprve k dešifrování dokumentu použije veřejný klíč odesílatele dokumentu, který je volně dostupný a není nijak skrývaný.

Po dešifrování veřejným klíčem se ještě zkontroluje totožnost hashe s originálním hashem a pokud jsou oba totožné, tak je zajištěna neměnnost a původ elektronického dokumentu. Zásadní je v tomto případě důvěra třetí straně (certifikační autoritě), která musí být plně důvěryhodná, jelikož schraňuje informace o certifikátech každého vlastníka elektronického podpisu s certifikátem.

Soukromý klíč je uložen na fyzickém nosiči, kterým zpravidla bývá buď čipová karta nebo čip anebo nosič s USB portem označovaný jako USB Token. Tento Token je opatřen PINem, který je potřeba pro přístup na toto zařízení. Tyto fyzické nosiče jsou opatřeny dalším ochranným heslem a jejich nositel je povinen zabezpečit heslo před zneužitím. V případě nastalého bezpečnostního incidentu v podobě odcizení nosiče nebo jeho ztráty, musí vlastník neprodleně tento incident nahlásit zřizovateli, který provede zneplatnění certifikátu. Procesu zneplatnění

[63]Za pomocí hrubé síly, by bylo potřeba i pro moderní, velice výkonné počítače několik staletí k jejímu prolomení.

certifikátu a obou klíčů, jak veřejného, tak soukromého se říká revokace. eDokumenty podepsané odvolaným certifikátem se považují za nepodepsané[64]

3.2.7. Elektronické doporučené doručování

V oddílu 7 definuje eIDAS službu Elektronické doporučené doručování, která umožňuje odesílání a příjem dat mezi dvěma stranami s platnou právní hodnotou. Takováto data musejí mít zajištěnu svou integritu. Totožnost odesílatele a příjemce musí být známa, stejně jako datum a čas příjmu a odeslání dat. V Českém prostředí se využívá spíše systému Datových schránek, který slouží k elektronickému doručování dat také. Výhodou, kterou má tato služba oproti Datovým schránkám je potom fakt, že je využitelná napříč Evropskou Unií, kdežto Datové schránky jsou záležitostí pouze České republiky.

3.2.8. Autentizace webových stránek

EIDAS v krátkém oddílu 8 zavádí tzv. autentizaci webových stránek pomocí kvalifikovaných certifikátů. Oproti používání elektronických podpisů a jiných prvků eIDAS je toto založeno pouze na dobrovolné bázi, a tudíž se jedná spíše o nevyužívanou službu. Zde ovšem také naráží na problém s integrací do webových prohlížečů, kdy největší giganti jako jsou Google, Mozilla či Microsoft mají své vlastní seznamy certifikačních autorit s vlastními podmínkami pro vydávání certifikátů. Zde rozhoduje především cena a ta je u komerčních nabídek certifikačních autorit, nikoliv kvalifikovaných certifikačních autorit, zpravidla nižší. Určitou výhodou těchto certifikátů oproti ostatním je fakt, že jsou poskytovány kvalifikovanou certifikační autoritou, která má výslovný souhlas od Evropské Unie či její členské země.

[64]JIROTKA, Tomáš. Slovníček pojmů. *Digipodpis* [online]. [cit. 2018-07-23]. Dostupné z: http://www.digipodpis.cz/slovnicek.php

4. Český eGovernment

Ideou eGovernmentu je, že správa věcí veřejných by měla být díky IT prostředkům rychlejší, efektivnější, dostupnější a celkově přístupnější.[65]

Česká republika sice přijímá jednotlivá nařízení budující standard pro eGovernmenty po celé Evropě, ale zároveň zavádí své vlastní prvky českého eGovernmentu. Hlavním prvkem jsou potom tzv. ISVS – informační systémy veřejné správy. To jsou takové informační systémy, které slouží pro výkon veřejné správy dle zákona č.365/2000 Sb, který jej definuje jako „…*funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností.“*[66].

4.1. Portál veřejné správy

Jako vstupní bod pro jakéhokoliv občana do elektronické veřejné správy funguje Portál veřejné správy. Portál slouží jako informační servis týkající se jednotlivých prvků eGovernmentu a jako místo, které umožňuje občanovi přístup k jeho funkcím a zároveň shromažďuje ostatní prvky eGovernmentu. Jedná se především o tyto funkce či prvky typické pro jejich časté využití jako jsou datové schránky, eIdentita, eOP, výpis z rejstříku trestů apod.

Portál veřejné správy je rozdělen na 4 základní kategorie: občan, úředník, podnikatel a cizinec. Má jednoduché, přívětivé responzivní uživatelské rozhraní a podporu pro český a anglický jazyk.

Velkým kladem těchto webových stránek je to, že i když občan nevyužívá žádný prvek eGovernmentu (Datová schránka, eOP aj.), tak je web stále velmi užitečný v poskytování informačního servisu. Na jedné webové stránce je tedy

[65]Co je eGovernment?. *Ministerstvo vnitra České republiky* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

[66]Zákon č. 365/2000 Sb.: Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. *Zakonyprolidi.cz* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365

možné nalézt aktuální informace veřejné správy, včetně zákonů a různých formulářů.[67]

4.2. eJustice

eJustice funguje velmi obdobně jako Portál veřejné správy s tím rozdílem, že je zaměřen pouze na justici, která naopak není plně zahrnuta v Portálu veřejné správy. Poskytuje svým uživatelům vyčerpávající informační servis týkající se všeho spojeného s justicí v České republice. Lokace soudů, různé zákony, poradenství, hledání v různých rejstřících a mnoho dalšího.

Zatímco webové stránky jsou vcelku moderní, responzivní a jednoduché na navigaci, tak bohužel její jednotlivé prvky ještě neprošli modernizací. Například systém ePodatelny je viditelně zastaralý. Nepodporují mobilní zařízení, nejsou responzivní a nesplňují standardy kladené na moderní webové stránky.

Znovu platí, že stránky jsou velmi užitečné i občanům, kteří nevyužívají žádných prvků eGovernmentu, jelikož jejich informační servis je velmi rozsáhlý.

4.3. Základní registry

Základní registry veřejné správy jsou jedním ze základů českého eGovernmentu. Jejich cilem je zefektivnění využívání IT prostředků a zvýšení výkonnosti státní správy snížením byrokracie a zrychlením vyřizování žádostí ze strany občanů. [68]Jedná se o informační systém propojující jednotlivé registry, které udržuje aktuální a právně závazné.

[67]Portál veřejné správy. *Ministerstvo vnitra České republiky* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.mvcr.cz/clanek/portal-verejne-spravy.aspx

[68]Základní registry veřejné správy. *BusinessInfo.cz* [online]. 2016 [cit. 2019-04-20]. Dostupné z: https://www.businessinfo.cz/cs/clanky/zakladni-registry-verejne-spravy-ppbi-82624.html#!&chapter=1

Jednotlivé úřady mohou k těmto registrům přistupovat vzdáleně a nebudou si muset vést vlastní evidenci.

Základní registry jsou členěny na:

- Registr obyvatel,
- Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci,
- Registr územní identifikace, adres a nemovitostí,
- Registr agend orgánů veřejné moci a některých práv a povinností[69].

Jelikož se v registrech vyskytují citlivá osobní data, tak je přístup do nich výrazně omezen a každý jednotlivý přístup je zaznamenáván.[70] Nemělo by tedy dojít ke zneužití údajů v nich se nacházejících.

4.4. Datová schránka (ISDS)

Mezi základní prvky eGovernmentu České republiky patří datová schránka. Jedná se vlastně o síť datových úložišť[71], které umožňují oběh eDokumentů mezi jejími uživateli, což jsou jak státní instituce, tak soukromé právnické osoby, fyzické osoby podnikající či fyzické osoby.

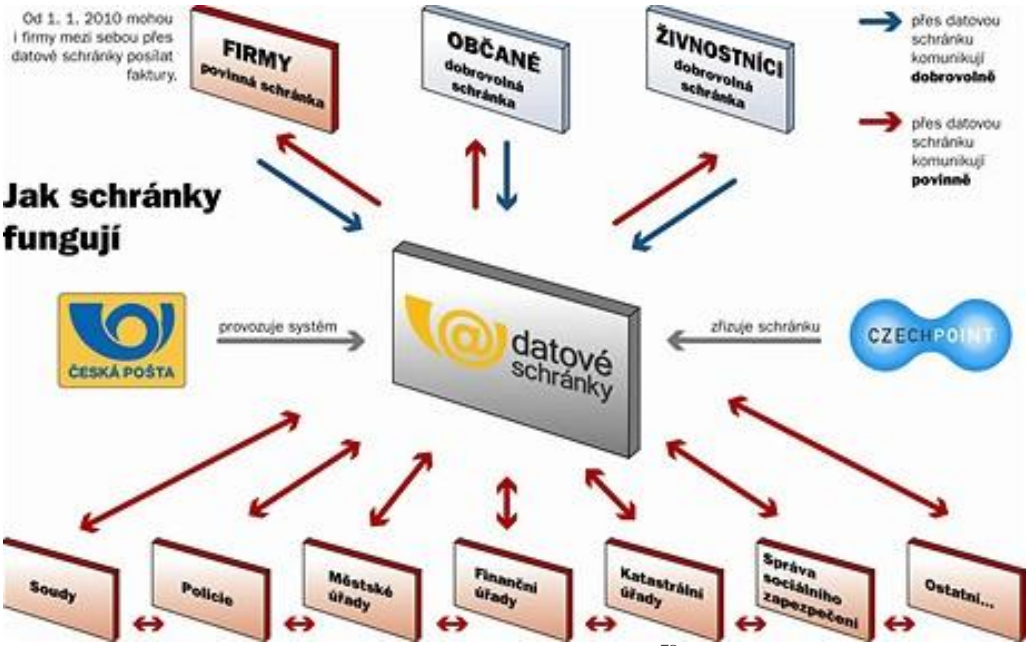
Každý občan má právo na zřízení Datové schránky, jejíž zřízení a provoz nemusí uživatel platit, zřízená datová schránka má potom neomezenou kapacitu a zavedenou maximální dobu po kterou všechny přijaté dokumenty ve schránce zůstanou 3 měsíců.

[69]Základní registry. *Management Mania* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://managementmania.com/cs/zakladni-registry

[70]Základní registry. Ministerstvo vnitra České republiky [online]. [cit. 2019-04-20]. Dostupné z: https://www.mvcr.cz/clanek/zakladni-registry-zakladni-registry.aspx

[71]Datové schránky jako součást eGovernmentu. *Datové schránky* [online]. [cit. 2019-04-19]. Dostupné z: https://www.datoveschranky.info/o-datovych-schrankach/datove-schranky-jako-soucast-egovernmentu

Hlavním cílem, při tvorbě tohoto komunikačního systému bylo urychlit komunikaci mezi jednotlivými státními institucemi a uživateli datových schránek.



Obr. 5 – princip fungování ISDS[72]

Dle obrázku prezentující schéma si schránku musí zřizovat pouze firmy a státní instituce. Státní instituce dále mají povinnost datové schránky využívat a s právnickými, fyzickými, fyzickými podnikajícími osobami mající datovou schránku, tak musí státní správa prostřednictvím této schránky komunikovat.

Naopak subjekty vlastnící datovou schránku mimo státní instituce nemusí v komunikaci až na výjimky (finanční správa) tuto datovou schránku využívat, ale zato mají povinnost svojí datovou schránku pravidelně kontrolovat z důvodu možného zaslání zpráv a dokumentů od státních institucí.

Mezi fyzickými osobami a fyzickými osobami podnikajícími je právě z důvodu výše uvedené povinnosti datová schránka nepříliš oblíbená a méně rozšířená, i když existuje aplikace Datovka, která spravuje dokumenty v datové schránce. Vypadá podobně jako email a její používání je dostatečně uživatelsky přívětivé. Umožňuje

[72]Datové schránky. In: *Město Broumov* [online]. [cit. 2018-07-23]. Dostupné z: http://m.broumov-mesto.cz/datove-schranky/d-2525

příjem zpráv, jejich čtení a odesílání.[73] O této aplikaci ovšem není dostatečné povědomí.

Naopak výhodou datových schránek je jejich neomezená kapacita, relativně dlouhá životnost přijatých dokumentů, až tří měsíce. Vlastník datové schránky si může dokumenty, které se v ní nachází uložit na vlastní média a eDokument, který je podepsán kvalifikovaným elektronickým podpisem i časovým razítkem tím neztrácí žádnou právní váhu. Na stanovištích CzechPOINT si také může nechat udělat převod z digitální do analogové podoby bez ztráty právní hodnoty dokumentu.

Veškeré eDokumenty podepsané kvalifikovaným elektronickým podpisem jsou v této datové schránce považovány za plnoprávné dokumenty. Datovou schránku je možné zřídit na Ministerstvu vnitra České republiky anebo na kontaktních místech tzv. CzechPOINTech.[74]

Po zřízení datové schránky je možné zažádat o konverzi jakýchkoliv dokumentů v ní se nacházejících. Touto konverzí daný konvertovaný dokument neztrácí žádnou právní účinnost. Konverze se provádí pouze z datové schránky do fyzické analogové podoby, obráceně, z fyzické do datové podoby lze dokument také převést, ale musí být opatřen jak kvalifikovaným elektronickým podpisem, tak časovým razítkem.

Datovou schránku si kdykoliv může nechat její uživatel zrušit či dočasně deaktivovat. Naopak mu také může být zrušena například při výkonu trestu nebo při ztrátě svéprávnosti.

[73]Mobilní aplikace. *Datovka* [online]. [cit. 2018-07-23]. Dostupné z: https://www.datovka.cz/cs/pages/mobilni-datovka.html

[74]Zákon č. 300/2008 Sb.: Zákon o elektronických úkonech a autorizované konverzi dokumentů. Zakonyprolidi.cz [online]. 2009 [cit. 2019-04-24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-300

4.5. CzechPOINT

CzechPOINT lze definovat jako síť kontaktních míst veřejné správy, na kterých mohou občané komunikovat se státní správou. Například podat žádost o výpis z různých rejstříků a registrů, nebo učinit podání vůči státní správě.[75]

Ministerstvo vnitra zřídilo Český Podací Ověřovací Informační Národní Portál označovaný pod zkratkou CzechPoint, aby vytvořilo komunikační systém napříč všemi sférami státu. Ze schématu datových schránek z předcházející kapitoly, je patrné, že CzechPoint[76] je zřizovatelem Datových schránek. CzechPoint tedy zaštiťuje službu Datové schránky, nestará se však o jejich provoz, ten byl svěřen České poště.

CzechPoint je základní stavební kámen českého eGovernmentu, cílem je zrychlení oběhu dokumentů mezi jednotlivými institucemi státní správy a samozřejmě i mezi subjekty, které mají povinně či dobrovolně zřízené datové schránky. Zároveň by měla být tato varianta, oproti běžnému oběhu analogových dokumentů, levnější a rychlejší v jejich zpracovávání a měla by přinést pohodlnější vyřizování dokumentů pro uživatele datových schránek.

Na stanovištích CzechPoint lze také vyřídit téměř všechny běžné záležitosti, které může každý občan využívat například výpisy z různých rejstříků (trestního, katastru nemovitostí a jiných), výpis bodů vlastníků řidičského oprávnění a jiných, zde je vhodné uvést, že o výpisy apod. může zažádat každý bez ohledu na to, zda vlastní datovou schránku.

4.6. ESSL Elektronický systém spisové služby

Jedná se o informační systémy sloužící pro správu a výkon spisové služby. V dnešní době je již drtivá většina dokumentů ve formě elektronické, a tudíž je tato

[75] Základní informace. *CzechPOINT* [online]. [cit. 2018-07-23]. Dostupné z: http://www.czechpoint.cz/public/kontaktni-misto/zakladni-informace-kmvs/

[76] Složenina anglických slov Czech Point (doslovně Český Bod) je podoba anglického slova Checkpoint, což znamená, volně přeloženo, kontrolní bod nebo kontrolní místo, což je vcelku přesné označení pro místa, tzv. CzechPOINTy (kontrolní body), které slouží jako místa pro zřízení datových schránek (často úřady měst, budovy České pošty aj.)

varianta skartačního řízení preferovaná. Skartační řízení se řídí podle metodického pokynu Národního digitálního archivu, a především poté dle Národního standardu pro elektronické spisové služby (NSESSS) a zákonem o archivnictví a spisové službě 499/2004 Sb.

K plnění tohoto standardu existuje Metodický návod pro kontrolu výkonu spisové služby vedené prostřednictvím elektronického systému spisové služby u veřejnoprávních původců[77], který by měl fungovat jako pomůcka pro korektní práci s elektronickou skartací. Je určen veřejnoprávním původcům, kteří si chtějí ověřit správnost jejich výkonu spisové služby[78].

Tyto legislativní opatření mají za cíl zajistit kompatibilitu mezi všemi prvky českého eGovernmentu a tím umožnit hladký oběh eDokumentů, kdy skartace je jeho poslední část před nástupem do digitálního archivu. Jako vlastně všechny další moderní legislativní opatření jsou i tato opatření zavedena s důrazem na kompatibilitu směrnic a nařízení plynoucí z Evropské Unie.

K efektivnímu provedení skartace eDokumentů se využívají sofistikované ESSL systémy. Tyto systémy mají potom zpravidla těsnou vazbu na státní službu Datových schránek a systémem Czechpointů.

ESSL systém vlastně umožňuje vzniku jedné konečné verze eDokumentu se všemi svými platnými metadaty a dalšími prvky (podpis, razítko aj. viz eIDAS výše). Umožňuje zároveň provozovat kontrolu nad eDokumenty a nabízí široké možnosti strukturalizace. Jedná se velmi sofistikovaný informační systém, který je „ušit na míru“ eDokumentům a jejich životním cyklům před tím, než se dostanou do digitálního archivu.

Dnes běžný ESSL informační systém nabízí integraci se systémem Datových schránek a umožňuje jak jejich příjem, tak také odesílání jejich obsahu. Další běžnou funkcí je zajištění správného chodu životního cyklu eDokumentu, tj. od jeho

[77]Dostupný z webových stránek Ministerstva Vnitra v sekci Spisová služba (http://www.mvcr.cz/clanek/spisova-sluzba-metodiky.aspx)

[78]*Ministerstvo Vnitra České republiky* [online]. Praha: Ministerstvo Vnitra, 2018 [cit. 2018-10-11]. Dostupné z: http://www.mvcr.cz/clanek/spisova-sluzba-metodiky.aspx

vzniku až po elektronické skartační řízení a přípravu vstupu do digitálního archivu. Mezi další funkce ESSL systémů může patřit také autorizovaná konverze, která umožňuje převod analogového dokumentu na dokument digitální (eDokument) se zachováním jeho právní hodnoty. Toto umožňuje úzká návaznost na Czechpoint, kde je tato konverze jeho základní součástí.

Důležitá je potom také ochrana eDokumentů a dohled nad jeho životním cyklem. Tuto ochranu eDokumentů nyní výrazně podpořily nově zavedené novelizace zákona o Kybernetické bezpečnosti, Malá novela Zákona o Kybernetické bezpečnosti a Velká novela Zákona o Kybernetické bezpečnosti.

4.6.1. EDMS Systém správy elektronických záznamů

Systém správy elektronických záznamů, z anglického Electronic Document Management System, jak už z názvu vyplívá, je program, který slouží ke správě elektronických záznamů. Pod správou si lze představit vytváření, ukládání a kontrolování elektronických záznamů.[79] Často bývá velmi úzce integrován se systémem Elektronické správy spisové služby.

Zásadní je v tomto případě pojem záznam. V českém prostředí je anglický pojem Document chápán jako záznam, nikoliv jako dokument, jak je chápán například z pohledu zákona č. 499/2004 Sb.. EDMS tedy nespravuje dokumenty, ale pouze vede záznamy. Záznam lze potom definovat jako informace, která nespadá pod definici dokumentu, nebyla tedy zatříděna, evidována a uzavřena proti změnám.[80]. Pro zjednodušení terminologie byl anglický pojem pro Elektronickou správu spisové služby ERMS nahrazen ryze českým pojmem ESSL[81] ve 4 znění Národního standardu elektronického systému spisové služby (NSESSS).

---

[79]EDMS - Electronic Document Management System. *EDMS* [online]. 2014 [cit. 2019-04-20]. Dostupné z: http://www.edms.net/

[80]KUNT, Miroslav. Novela národního standardu pro elektronické systémy spisové služby. *ISSS* [online]. 2017 [cit. 2019-04-20]. Dostupné z: https://www.isss.cz/archiv/2017/download/prezentace/na_kunt.pdf

[81]Návrh čtvrtého znění NSESSS. *CNZ.cz* [online]. 2017 [cit. 2019-04-20]. Dostupné z: http://www.cnz.cz/odborne-aktivity/pracovni-skupina-nsesss/aktualni-zneni-nsesss/ctvrte-zneni-nsesss/

4.7. Informační systémy ESSL ve státní sféře

Každý ESSL se samozřejmě liší, ale jejich základní funkce zůstávají stejné, požadavky kladené na tyto systémy jsou totiž takřka totožné, největším rozdílem je potom celková rozsáhlost systému a samozřejmě finanční náklady a poskytované záruky. Před samotným srovnáním potom ještě je potřeba podotknout, že většina firem poskytujících ESSL zároveň nabízí další prvky eGovernmentu, jako například časová razítka, pečetě aj. a tyto produkty mohou nabízet ve specializovaných balíčcích, které jsou cenově výhodnější nežli produkty zakoupené zvlášť. V dalších kapitolách je popisováno několik nejrelevantnějších ESSL.

4.7.1. Gordic Ginis

Gordic Ginis je nejrozšířenějším ESSL ve státním sektoru. Mezi jeho největší zákazníky se řadí Ministerstvo obrany, Ministerstvo vnitra, Ministerstvo práce a sociálních věcí, Ministerstvo průmyslu a obchodu, Ministerstvo zdravotnictví, Ministerstvo kultury a další, velmi rozsáhlé a významné státní instituce.

Obr. 6 – Počet zakázek Gordic od r. 2009[82]

Gordic poskytuje v ČR asi nejkomplexnější řešení pro elektronickou spisovou službu ve státní sféře. Sám sebe označuje Gordic svůj ESSL Ginis jako 100 % bezpečný, lehce integrovatelný s možností snadného začlenění dalších aplikací do svého systému a také stále aktuální s nynějšími informačními technologiemi.

[82]Gordic spol. s.r.o.: TOP 10 ZADAVATELŮ. *VsechnyZakazky.cz* [online]. Praha, 2018 [cit. 2018-10-13]. Dostupné z: https://www.vsechnyzakazky.cz/supplier/detail/396115/GORDIC-spol-s-ro

Při přečtení takového popisu není těžké uhodnout, proč je tento systém tolik rozšířený mezi českými institucemi, integrace s aplikacemi třetí strany je nutná k provázání s Datovými schránkami a Czechpointy. Samozřejmě pyšnit se 100 % bezpečností svého systému je přestřelené, nic jako 100 % bezpečný systém neexistuje a jedná se tedy spíše o nějaký druh marketingu.

Nedostatkem je potom ne úplně přehledné uživatelské rozhraní, zastaralé i vzhledově, které zajisté úředníkům, kteří nejsou zdatní v ovládání počítače, může dělat potíže. Mezi další nedostatek se může řadit fakt, že GINIS není kompatibilní s databázovými servery MySQL, klienta lze použít jen na platformě operačních systémů Windows, nikoliv na linuxových distribucích.

Naopak mezi výhody tohoto systému můžeme započítat jeho modulárnost; Produkt si může zákazník nastavit do velké míry podle sebe[83] a nemusí kupovat zbytečně něco navíc či být o něco ochuzen.

Výše zmíněné uživatelské rozhraní může zároveň být i výhodou; potřebný výpočetní výkon je na moderní standardy velmi nízký. Pro referenci jsou v manuálu uvedeny minimální požadavky (Procesor: Intel Pentium[84] 4 o 2Ghz, Operační paměť: 2 GB, Prostor na pevném disku: 10 GB, zobrazovací zařízení s rozlišením minimálně 1024x768, operační systém: Windows 7 a vyšší.) na úrovni osobních počítačů starých více než 10 let.

Gordic nabízí komplexní řešení nejen pro spisovou službu a skartaci, ale také další, pro státní správu důležitá, softwarová řešení, je velmi vhodný pro větší firmy/státní instituce, svou funkci splňuje vcelku dobře. Důvodem, proč je GINIS využíván ve velkých společnostech/státních institucích je fakt, že dobře funguje se svými dalšími moduly, přímo nesouvisejícími se spisovou službou, a tak si je velké korporace či státní instituce kupují dohromady, aby zajistili co nejplynulejší chod.

[83]Platforma GINIS. *Gordic* [online]. [cit. 2019-04-29]. Dostupné z: https://www.gordic.cz/produkty/ginis/

[84]Například tento procesor Intel Pentium 4 vyšel už před 18 lety v roce 2000. De facto všechny dnešní nové procesory osobních počítačů, které si lze koupit jsou výkonnější než tento zmíněný.

Navíc zajišťování kompatibility mezi konkurenčními produkty je vždy nesnadné, buď vůbec není možné, nebo funguje jen do určité míry a poté se musejí hledat kompromisy, což může přinášet další potíže.

4.7.2. Software 602 ESSL

Software 602 je v porovnání s Gordicem relativně méně rozšířeným řešením eSSL. Mezi jeho klientelu patří například Státní ústav pro kontrolu léčiv, Český úřad pro zkoušení zbraní, Psychiatrická nemocnice Bohnice, Geodetická kancelář GEOMAP a CzechPOINT. Jelikož jeho systémy jsou v mnohem menším měřítku v porovnání s GINISem, tak Software 602 nachází zákazníky i v soukromé sféře. Přeci jen v České republice není tolik dostatečně velkých korporací na úrovni státu, že by nutně potřebovali systémy GINIS.

Toto ovšem neznamená, že Software 602 nějak zaostává za konkurencí. Oproti GINISu je Software 602 novějším systémem, a tudíž jak dnešní trendy nařizují také mnohem více uživatelsky přívětivější. Stejně jako GINIS jej lze plně integrovat s Datovou schránkou a Czechpointem.

Cílenou skupinou Software 602 jsou středně velké firmy/státní instituce a pro ně představuje dobré řešení spisové služby, které má přívětivé prostředí a všechny funkce, které pro práci ve spisové službě může její uživatel potřebovat. Mezi jeho další funkce patří například možnost pracovat na daném eDokumentu na více pracovních stanicích souběžně a zároveň umožňuje dobrou kontrolu nad prováděnou prací na eDokumentu. Další výhodou tohoto systému je fakt, že k němu lze přistupovat libovolně, nikoliv pouze jen z pracoviště. Má vlastní cloudové prostředky[85]. Software 602 nabízí také ne úplně standardní podporu biometrického podpisu.

Mezi jeho menší nevýhodu můžeme zařadit například nedostatečnou dokumentaci dostupnou online (oproti GINISu, který má manuál volně dostupný

[85]Spisová služba, archivace, skartace: Dlouhodobá archivace a skartace. Software 602 [online]. [cit. 2019-01-11]. Dostupné z: https://www.602.cz/reseni/spisova-sluzba-archivace-skartace/

na svých webových stránkách). Toto může ovšem být jen nevýhoda pro veřejnost, při koupi produktu může být tato dokumentace zákazníkovi zveřejněna.

Software 602 se řadí mezi přední ESSL systémy používané v ČR, svým přívětivým prostředím a libovolným přístupem značně usnadňuje práci daného uživatele, zároveň ale má všechny funkce, které od ESSL očekáváme. Dokáže plnit veškeré potřebné úkony.

4.7.3. SoftHouse EZOP

Tak jako je Software 602 zaměřen na středně velké společnosti a státní instituce, tak je EZOP zaměřen na menší státní instituce a firmy. Cenově vcelku přívětivý informační systém, který však svými funkcemi a podporou zaostává za výše zmíněnými systémy.

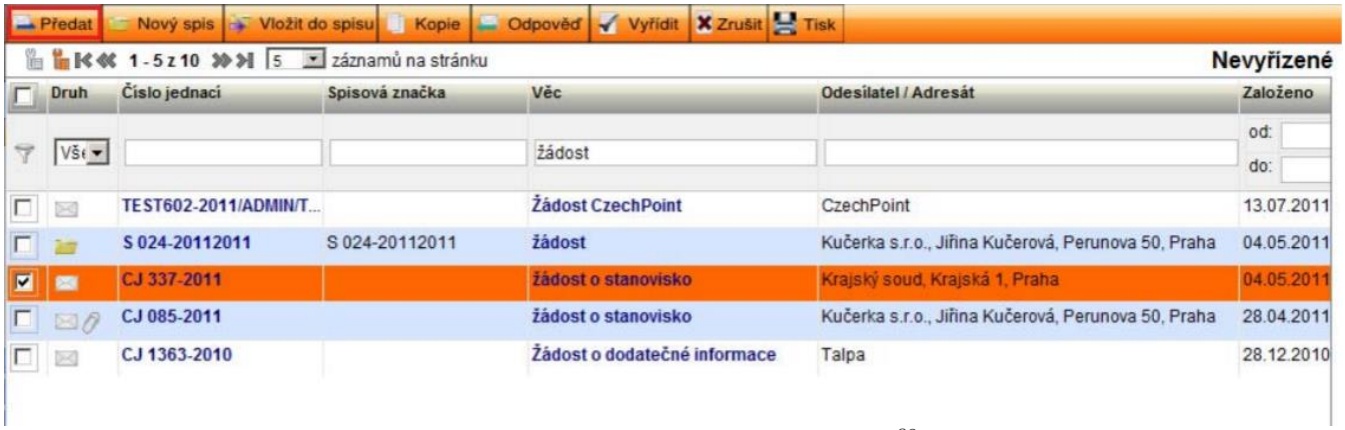
Zde by platilo tvrzení, že cena odpovídá kvalitě. EZOP je z dnešního pohledu nepřehledný, zastaralý (především vzhledově; jeho uživatelé mohou mít problémy s jeho navigací). Je především vhodný pro základní funkce spisové služby, avšak v něm nelze nalézt pokročilé způsoby filtrování, podporu Datových Schránek a dalších, především tzv. „quality of life“ funkcí. Samozřejmě umožňuje kompletní práci s životním cyklem eDokumentu.

Využívá externí úložiště v podobě MS SharePoint; předávat část svých funkcí na třetí stranu je vždy velmi složité a může být i nebezpečné; daná služba může kdykoliv ukončit činnost, a proto by se musela okamžitě hledat alternativa, to může způsobit zbytečné starosti. Webové stránky SoftHouse jsou také velmi nepřehledné a nedopovídají dnešnímu standardu, a navíc na nich nejsou nikde k dispozici žádné dokumentace či manuály k danému systému.

Další nevýhodou EZOPu je jeho neflexibilnost; daný eDokument je přístupný pouze danému uživateli, který na něm pracoval a administrátorovi. Nelze počítat s prací více uživatelů na stejném eDokumentu nebo například na úřední desce EZOPu nelze měnit vyvěšené eDokumenty, toto spojené s nepřívětivým uživatelským prostředím pravděpodobně spoustě úředníkům spíše práci prodlužuje a neusnadňuje ji.

4.7.4. ICZ e-spis Lite

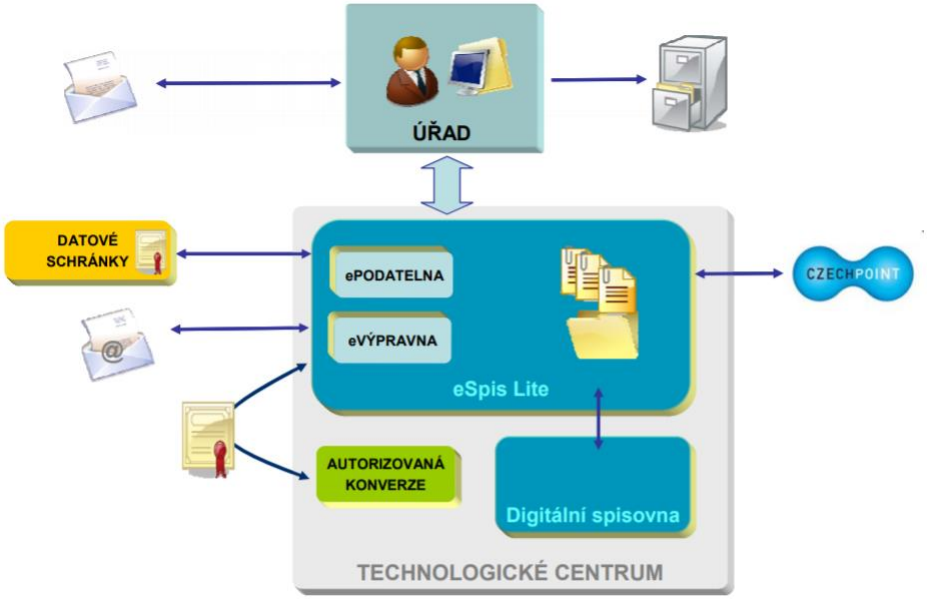
Systém e-Spisová služba (zkráceně e-spis) Lite je rozsahem nejméně rozsáhlá aplikace pro elektronickou spisovou službu. Hned na začátek je potřeba zmínit, že vývojář e-spisové služby ICZ poskytuje k tomuto produktu rozsáhlý informační servis skládající se ze 141stránkové uživatelské příručky přesně popisující všechny jeho funkce, samotné uživatelské prostředí, fungování programu a logikou za danými funkcemi, 2 informačních několikastránkových dokumentů a několika webových článků na svém webu. V porovnání s EZOPem si může jeho uživatel nastudovat všechno sám a v případě potřeby si doplnit znalosti o systému ze zmíněné příručky. Ze všech ESSL poskytuje, kupodivu, největší informační servis uživateli právě tento systém společně s GINISem (který je cenově naprosto někde jinde).



Obr. 7 – uživatelské prostředí ESSL espis Lite[86]

Uživatelské prostředí samotného klienta je standardní, pro běžného uživatele nemusí být úplně přehledné a jednoduché na navigaci, ale s dostupnou dokumentací, si lze vždy nalézt odpověď. Ztrácet se v něm uživatelé pravděpodobně budou jen v počátcích, i když rozhraní není nijak vzhledově povedené, tak tento program není natolik složitý.

[86] *Hostovaná elektronická spisová služba* [online]. 2018 [cit. 2018-10-13]. Dostupné z: https://www.kraj-jihocesky.cz/tck/espis/files/e-learning/2_6_0_UzivatelskaDokumentace_spslite.pdf



Obr. 8 – schéma ESSL eSpis Lite[87]

Z obrázku prezentující schéma eSpisové služby Lite je patrná další výhoda tohoto systému a tou je jeho kompatibilita s Datovými schránkami a CzechPoint.

Nadstandardní funkcí je potom autorizovaná konverze, kdy je možný autorizovaný převod analogového dokumentu na eDokument se všemi svými vlastnostmi. Tento program má navíc integrovaný konvertor mezi různými formáty textových procesorů do souborového formátu PDF (ve svých archivačních variantách).

Klient je zároveň nenáročný na výpočetní výkon, takže dobře zapadá do nepříliš výkonných počítačů malých obcí, muzeí a dalších institucí, na které se soustředí.[88]

4.7.5. M.I.T ESSL

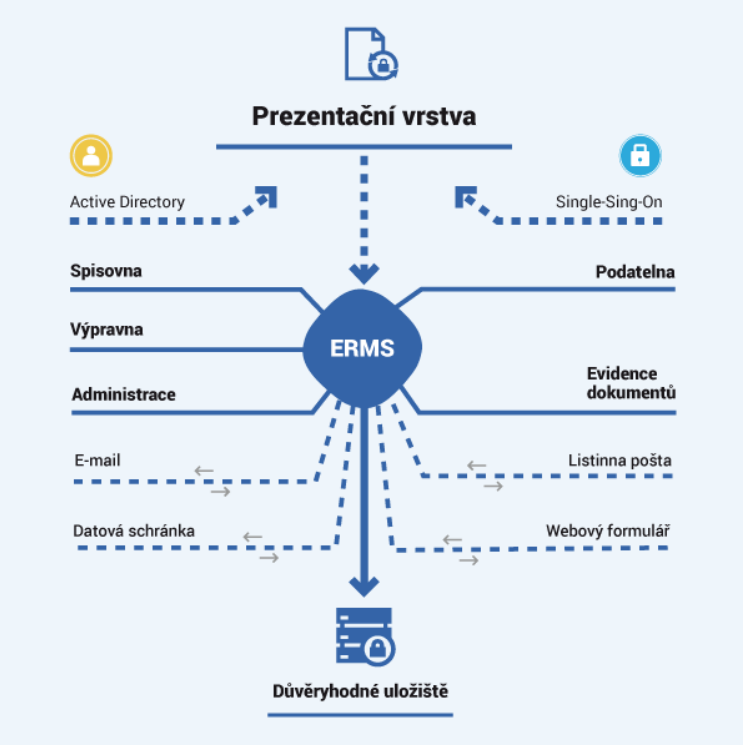
M.I.T Consulting je společností zabývající se systémy pro elektronickou státní správu. Vyvíjí a poskytuje elektronický informační systém spisové služby dotovaný

[87]ICZ e-spis® LITE: Produktový list. *ICZ* [online]. Praha, 2018 [cit. 2018-10-13]. Dostupné z: https://www.iczgroup.com/wp-content/uploads/2017/08/PL_e-spis-LITE.pdf

[88]ICZ e-spis® LITE: Produktový list. *ICZ* [online]. Praha, 2018 [cit. 2018-10-13]. Dostupné z: https://www.iczgroup.com/wp-content/uploads/2017/08/PL_e-spis-LITE.pdf

Evropskou Unií, zabývá se kybernetickou bezpečností, GDPR, EIDAS a další legislativou s nimi související.[89] Všechny tyto položky jsou v dnešní době velmi žádoucí.

Samotný ESSL je potom například oproti systému e-Spis Lite propracovanějším a modernějším systémem. Podporuje Datové schránky a Czechpoint, plně umožňuje řídit průběh spisové služby, navíc potom poskytuje vlastní důvěryhodné úložiště, které chrání daný eDokument před odcizením či jinou neoprávněnou manipulací, využívá pravidelné automatické zálohování, sledování historie práce s eDokumentem, a tak by se nemělo stát, že by daný eDokument byl odstraněn bez toho, aniž by o tom byl někde záznam.



Obr. 9 – schéma ESSL M.I.T[90]

[89]ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA. *M.I.T Consulting* [online]. [cit. 2019-04-29]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

[90] ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA: HLAVNÍ RYSY ŘEŠENÍ. *M.I.T Consulting* [online]. [cit. 2018-11-10]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

Z daného obrázku prezentujícího schéma lze vyčíst, že ESSL poskytuje všechny standardní funkce elektronického systému pro spisovou službu (práce se spisy, propojení s Datovou Schránkou, evidencí dokumentů, vytváření skartačních návrhů, elektronická pošta, propojování spisů s eDokumenty aj.)

Zajímavé je potom jejich vlastní důvěryhodné úložiště zvané TDPS, které umožňuje až střednědobou archivaci eDokumentů. Navíc potom umožňuje uchovávat „*…i papírové dokumenty převedené do elektronické podoby (např. formou scanu – obrázku) nebo i jakékoliv multimediální soubory.“*[91]. Toto může být považováno za solidní výhodu, avšak je je potřeba počítat s tím, že takovéto úložiště nedosahuje kvalit úložišť v digitálním archivu.

Výhodou tohoto řešení se zdá být především zkušenost jejich autorů s kybernetickou bezpečností a právní legislativou dotýkající se eDokumentů a práci s nimi.

Dle vlastních slov je jejich systém elektronické spisové služby určen jak veřejnoprávním, tak soukromým subjektům, které zpracovávají a evidují větší množství dokumentů[92]. Pod pojmem „větší množství dokumentů“ si lze jen těžko představit, o jak velké množství se jedná.

Po prozkoumání veřejně dostupného seznamu klientů[93] M.I.Tu lze konstatovat, že je tento produkt určen spíše pro velké soukromé společnosti či státní organizace nebo jiné instituce, které zpracovávají opravdu velké množství dokumentů. Rozhodně se nejedná o systém pro například městské úřady, soudy aj. Spíše o státní instituce na úrovni ministerstva. Oběh dokumentů musí být v této instituci značný.

[91]ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA: DŮVĚRYHODNÉ ÚLOŽIŠTĚ. *M.I.T Consulting* [online]. [cit. 2018-11-10]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

[92]ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA: KOMU JE APLIKACE ERMS URČENA? *M.I.T Consulting* [online]. [cit. 2018-11-10]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

[93]Mezi zákazníky M.I.T patří například O2 Czech republic, IBM, Česká republika, České Dráhy a její informační systémy, ČD Cargo, Česká pojišťovna.

5. General Data Protection Regulation

Po dlouhé době ale přece přichází Obecní nařízení o ochraně osobních údajů. Zkráceně GDPR z anglického General Data Protection Regulation, je největší „strašák“ pro všechny firmy pracující nějakým způsobem s osobními údaji. Jedná se o nové legislativní opatření ošetřující ochranu osobních údajů občanů členských zemí Evropské Unie.

V České republice nahrazuje směrnici 95/46/ES a související zákon č. 101/2000 Sb. Jak zmíněný zákon, tak směrnice jsou výrazně zastaralé, obzvláště poté z pohledu dnes výrazně se vyvíjejících informačních technologií[94].

GDPR, oproti dřívější legislativě[95] hledí na osobní údaje jako na důležitou komoditu, která v dnešním světě masivních Big Data analýz a metodách Data miningu má opravdovou hodnotu nejen pro soukromí sektor, ale i pro stát samotný.

5.1. Osobní údaje

Samotný pojem osobní údaje GDPR značně rozšiřuje o nové položky a definuje je jako „*..veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě.“*[96] Mezi základní osobní údaje jako je jméno, příjmení, adresa, věk, pohlaví a osobní stav na které byla minulá legislativa již dlouhou dobu zvyklá, zařazuje GDPR navíc nové elektronické údaje jako je IP adresa, fotografii, e-mailová adresa, telefonní číslo, cookies soubory a další údaje (například na občanském průkaze nebo řidičském oprávnění).

Dále je potřeba zmínit také ty osobní údaje, které přináší nové možnosti z hlediska bezpečnosti jak kybernetické (biometrické údaje -> otisk prstů, sítnice oka aj.), tak bezpečnosti fyzického světa (záznamy o trestní činnosti). Velmi citlivé jsou potom údaje typu náboženského vyznání a rasových informací, které jsou

[94]Směrnice byla vydána roku 1995 a zákon roku 2000.

[95]V kompletním znění GDPR je vyjmenováno 173 důvodů pro jeho vstoupení v platnost.

[96]Co považuje GDPR za osobní údaje. *GDPR: Obecné nařízení o ochraně osobních údajů* [online]. Praha, 2017 [cit. 2018-07-25]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

z hlediska bezpečnosti velmi významné s ohledem na současnou politickou a bezpečnostní situaci v Evropských zemích a ve světě. (Válka proti teroru[97] pokračuje od 11. září 2001 doposud). Další osobní údaje, které jistě stojí za zmínku jsou údaje o sexuální orientaci a politické příslušnosti, které mohou být také velmi citlivé. V posledním desetiletí se výrazně zvýšila jejich důležitost jak v politickém, tak běžném životě lidí, kdy roste důležitost tzv. Politické korektnosti.

Toto samozřejmě není kompletní výčet, ale poskytuje alespoň základní přehled. Obecně lze říci, že se GDPR snaží cílit zavádění nových osobních údajů na takové osobní údaje, které mají reálnou obchodní hodnotu pro veřejný i státní sektor (především pro jejich marketingové využití).

5.2. Ochrana osobních údajů

S GDPR je zavedeno mnoho nových systémů prevence a ochrany osobních údajů. Stejně jako směrnice NIS pro kybernetickou bezpečnost se i GDPR zakládá na co nejvyšší úrovni transparentnosti, rychlosti oznamování incidentů a jejich co možná nejrychlejšímu řešení.

5.2.1. Zabezpečení manipulace osobních údajů

Prvním novým prvkem, který GDPR přináší je tzv. pseudonymizace, což je způsob zpracování osobních údajů tak, aby nebylo možné k nim přiřadit identitu jedince[98]. Toho je zpravidla docíleno přiřazením ID k dané osobě, kdy je tato informace samozřejmě zašifrována. Každý daný jedinec má tedy vlastní alias (ID) pod kterým je jeho identita skryta, ale s jeho osobními údaji se dá stále pracovat. Každý osobní údaj musí být samozřejmě sám šifrován, není možné, aby byl v prostředí jak internetu, tak intranetů tak extranetů přenášen nešifrován.

[97] Anglicky War on Terror, kdy jako casus belli posloužil teroristický útok na Světové obchodní centrum v USA.

[98] Pseudonymizace osobních údajů. *GDPR: Obecné nařízení o ochraně osobních údajů: prakticky* [online]. [cit. 2019-04-20]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/

Dalším novým bezpečnostním prvkem je zavedení vlastního kodexu[99] chování pro zpracovatele osobních údajů. Tento kodex má pomoci v utajení osobních údajů před veřejností ale na určité úrovni i před některými zaměstnanci jako takovými. Samozřejmě uvnitř instituce je nemožné tyto věci udržet, a tudíž se jedná spíše o formální záležitost. Jedná se o jeden z hlavních důvodů, proč je GDPR vnímáno veřejností spíše negativně.

Zpracovatel údajů musí také zajistit neustálou důvěrnost, integritu a dostupnost zpracovaných osobních údajů. Důležité z této definice je fakt že se klade důvěrnost, integrita a dostupnost na stejnou úroveň a teoreticky by na ně měl být dbán stejný důraz. Samozřejmě v reálném životě je mnohem důležitější samotná důvěrnost a integrita osobních údajů a na jejich dostupnost se neklade až takový důraz.

V případě možné technické závady či fyzického incidentu (pod tím si můžeme představit cokoliv – výpadek proudu, záplavy, silné sněžení aj.) má také zpracovatel povinnost být schopen obnovit dostupnost osobních údajů. V přímé definici z GDPR není ovšem uveden žádná doba, do kdy tak musí učinit. Trochu zarážející je, že zde chybí také část definice „obnovit, jak nejdříve to bude možné“, která je v mnoha dalších případech přítomná.

5.2.2. Hlášení bezpečnostních incidentů

Pokud už k nějakému incidentu dojde, tak první věc, na kterou GDPR hledí je rychlost nahlášení tohoto incidentu a poskytnutí co možná nejhlubšího informačního servisu o daném problému. Konkrétně potom je nutné ohlásit tuto skutečnost ÚOOÚ do tří dnů[100]. Zároveň je ale uvedeno, že zpracovatel musí

[99]Z běžného života lze například odpozorovat u lékařů, kdy by Vás neměl oslovovat jménem natož přiřazovat k některému vyšetření aj. Jedná se pravděpodobně o jednu z nejméně oblíbených věcí, které přímo dopadají na běžný život občana.

[100]Incidenty, Úniky dat: Hlášení incidentů. *Národní platforma pro GDPR* [online]. [cit. 2019-04-20]. Dostupné z: http://www.gdpr-platforma.cz/index.php/gdpr/hlaseni-incidentu

incident nahlásit bez zbytečného odkladu a ihned potom, co si všimne[101], že problém nastal.

V případě bezpečnostního incidentu má také zpracovatel povinnost informovat osoby, kterýchž osobní údaje byly zkompromitovány. V tomto případě už ale neexistuje žádná definice, která by zavedla nějaký časový limit do kdy tak musí být učiněno. Trochu úsměvná je potom samotná definice, která říká, že subjekt musí být informován za použití jasných a jednoduchých jazykových prostředků.

5.2.3. Pověřenec pro ochranu osobních údajů

Naprosto nová pozice, kterou GDPR zavádí je pověřenec pro ochranu osobních údajů (DPO – data protection officer). „*Hlavním úkolem ... bude monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat.“*[102]

Tohoto pracovníka nemusí mít ale každá společnost či instituce pracující s osobními údaji. Musí jej však mít všechny instituce veřejné moci a společnosti, které už ze své podstaty pracují s velkým množstvím osobních údajů a provádějí jejich systematické monitorování.

Důležitá je také nezávislost tohoto pracovníka; není možné, aby byl ve střetu zájmů a jeho úsudek byl ovlivněn něčím nebo někým ve svém pracovním prostředí. Proto je v GDPR přesně uvedeno, že pověřenec sice může plnit další povinnosti v dané společnosti či instituci, ty ale nesmí vést ke střetu zájmů. Pověřenec také nenese žádnou zodpovědnost na plnění GDPR v dané organizaci.[103] Má značnou

[101]Toto je velký problém u spousty velkých incidentů, kdy si jejich zpracovatel velmi často „nevšimne“, že k nějakému bezpečnostnímu incidentu vůbec došlo a ohlásí jej po delší době, než by bylo vhodné. Další vyšetřování je potom zdlouhavé a nemusí přinést žádné výsledky.

[102]DPO čili Pověřenec pro ochranu osobních údajů. *GDPR Obecné nařízení o ochraně osobních údajů prakticky* [online]. 2016 [cit. 2019-02-11]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/

[103]DPO čili Pověřenec pro ochranu osobních údajů. *GDPR Obecné nařízení o ochraně osobních údajů prakticky* [online]. 2016 [cit. 2019-02-11]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/

úroveň nezávislosti – je odpovědný pouze správci či zpracovateli a nejvyšším představeným. Od nich ale nepřijímá žádné pokyny a za svou činnost nesmí být sankcionován anebo propuštěn. Jeho propuštění či případná sankce musí být řádně vysvětleny a odůvodněny. Samotná práce pověřence jej může velmi snadno přivést do střetu zájmů se svými nadřízenými. Tato část je velmi problematická, DPO by se teoreticky neměl v žádném případě bát o svou pozici, ale zároveň lze k propuštění zaměstnance nalézt vždy nějaký důvod (ať už může tento důvod být jakkoliv nepřímý). Dokud je DPO přímým zaměstnancem dané firmy, tak tuto skutečnost nelze ničím vyloučit.

Možným řešením by bylo mít tuto pozici podřízenou pouze dozorovému úřadu a do institucí, kde musí být je dosazovat, takže by nebyli nijak podřízení daným zpracovatelům ale pouze úřadu jako takovému. Na druhou stranu toto řešení přináší značnou finanční zátěž pro úřad, který by potřeboval navýšit finanční prostředky z rozpočtu. Dalším problémem tohoto řešení je jeho přijetí. Určitě by existovala myšlenka státního dohlížitele, která by mohla být vnímána spíše negativně.

5.3. Práva subjektů

GDPR zavádí několik nových práv, které by měli umožnit občanům jak větší kontrolu nad svými osobními údaji a jejich zpracováním, tak také zvýšit hladinu informovanosti o svých osobních údajích. Tato práva tvoří základ pro model ochrany osobních údajů.[104]

5.3.1. Právo na přístup

Prvním z nich je právo na přístup, které říká, že každý občan má právo na to, být informován o nakládání zpracovávaných osobních informací. „*Přístupem k osobním údajům se rozumí oprávnění subjektu údajů na základě jeho aktivní*

[104]6. Práva subjektu údajů. *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

žádosti získat od správce informaci (potvrzení).“[105] Základní informace, které si může každý subjekt zpracovávaných osobních údajů běžně vyžádat jsou:

- charakteristika zpracovávaných osobních údajů,
- Time to live zpracovávaných osobních údajů,
- Účel zpracovávání osobních údajů,
- Přístup k osobním údajům,
- Způsob zpracovávání osobních údajů.

O toto zpravidla (V 99 % případů se jejich zpracovatel nebude sám pokoušet občanovi cokoliv sdělit, pokud přímo nemusí.) musí zpracovatele požádat subjekt těchto osobních údajů, na což mu potom zpracovatel musí „co nejdříve“ informace poskytnout. Naštěstí je toto omezeno maximální lhůtou jednoho měsíce (v reálném světě to přesně tak dlouho samozřejmě také trvá).

Měsíc je velmi dlouhá doba pro poskytnutí těchto údajů. Možným řešením, jak dostat tyto informace subjektům osobních údajů je zavést instancování, které zavede přesné kategorie, kdy pro poskytnutí menšího objemu informací o osobních údajích jejich vlastníkovi je potřeba méně času a opačně.

5.3.2. Právo na přenositelnost údajů

Právo doplňující původní právo na přístup. Říká, že zpracovatel osobních údajů musí být schopen subjektu, kterému jsou osobní údaje zpracovávané poskytnout tyto údaje v podobě strukturovaného dokumentu čitelného strojově. Toto právo je zavedeno především z důvodů strojově zpracovávaných osobních údajů, které nejsou pro lidi čitelné (nebo jen velmi složitě).

[105]GDPR stručně: O ochraně osobních údajů stručně a jasně. *Úřad pro ochranu osobních údajů: The office for personal data protection* [online]. [cit. 2019-02-07]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

Proto je v právní definici uvedeno slovo strukturované. Automatizované systémy vůbec například vůbec nepočítají s mezerami[106], které také, i když velmi drobně, zpomalují jejich automatickou četbu.

5.3.3. Právo nebýt předmětem automatizovaného individuálního rozhodování, včetně profilování

Toto právo navazuje na právo na přenositelnost údajů. Dává tak právo subjektům, jejichž osobní údaje jsou zpracovávány automatizovaně, nebýt předmětem tohoto automatizovaného zpracování.[107] S tímto právem je spojeno také mnoho výjimek. Pokud subjekt výslovně souhlasí s automatizovaným zpracováním, tak toto neplatí. (Souhlasy na webových stránkách). Toto právo se také neaplikuje, pokud mezi subjektem a druhou stranou dochází ke vzniku smlouvy. (Například e-shopy).

5.3.4. Právo na opravu

Přímo navazující na právo na přístup je právo na opravu (a doplnění), které jak z názvu vyplývá umožňuje subjektu osobních údajů informovat zpracovatele o chybnosti daného údaje. Možná kontrola pravosti osobních údajů je z důvodu jejich obrovského datového množství asi nemožná nebo jednoduše příliš nevýhodná, a tak je spíše na jejich vlastnících, zda si je dají do pořádku či nikoliv.

Za zmínku stojí fakt, že zpracovatel osobních údajů má povinnost po nahlášení tyto osobní údaje opravit „Bez zbytečného odkladu“ (Pod čímž si lze představit různě dlouhou dobu, většinou by ale zpracovatelé byli sami proti sobě). Naopak subjekt osobních údajů nemá vlastně žádnou povinnost tyto opravy hlásit. Samozřejmě že u základních údajů typu jméno, bydliště, telefonní číslo, email aj. lze počítat s tím, že si je vlastníci těchto údajů nechají u zpracovatelů opravit, zvlášť

[106]S další strukturou, kterou tvoří například odstavce a nadpisy už vůbec nepočítají. Pro strojovou četbu jsou to pouze další zbytečné údaje, s kterými by museli počítat.

[107]6. Práva subjektu údajů. *Úřad pro ochranu osobních údajů* [online]. 2017 [cit. 2019-04-29]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

pokud jde například o jejich zaměstnání, pojišťovnu, banku anebo jiné, pro občany důležité instituce. Naopak u dalších údajů, které se přímo netýkají subjektu osobních údajů nelze počítat s tím, že by si kterýkoliv občan nechával opravovat jiné údaje, které nejsou pro jeho život či finance důležité.

Přemýšlet se potom dá také o pravosti nahlášených opravených údajů, které se určitě velmi těžce ověřují, jestli vůbec, což může být pravděpodobně problematické.

5.3.5. Právo na námitku

Další je právo na námitku, kdy každý občan, pokud si myslí, že se s jeho osobními údaji nakládá neoprávněně, může podat námitku na zpracování osobních údajů a žádat i výmaz[108].

Toto právo je velmi důležité z hlediska ochrany osobních údajů. Velkým problémem je ale prostá neznalost občanů, kteří o těchto právech nejsou nijak informováni. Musí si tedy informace dohledat sami. Tím pádem je tato možnost používaná jen (v porovnání s celkovým počtem subjektů, kterým jsou zpracovávána osobní údaje) mizivým počtem osob, které jsou technicky zdatnější a mají ponětí o existenci ochrany osobních údajů a jejích prostředcích.

Důležité je v tomto případě rozlišovat námitku na zpracování osobních údajů z pohledu státní sféry a z pohledu soukromých institucí, firem a dalších.

Námitka na zpracování osobních údajů se netýká takových osobních údajů, které jsou důležité z hlediska veřejného života a bezpečnosti státu (V původním legislativním dokumentu GDPR je vyjmenován celý seznam[109] důvodů, proč může stát tuto námitku jasně zamítnout). Zajímavé je, že se toto nevztahuje jen na samotný členský stát, ale také na „zájem Unie“, ať si pod tím můžeme představovat

[108] 6. Práva subjektu údajů. *Úřad pro ochranu osobních údajů* [online]. 2017 [cit. 2019-04-29]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

[109] Stojí za to vypíchnout některé body, které nejsou až tak jasné a s kterými by se dalo dále pracovat: 1) inspekční a monitorovací funkce veřejné moci, 2) vymáhání občanskoprávních nároků, 3) jiné důležité cíle veřejného zájmu Unie nebo členského státu, zejména hospodářský či finanční zájem a sociální zabezpečení.

cokoliv. Z této krátké poučky lze tedy vyvodit, že stát si může s našimi osobními údaji dělat cokoliv co je pro něj kvalifikováno jako důležité.

Z tohoto pohledu tedy proti státu a jejím institucím není zdaleka tak efektivní jako proti soukromým zpracovatelům osobních informací, na které jednoduše platí více. Toto je jedna z věcí, které by bylo vhodné ošetřit v možné novější legislativě.

Samozřejmě je toto z hlediska bezpečnosti státu pravděpodobně dobrý krok, který zvyšuje míru monitorování a tím pádem možné prevenci před narušením bezpečnosti. Zároveň se ale může jednat o velmi kontroverzní záležitost, kdy zvyšující se dohled na svým obyvatelstvem a shromažďováním více a více informací o nich není zdaleka tak jednoznačné z hlediska morálního.

5.3.6. Právo na výmaz

V legislativě označované taky jako právo na zapomnění. Umožňuje subjektu vyžádat si u zpracovatele osobních údajů o jejich kompletní vymazání. Subjekt je tedy „zapomenut“, což znamená, že o něm neexistuje žádná zmínka a není možné danou osobu přiřadit k jakýmkoliv datům zbylým po výmazu.

Samozřejmě existuje řada podmínek pro to, aby si mohl občan zažádat o tento výmaz. Není možné jej tedy teoreticky nijak zneužít a může být použito pouze za daných podmínek. „*Nelze … žádat likvidaci všech osobních údajů např. při ukončení zaměstnání či poskytování finančních služeb, jelikož na správce se vztahují povinnosti o dalším uchování některých osobních údajů.*“[110]

V GDPR se tyto podmínky stanovují tak, že k výmazu musí být vždy splněna alespoň jedna z uvedených jinak výmaz není možný. Nejdůležitější z daných podmínek jsou odvolání souhlasu[111] subjektu o zpracování osobních údajů, vznesení námitky na zpracování osobních údajů (předchozí kapitola), osobní údaje

[110]6.Práva subjektu údajů: Co znamená právo být zapomenut?. *Úřad pro ochranu osobních údajů: The office for personal data protection* [online]. Praha, 2018 [cit. 2019-02-08]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

[111]S tímto souvisí i dopad GDPR na běžný život občana, kdy se na libovolných webových stránkách jejich autoři snaží o získání souhlasu o zpracování osobních údajů různými pop up boxy, nebo přímým zablokováním obsahu, dokud není souhlas udělen.

ztrácí svůj účel pro zpracovatele a naposledy že osobní údaje byly zpracovány neoprávněně.

Samozřejmě existuje řada výjimek, které jdou mimo tyto podmínky, a i přes to, že byly splněny neuplatňují právo na výmaz. Z pohledu archivu a jiných institucí, archivu nejbližších, je velmi důležitá výjimka bodu 3 písmena f článku 17, která říká, že pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely není výmaz možný i přes splnění jedné z uvedených podmínek.

V kontrastu předcházející kapitoly, kdy si stát činí určité rezervy sám pro sebe je v této kapitole uvedena jedna velmi důležitá výjimka, která říká, že výmaz nemůže proběhnout, pokud narušuje výkon práva na svobodu projevu a informace.

Další výjimky by se dali shrnout do několika slov. Výmaz se neuplatňuje, pokud jsou daná osobní data veřejně prospěšná (například z pohledu sociálního, zdravotního, bezpečnostního a jiného) anebo jsou užitečná z pohledu právního (soudnictví, armádní či policejní vyšetřování a jiné).

5.3.7. Právo na omezení zpracování

Stejně jako má subjekt právo na výmaz osobních údajů u zpracovatele, tak má právo na omezení zpracování daných osobních údajů. Znovu je zde uvedeno několik podmínek, za kterých lze toto privilegium uplatnit. Nejsou ovšem zdaleka tak tvrdé jako u předchozího.

Subjekt může o toto právo požádat, pokud si myslí, že dané v daných osobních údajích existují nepřesnosti. V tomto případě platí omezení zpracování, dokud si nedokáže zpracovatel ověřit pravost těchto údajů.

Subjekt může požádat o omezení zpracování, pokud je samotné zpracování protiprávní, ale subjekt nechce požádat o výmaz. Věří tedy že brzy dojde k nápravě situace, ale nechce, aby musel všechny osobní údaje znovu poskytovat. Toto je pravděpodobně rychlejší proces, než kdyby byly všechny údaje vymazány a poté znovu zavedeny. Jedná se tedy o méně extrémní řešení než úplný výmaz, ale za po odstranění daného problému může být efektivnější.

Pokud subjekt podal námitku na zpracování, tak by mělo automaticky dojít k omezení zpracování do té doby, než bude námitka vyřešena.

Zpracovatel osobních údajů již tyto údaje nepotřebuje, ale stále jsou potřeba z důvodu obhajoby právních nároků (soudy, důkazní materiál pro policii, armádu, různé úřady, školy a další).

Důležitý je potom také bod, který říká, že pokud je omezení povoleno, tak musí zpracovatel vždy po subjektu žádat souhlas s dalším zpracováním.

5.4. Povinnosti zpracovatelů osobních údajů

GDPR říká, že zpracovatelé osobních údajů (firmy, státní instituce, korporace aj.) musejí „*zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR.*“[112]

Nad tím, zda daná instituce splňuje tyto podmínky dohlíží Úřad pro ochranu osobních údajů, jehož hlavním prostředkem je posuzování vlivu na ochranu osobních údajů (DPIA)[113], které tomuto úřadu poskytují dané firmy anebo pověřenci, a kontrola záznamů o zpracovávání osobních údajů poskytovanými jejich zpracovateli. Obě tyto povinnosti, jak vypracovávat DPIA, tak vést záznamy o zpracovávání osobních údajů umožňují snazší kontrolu úřadu nad zpracovateli osobních údajů. (A také jim přidávají značně na vnitřní byrokracii v podobě administrace). Kontrola osobních údajů, i díky povinnosti oznamovat narušení bezpečnosti či kompromitace osobních dat, je tudíž na mnohem vyšší úrovni než před aplikací GDPR.

5.5. Úřad pro ochranu osobních údajů

Tento úřad s dozorčí funkcí na ochranu osobních údajů vznikl již v roce 2000, kdy byl do právního řádu zanesen původní zákon č. 101/2000 Sb. o ochraně

[112]Co je GDPR?. *KYBEZ* [online]. 2018 [cit. 2018-07-28]. Dostupné z: https://www.kybez.cz/gdpr

[113]General Data Protection Regulation (GDPR). *EARCHIVACE.CZ* [online]. [cit. 2019-04-29]. Dostupné z: http://www.earchivace.cz/clanky/general-data-protection-regulation-gdpr/

osobních údajů[114]. Úřad podle zákona má jako hlavní funkci stanovenou funkci dozorčího[115]. Dbá tedy na to, aby byl dodržován zákon o ochraně osobních údajů.

S příchodem GDPR tomuto úřadu značně narostli pravomoci a povinnosti. Podstata tohoto úřadu zůstává ale tatáž a jádro věci se nijak nemění, stále tento úřad působí jako dozor nad dodržováním ochrany osobních údajů, nyní ve formě GDPR.

U nařízení EU lze vysledovat určitý trend, kterým je snaha provázat spolupráci[116] mezi členskými zeměmi. To platí samozřejmě i pro tento úřad, který má povinnost spolupráce[117] s dalšími dozorovými úřady členských zemí.

Pojem dozorový úřad zavádí až GDPR, které říká že v každé členské zemi musí být alespoň jeden nezávislý dozorový úřad, který má jak funkci monitorovací, tak hlavně kontrolní, dále pak funkci osvětovou a vymáhací (vymáhá plnění GDPR). U nás je jím právě Úřad pro ochranu osobních údajů, který k převzetí všech povinností měl v ČR nejlepší předpoklady. Tento úřad nabývá s GDPR také velmi silné nezávislé pozice, kdy nemá žádného přímého nadřízeného a funguje zcela samostatně (se samostatným rozpočtem).

Osvětová funkce je samozřejmě velmi důležitá, znovu ovšem ale platí pravidlo, že pokud se o dané téma člověk nezajímá sám od sebe, tak se příliš mnoho věcí nedozví. Webové stránky úřadu poskytují jejich uživateli solidní informační servis o GDPR a úřadu jako takovém. Úřad má dále potom vlastní semináře a poskytuje poradenství ohledně GDPR buď skrze písemnou formu nebo i vlastní telefonní

---

[114]Úřad pro ochranu osobních údajů. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2019-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/%C3%9A%C5%99ad_pro_ochranu_osobn%C3%ADch_%C3%BAdaj%C5%AF

[115]V tomto ohledu lze nalézt určitou podobnost s NÚKIBem, s tím rozdílem že jeho pole působnosti není kybernetická bezpečnost ale ochrana osobních údajů (což spolu samozřejmě úzce souvisí)

[116]Zákon o kybernetické bezpečnosti je aplikací dalšího nařízení EU, které se také snaží o provázání a spolupráci mezi členskými zeměmi.

[117]EU také zakládá tzv. Evropský sbor pro ochranu osobních údajů, který je tvořen vybranými členy dozorčích úřadů všech členských zemí. Mezi hlavní činnosti tohoto sboru patří formování ochrany osobních údajů v členských zemí, dozorčí a poradenská funkce.

linku. „*Telefonní číslo GDPR linky je k dispozici pro rychlé konzultace k obecnému nařízení (GDPR). Linka je určena občanům, subjektům údajů, pověřencům či menším správcům a zpracovatelům.“*[118]

5.6. Přínosy GDPR

Veřejností je Obecné nařízení o ochraně osobních údajů vnímáno spíše negativně. Většinou se vyzdvihují milionové pokuty či zpomalení byrokracie anebo drobné nedostatky typu přímého oslovování osob. GDPR samozřejmě není dokonalé, ale jedná se o dobrý krok kupředu k ochraně osobních údajů, která každým rokem nabývá na důležitosti. Informační technologie jdou stále rychleji dopředu, metody k zpracování osobních údajů jsou stále sofistikovanější a není možné, aby se stát zasekl na místě a pořád dále používal tutéž legislativu reagující na svět, který tu už dávno není.

Největším přínosem GDPR pro běžného občana je možnost rozhodovat o svých osobních údajích v online světě. (viz. kapitola práva subjektu). Před aplikací GDPR se běžného uživatele na internetu nikdo neptal, zda může použít jeho informace k dalším svým účelům. Nikdo mu nedal vědět, když došlo k jejich kompromitaci. Nikdy neměl možnost zažádat o vymazání všech jeho osobních údajů. Tyto údaje de facto vlastnili dané společnosti a není třeba dodávat, že z nich profitují. Toto všechno může občan udělat naprosto zadarmo (v zákoně č. 101/2000 Sb. je toto zpoplatněno tak, aby si občan sám pokryl náklady za zpřístupnění těchto informací).

Dalším přínosem GDPR běžnému občanovi je, že mu dává přehled. Občan si může zažádat o výše zmíněné věci, a hlavně dostane vědět, když byly jeho osobní údaje zkompromitovány. V uvozovkách zářným příkladem je aféra společnosti T-mobile z roku 2016, kdy došlo k zcizení osobních údajů (jméno, telefonní číslo, bydliště, číslo bankovního účtu aj.) 1,2 milionu zákazníků, kteří o tom nebyli nijak informováni. T-mobile byl pokutován 3,6 miliony, což je ohledem k situaci velmi

[118]GDPR telefonní linka. *Úřad pro ochranu osobních údajů* [online]. Praha, 2016 [cit. 2019-02-10]. Dostupné z: https://www.uoou.cz/gdpr-telefonni-linka/ds-5287/archiv=0&p1=1059

nízká částka. „*Za obří únik dat, k němuž došlo letos v dubnu, dostala společnost T-Mobile vysokou pokutu. Úřad pro ochranu osobních údajů rozhodl, že operátor dostatečně nezabezpečil data svých klientů a má za to zaplatit pokutu ve výši 3,6 milionu korun.“*[119] Samozřejmě v případě GDPR by k tomu samému mohlo také dojít; občan by byl ale alespoň informován o dané situaci a společnosti by byla udělena mnohem vyšší pokuta.

[119]T-Mobile dostal pokutu za obří únik dat o klientech. Utekly adresy nebo výše plateb. *Aktuálně.cz* [online]. 2016 [cit. 2019-02-11]. Dostupné z: https://zpravy.aktualne.cz/ekonomika/t-mobile-dostal-pokutu-za-obri-unik-nezabezpecil-data-uvedl/r~0dc2bc1c63c011e6bc7c0025900fea04/?redirected=1549900938

6. Zákon o kybernetické bezpečnosti

Každým rokem se informační a komunikační technologie posouvají dále a dále a dostávají se do běžného života více a více lidí. S tímto rozmachem ICT roste zároveň riziko jejich zneužití, na což reaguje právě Velká a Malá novela zákona o kybernetické bezpečnosti. Právě zákony zabývající se oblastmi informačních a komunikačních technologií jsou (nebo by alespoň měli být) jedny z nejčastěji novelizovanými zákony, jelikož musí stále reagovat na rychle se rozvíjející ICT. Jsou velmi nestálé, a z právního hlediska, mnohdy velmi složité na zavedení a zpracování.

Právě na tuto skutečnost reaguje stát zavedením dvou novel zákona o kybernetické bezpečnosti tzv. Malou novelou Zákona o kybernetické bezpečnosti a Velkou novelou Zákona o kybernetické bezpečnosti.

6.1. Malá novela Zákona o kybernetické bezpečnosti

Malá novela Zákona o kybernetické bezpečnosti upravuje zákon č. 181/2014 Sb. zákonem č. 104/2017 Sb.[120] Vstoupila v platnost 1. 7. 2017 a má 7. základních bodů (proto Malá novela Zákona o kybernetické bezpečnosti).

Zavádí pojem provozovatel a upravuje stávající pojetí správce. Provozovatelem se rozumí firma, která zajišťuje běh ICT prostředků (například dodavatel) a správcem se rozumí ten, kdož tyto prostředky využívá a pracuje s nimi. Provozovateli tedy přidává tato novela na povinnostech a činí jej více zodpovědným za svůj produkt.

Zároveň je potom upraven vztah mezi provozovatelem a správcem, kdy je provozovatel povinen v případě, že skončí s provozem daného ICT systému bezpečně zničit všechna sesbíraná a provozní data získaná během provozu daného systému a je povinen zbavit se i vlastních kopií či záloh těchto dat. Ve výsledku by

[120]Malá novela Zákona o kybernetické bezpečnosti. *CZ.NIC* [online]. 2017 [cit. 2019-04-20]. Dostupné z: https://www.csirt.cz/page/3581/mala-novela-zakona-o-kyberneticke-bezpecnosti/

provozovateli daného informačního a komunikačního systému neměla zůstat žádná data sesbíraná během jeho provozu.

Další povinností provozovatele je tyto nashromážděná data odevzdat správci, pokud o to požádá. Pokud je některá z těchto podmínek nedodržena, hrozí provozovateli různě odměřené pokuty až do 1 000 000 Kč.

Další, pro kybernetickou bezpečnost velmi zásadní, změnou je povinnost provozovatele neprodleně informovat Národní úřad pro kybernetickou a informační bezpečnost o jakémkoliv bezpečnostním narušení či nové bezpečnostní hrozbě[121]. Tato změna je velmi zásadní z toho důvodu, že před aplikováním této novely nebyla povinnost neprodleně informovat o bezpečnostních hrozbách či narušeních, a tak se o nich vědělo mnohdy až s příliš dlouhým časovým odstupem. Velmi důležité je z právního hlediska slovíčko neprodleně (v samotném zákoně se uvádí fráze „bez zbytečných odkladů“). Před aplikací tohoto zákona sice tato povinnost také byla aplikována, avšak bez nutnosti informovat o daném bezpečnostním incidentu neprodleně. V této části je do zákona zavedena ještě další, menší změna a to ta, že provozovateli ukládá povinnost informovat neprodleně o bezpečnostní hrozbě i Správce. Provozovatel má dále povinnost NÚKIB hlásit seznamy kontaktních údajů.

V případě, že daný ICT systém není provozovatelem dostatečně ochráněn, má Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) možnost nařídit provozovateli přesun dat daného systému na jeho úložiště a vymazání všech dalších kopií a záloh. V případě porušení tohoto nařízení mu může být uložena pokuta do výše 1 000 000 Kč.

Méně důležitým je potom bod, který říká, že provozovatel má půl roku čas na to, aby své produkty a jejich správu zařídil tak, aby splňoval podmínky dané Zákonem č. 104/2017 Sb. Tomuto bodu se říká přechodné období. V době psaní této práce již dávno půl rok od započetí fungování této novely uběhl.

[121]Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Zákony pro lidi.cz* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Posledním bodem Malé novely Zákona o kybernetické bezpečnosti je zvýšení částek pro pokuty, které jsou nyní mnohem přísnější než před aplikací této novely. Například *„V § 25 odst. 3 písm. a) se částka „100000 Kč“ nahrazuje částkou „1000000 Kč““*[122].

6.2. Velká novela Zákona o kybernetické bezpečnosti

Vydaná o měsíc později po Malé novele Zákona o kybernetické bezpečnosti, tato Velká novela má za cíl především přenést do českého prostředí směrnici Evropské Unie NIS, kdy tato směrnice zavádí nová bezpečnostní pravidla a pravidla pro hlášení bezpečnostních incidentů a (jako všechna nařízení z Evropské Unie) se snaží o prohloubení mezinárodní spolupráce, především mezi jednotlivými členskými zeměmi v oblasti kybernetické bezpečnosti. Tato směrnice (značená 2016/1148) je v českém prostředí zaváděna pomocí zákona č. 205/2017 Sb.[123]

6.2.1. Národní úřad pro kybernetickou bezpečnost (NÚKIB)

Směrnice NIS dává daným členským státům Evropské Unie povinnost zřídit státní orgán, který by měl spravovat a zajišťovat kybernetickou bezpečnost pro daný stát. Proto byl v České republice vyčleněn z Národního bezpečnostního úřadu nový úřad sídlící v Brně – Národní úřad pro kybernetickou bezpečnost (NÚKIB).

„Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů“[124]

[122]Zákon č. 104/2017 Sb. *Zákony pro Lidi.cz* [online]. [cit. 2018-07-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104#cast2

[123]Zákon o kybernetické bezpečnosti a jeho aktuální novelizace. *Epravo.cz* [online]. [cit. 2019-04-20]. Dostupné z: https://www.epravo.cz/top/clanky/zakon-o-kyberneticke-bezpecnosti-a-jeho-aktualni-novelizace-106268.html

[124]CO JE NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB* [online]. Brno, 2017 [cit. 2018-07-26]. Dostupné z: https://www.govcert.cz/

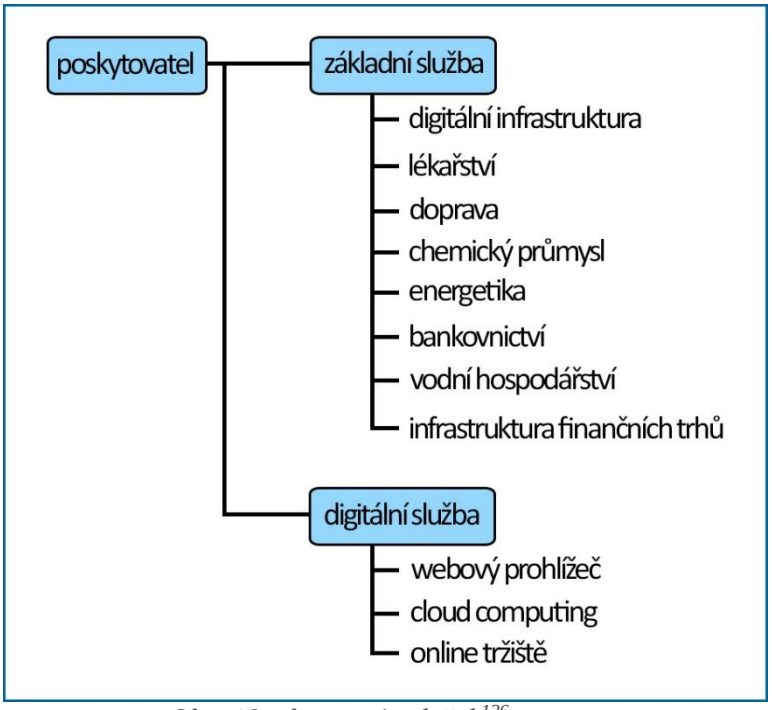
Tento úřad zastává právě daný orgán spravující kybernetickou ochranu země. Mezi jeho hlavní povinnosti patří kontrola, kdy je úřad povinen kontrolovat plnění zákona o kybernetické bezpečnosti. Kontrola probíhá pouze, pokud existuje podezření na porušení některých ze zákona daných povinností provozovatelů informačních a komunikačních systémů, nebo v případě podezření na jejich bezpečnostní narušení.

Mezi jeho další povinnosti patří vývoj nových technologií a systémů pro zajištění kybernetické bezpečnosti a také zajišťuje vzdělávání a školení v této oblasti (například pomocí dvou modulového e-learning kurzu aj.). Informační servis na jeho webových stránkách je velmi rozsáhlý, poskytuje také jednodušší popisy a vysvětlivky různých zákonů a jejich právnických definic, které nemusí být běžnému občanovi zcela jasně srozumitelné.

Další funkcí úřadu je zajištění ochrany utajovaných informací. Tato funkce je samozřejmě velmi těžce popsatelná, jelikož k ní nemá veřejnost příliš mnoho dostupných informací, což je vcelku logické z podstaty své věci. Důležitá je potom také funkce osvětová, kdy má úřad za úkol vnášet povědomí o kybernetické bezpečnosti mezi co nejširší vrstvu obyvatelstva.

6.2.2. Obsah Velké novely Zákona o kybernetické bezpečnosti

Z právního hlediska Velká novela Zákona o kybernetické bezpečnosti přináší nové pojmy – Základní službu a digitální službu. Základní služba je taková služba, která je provozně závislá na ICT systému a zároveň spadá pod jednu z kategorií vypsaných ve schématu.[125] Digitální služba je potom taková služba, která má ryze elektronický charakter (například služby cloudu, pošty, internetový vyhledávač aj.).



Obr. 10 – kategorie služeb[126]

Zavádí také tzv. informační povinnost, která říká, že úřad musí být vždy neprodleně informován o jakémkoliv bezpečnostním incidentu v případě porušení pravidel stanovenými touto novelou. Tato povinnost platí pro jak poskytovatele základní, tak digitální služby. K odeslání slouží univerzální formulář dostupný na stránkách Národního úřadu pro kybernetickou a informační bezpečnost.[127]

---

[125] Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Zákony pro lidi.cz* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[126] Zdroj: vlastní tvorba

[127] https://www.govcert.cz/

Tato novela nařizuje poskytovatelům digitálních i základních služeb zavádění tzv. ochranných a reaktivních opatření v případě bezpečnostního incidentu. Poskytovatel základní služby má po bezpečnostním incidentu nahlášeném na úřadě povinnost zavést nová bezpečnostní opatření, která mu Národní úřad pro kybernetickou bezpečnost udělí.

Dále novela ošetřuje také zveřejňování informací týkajících se daných základních či digitálních služeb. Zadává poskytovatelům a správcům povinnost zajistit si takovou vnitřní politiku, která zajišťuje bezpečnost informací, týkajících se dané služby. Přístup k informacím, kritickým pro bezpečnost dané služby je omezen a není volně přístupný.

Celkově si nelze než nepovšimnout, že nařízení z Evropské Unie GDPR a NIS (ve formě ZKB) mají společný trend především incidenty co nejrychleji identifikovat a pokud se tak neděje, tak je subjekt těžce pokutován. Zvyšují tak transparentnost subjektů.

7. Srovnání ZKB před a po novelizaci

Původní zákon o kybernetické bezpečnosti vydaný v roce 2014 označen jako zákon č. 181/2014 Sb. byl změněn nově vydaným zákonem č. 205/2017 Sb. a zákonem č. 104/2017 Sb. Tyto dva zákony upravující starší zákon z r. 2014 si kladou za cíl zefektivnit rychlost odhalování možných bezpečnostních incidentů a ty potom rychle řešit.

Rozdíl mezi vydáním zákonů činí 3 roky, což v prostoru rychle se rozvíjejících informačních technologií je velmi dlouhá doba a je třeba na tyto nové skutečnosti reagovat.

Na následujících řádcích je provedeno konkrétní srovnání jednotlivých bodů zmíněných zákonů. Autor v této části probere jednotlivé změny zákona řádek po řádku paragraf po paragrafu.

Komparace bude provedena mezi zněním zákona č. 181/2014 Sb. ve své původní platnosti 29. 8. 2014 (dále jako původní znění) a zákonem č. 205/2017 Sb. z léta 2017 (dále jako novém znění). Zákon č. 104/2017 Sb. je věnována samostatná kapitola, protože nepřináší tolik změn. Pokud je nějaký paragraf vynechán, znamená to, že v něm nedošlo k žádným relevantním změnám. Irelevantní změny jsou vynechány (například nahrazení čárky spojkou a).

7.1. Předmět úpravy § I

Paragraf I. definuje předmět úpravy zákona. Nově se od původního znění odlišuje tím, že zákon upravuje také příslušné předpisy Evropské Unie členským státům o kybernetické bezpečnosti.

Důvodem této úpravy je především fakt, že v novém znění zákona se zavádí směrnice NIS Evropské Unie, takže manipulace s dosavadním zněním v tomto ohledu je naprosto pochopitelná. V novém znění zákona se totiž upravuje stará směrnice, která se nahrazuje NISem. Více o ní v předchozích kapitolách a níže v patřičném paragrafu.

7.2. Definice pojmů § II, § III

Tato část zákona vymezuje pojmy použité v celém zákoně, zavádí některé nové a upravuje stávající. Velmi důležitá část, zpřesňuje definice různých pojmů. V novém znění zároveň dochází k jejímu zásadnímu rozšíření z původních 7 bodů na 13.

7.2.1. Bezpečnost informace

Důležitou změnou je v tomto paragrafu rozšíření definice bezpečnosti informaci. V původním znění se bezpečnosti informací rozumí zajištění její důvěrnosti, integrity a dostupnosti informací.

Nově jsou k tomuto bodu připojeny mezi výčet také data. V původním znění tedy nedocházelo k rozlišování mezi pojmem data a informace. Jak informace, tak data jsou přitom nejzákladnější pojmy informačních technologií ve všech jejích odvětvích (především potom z pohledu databází). Data lze přitom definovat jako zdroj a informaci jako poznatek, získaný z tohoto zdroje. Informace je tedy interpretace poznatků dat.

V novém znění zákona musí být tedy zabezpečené jak informace, tak data, z kterých tyto informace pocházejí. Toto ovšem neznamená, že v původním znění nebyla data vůbec nijak chráněna; znamená to ale, že jejich právní definice nebyla úplně jasná. Tato nová definice je z právního hlediska přesnější.

Pokud tedy novou definici „přeložíme“ do běžné mluvy, tak říká: Bezpečností informací se myslí zajistit jejich neměnnost (integritu), důvěryhodnost, její původní zdroj a další informace[128] o ní vypovídajících.

7.2.2. Významný informační systém

Další změnou v tomto paragrafu je úprava definice významného informačního systému. V původním znění je totiž významný informační systém definován jako

[128] Toto je i v novém znění docela problematická část definice, především z důvodu své nepřesnosti. Není totiž jasně specifikováno, co je a co není tato informace.

takový informační systém, který je spravován orgánem veřejné moci, který ale nesmí být kritickou informační infrastrukturou.

Nově se tato definice rozšiřuje a říká, že významný informační systém také nesmí být informačním systémem základní služby. Touto změnou je z definice vyloučen informační systém základní služby, který definují následující body tohoto paragrafu.

7.2.3. Základní a digitální služba

Tento velmi důležitý bod konečně kategorizuje[129] všechny, jak soukromé, tak veřejné, subjekty, které působí v kyberprostoru. V původním znění tato kategorizace neexistuje a ke všem se přistupuje naprosto totožně. (Více o základní a digitální službě v kapitole Zákon o kybernetické bezpečnosti.)

Velkým přínosem tohoto dodatku je jeho individuálnost. Nejen že přerozděluje subjekty do těchto 2 služeb, ale také je zařazuje do svých kategorií, které mají své specifická pravidla a ustanovení.

Například základní služba spadající do kategorie digitální infrastruktury má nově ze zákona mnohem více povinností, které musí splnit, aby byla v kyberprostoru považována za zabezpečenou. V původním znění se nečinil mezi službami žádný rozdíl, a tak měli všichni totožné povinnosti uložené zákonem.

Dále potom nově definuje, kdo smí a nesmí být provozovatelem dané instituce poskytující digitální nebo základní službu. Nejdůležitější je potom následující bod, který říká, že vybraná osoba (PO / FO) má informační povinnost vůči úřadu pro kybernetickou bezpečnost (který nové znění také ustanovuje).

Nic z tohoto vlastně v původním znění neexistovalo, a tak byl přístup úřadů k této problematice spíše individuální a záleželo na vlastním výkladu zákona a toleranci každého úředníka, což pouze působí zmatek.

[129]Vybrané kategorie nejsou úplně šťastně navržené. Vědecké instituce, které sice lze rozdělit mezi nabízený výběr, by si už jen z hlediska své velikosti a důležitosti zasloužili vlastní kategorii. Další institucí, která, dle autorova názoru, nemá úplně jasnou kategorii jsou například knihovny a archivy, které nakládají s informacemi. I když tyto instituce lze zařadit do některé z kategorií, tak by si zcela určitě zasloužili vlastní individuální kategorizaci.

7.2.4. Zástupce poskytovatele digitální služby

Dále je potom v paragrafu 3 zakotveno, že poskytovatel digitální služby, který nemá sídlo v členských zemích EU, musí stanovit svého zástupce, který má totožnou informační povinnost vůči úřadu kybernetické bezpečnosti.

Tento zástupce musí být ustanoven v České republice, nikoliv v jakékoliv členské zemi EU. V praxi to potom znamená, že pro uvedeného zástupce poskytovatele digitální služby platí stejné zákony jako v jeho sídle. Pokud sídlí v České republice, tak pro něj platí tento zákon, pokud v některé další členské zemi, tak pro něj platí zákony té dané země. Možná by stálo za to, aby poskytovatel digitální služby sídlící v některé členské zemi EU musel mít svého zástupce i v České republice, pokud v ní působí.

Problémem je totiž rychlost integrace směrnice NIS v členských zemích EU. Pokud by měl totiž poskytovatel služby sídlo v zemi, kde zatím NIS není implementována, tak by se měla řídit podle dosavadního znění zákona, ve kterých ve většině případů vůbec neexistují tyto pojmy. Řešení potencionálních bezpečnostních incidentů by potom bylo velmi složité. Velká část členských zemí EU je buď ve fázi implementace NISu (Portugalsko, Polsko, Nizozemsko, Litva, Itálie a další), nebo s implementací ještě vůbec nezačala (Například Španělsko, Řecko, Chorvatsko). Tato implementace bude trvat ještě pravděpodobně několik let, což je příliš dlouhé okno pro potencionální problémy. Nedávno skončila oficiální doba na implementaci, a tak je jistě odpověď v nedohlednu.

„Členské země budou od uveřejnění v Úředním věstníku Evropské Unie (srpen 2016) mít 21 měsíců na začlenění požadavků do svých legislativ, …“[130]

Řešením by bylo zanést do právního řádu povinnost mít svého zástupce přímo v České republice. Tím pádem by se musel daný poskytovatel řídit našimi zákony a situace by byla jasná.

[130]ŠULC, Roman. EVROPSKÁ UNIE PŘIJALA KYBERSMĚRNICI NIS. *Evropský bezpečnostní žurnál* [online]. Praha, 2016, 7.7.2016 [cit. 2018-12-06]. Dostupné z: https://www.esjnews.com/cs/evropska-unie-schvalila-kybersmernici-nis

7.3. Bezpečnostní opatření § IV, § V, § VI, § VII

S neustále rostoucím výkonem výpočetní techniky se také neustále zvyšuje riziko prolomení již existujících šifer. V paragrafech 4, 5 a 6 dochází ke změnám a doplňkům původní legislativy.

Na začátku této části zákona se vůbec definuje, kdo musí a nemusí bezpečnostní opatření používat. Do nového výčtu se doplňuje navíc informační systém základní a digitální služby (tyto pojmy novela zákona zavádí, takže je jasné, že se v tomto výčtu musí objevit). V daném výčtu systémů, které musí být nutně zabezpečeny proti kybernetickému útoku, stojí také kritický informační systém a informační systém kritického informačního systému. Definice toho, co to vůbec takový kritický informační systém je se upravuje v předchozím bodě (viz kapitola 6.2.2. Významný informační systém). Dalším bodem čtvrtého paragrafu je povinnost správců výše zmíněných systémů se nahlásit NÚKIB.

7.3.1. Cloud computing

Zvláštní pozornost je věnována v paragrafu 4 také Cloud computingu. Ten není v původním znění vůbec nijak odlišen. Novela spatřuje Cloud computing jako rizikový článek informačních systémů veřejné správy.

Toto je riziko velmi reálné. Orgán veřejné moci musí důvěřovat dané třetí straně poskytující tuto službu se svými daty. Musí k nim mít také neustálý přístup, a navíc musí umožnit NÚKIB neodkladný přístup k těmto datům z důvodu kontroly. (V zákoně se píše přímo o „*možnosti kontroly uchovávaných informací a dat v reálném čase.*“[131]). Je důležité si uvědomit, že i po finanční stránce se zřizování takovýchto služeb prodraží, což se promítne nejvíce v rozpočtech veřejných orgánů moci.

V novém znění zákona se přesně stanovuje, jak má taková smlouva mezi poskytovatelem Cloudové služby a orgánem veřejné moci. (Například se přesně

[131]Zákon č. 205/2017 Sb. *Zákony pro lidi.cz* [online]. Praha, 2017, 2017 [cit. 2018-12-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205/zneni-20170801#cast1

stanovují podmínky, za kterých může poskytovatel cloudové služby data uchovávat a kdy se jich musí neprodleně a kompletně zbavit.).

Další, drobnější úpravou, která až tak nesouvisí s kybernetickou bezpečností, ale pořád je docela důležitou, především z právního hlediska a možného soudního sporu, je dodatek, který říká, že zohlednění kladených požadavků dle tohoto zákona není nezákonné omezování hospodářské soutěže. Tímto bodem autoři pravděpodobně chtěli zamezit možným stížnostem a zbytečným tahanicím s účastníky hospodářské soutěže.

7.3.2. Organizační a technická opatření

Paragraf 5 v původním znění zavedl 2. úrovně opatření, zajišťujících bezpečnost. Přeloženo do běžné mluvy říká, že bezpečnostní opatření se dělí do kategorie organizační a technické. Nové znění přináší 2 novinky. První zavádí povinnost pro subjekty využívající služby Cloud upravit svou bezpečnostní politiku s ohledem na právě zmíněnou službu.

Druhým dodatkem je doplnění výčtu technických opatření, které musí subjekty zavést, o způsob likvidace dat a provozních údajů. V původním znění toto vůbec není zmíněné, což je velmi zarážející. Subjekty musí mít přesně zdokumentováno, jak probíhá likvidace dat a provozních údajů, co všechno se musí zlikvidovat, aby nezůstala žádná zbytková data a nemohlo dojít k bezpečnostnímu riziku.

7.4. Bezpečnostní incidenty § VIII, § IX, § X

Na tuto část se novela zákona o kybernetické bezpečnosti obzvlášť zaměřuje. Cílem ZKB je vůbec zrychlení identifikace bezpečnostních incidentů. Proto se zavedl vůbec NÚKIB a pojmy jako základní a digitální služba, proto má tento úřad také takové pravomoci, jaké má.

Mezi výčet již mnohokrát zmiňovaných informačních systémů se nadále doplňují poskytovatelé základních služeb, pro které platí stejné podmínky jako pro správce kritických informačních systémů. Incidenty se musí neprodleně po jejich odhalení hlásit buď národnímu CERTu, nebo v případě, že se jedná o kritický bezpečnostní incident NÚKIB přímo.

Zajímavá je potom situace poskytovatelů digitálních služeb. V novém znění je poskytovatel *„… povinen bez zbytečného odkladu hlásit kybernetický bezpečnostní incident s významným dopadem …, pokud má přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu.“*[132]

Velmi důležité je v krátké citaci znění zákona slovíčko pokud. Z citace vyplívá, že poskytovatel digitální služby tudíž tuto povinnost nemá, pokud nedisponuje dostatečnými informacemi pro posouzení dopadu daného incidentu. Hned následující bod říká, že pokud poskytovatel základní služby zjistí, že z důvodu závažného bezpečnostního incidentu poskytovatele digitální služby je narušena jeho bezpečnostní integrita, má povinnost tuto skutečnost hlásit na NÚKIB.

V původním znění zákona se zavádí povinnost mlčenlivosti zaměstnanců NBÚ i po skončení jejich pracovního poměru. Zajímavá je potom část, která říká, že ředitel tohoto úřadu může zaměstnance zprostit této mlčenlivosti. V novém znění sice nedochází k žádné úpravě, ale pouze se přidává další bod, který říká, že informace kritické pro kybernetickou bezpečnost nepodléhají svobodnému přístupu informací. Nic neobvyklého, člověk by očekával, že tato poučka bude obsažena i v původním znění.

7.5.Národní bezpečnostní úřad a NÚKIB § XI až § XXXIII

V původním znění měl na starosti kybernetickou bezpečnost Národní bezpečnostní úřad. V novém znění se z něj vyčlenil Národní úřad pro kybernetickou a informační bezpečnost. Toto byla také jedna z podstatných změn novelizace.

NÚKIB[133] přebírá povinnosti NBÚ a stává se specializovaným orgánem zastřešujícím kybernetickou bezpečnost státu. Výrazně se mu také oproti NBÚ zvýšili pravomoci, ale zároveň také povinnosti. Celkově se snaží nový systém

[132]Zákon č. 205/2017 Sb. *Zákony pro lidi.cz* [online]. Praha, 2017, 2017 [cit. 2018-12-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205/zneni-20170801#cast1

[133]S podivem se samotný NÚKIB definuje až v pozdějších paragrafech (20 a výše). Nejprve se v zákoně uvádí povinnosti a práva tohoto úřadu a až poté je vůbec zakotven.

zajišťující kybernetickou bezpečnost podstatně zvýšit kontrolu nad jejími subjekty a zároveň se snaží podchycovat bezpečnostní incidenty co nejrychleji.

Zajímavé je, že v novém znění je přesně zakotveno, že tento úřad má sídlo v Brně, pokud by někdy v budoucnu došlo k přesunu například do Prahy, tak by se musel také upravit zákon. Proč je toto v zákoně vůbec uvedeno?

Jinak samotný úřad je nezávislý na Národním bezpečnostním úřadě, má vlastního ředitele, který se zodpovídá nikoliv NBÚ, ale předsedovi vlády, který jej také jmenuje a odvolává. V zákoně se sice uvádí, že NÚKIB spolupracuje se státními institucemi zabývající se bezpečností, ale zase se v něm neuvádí žádná míre této spolupráce.

7.5.1. Práva a povinnosti

Zajímavé je potom právo NÚKIBu zveřejňovat informace o jednotlivých kybernetických incidentech společně se jmény subjektu, který byl tímto útokem postižen. Toto samozřejmě ale platí pouze, pokud je tento bezpečnostní incident vážnějšího stupně, který by mohl být nebezpečný i pro široké okolí. Tato pravomoc není v původním znění nikde k nalezení.

Pokud dojde k nějakému bezpečnostnímu incidentu, má Úřad povinnost vydávat opatření pro daný postihnutý subjekt, který musí splnit. V původním znění k tomuto nedochází. NÚKIB má tedy funkci nejen monitorovací a kontrolní, jako tomu bylo doposud, ale také funkci podpory, kdy by daným subjektům měl poskytovat odbornou pomoc v oblasti kybernetické bezpečnosti skrze jím vydaná opatření, které vznikají na profesionálním základě analýzy daného bezpečnostního incidentu. Toto není nijak finančně ohodnoceno. Samotnou realizaci si postihnutý subjekt hradí sám, ale nemusí si vytvářet vlastní analýzy a projekty. Analýzy bezpečnostních rizik a následné řešení jsou relativně drahou záležitostí. Placení pokut s nedodržením povinností je už jiná záležitost.

K tomu, aby Úřad mohl efektivně provádět analýzu vyskytnutých incidentů mu je přidělena řada práv. Například si může vyžádat veškeré informace s incidentem spojeným. Jména pracovníků, technické zázemí, zavedenou bezpečnostní politiku

a další. Úřad se také podílí na ochraně utajovaných informací, jak toto funguje a probíhá není samozřejmě veřejně dostupné.

Práv a povinností má tento úřad celou řadu, avšak je otázkou, jestli je k tomu všemu vybaven především personálně. Podílí se na analýze kybernetických hrozeb, vyvíjí a zkoumá oblast kybernetické bezpečnosti, vzdělává a doučuje pracovníky jak své, tak pracovníky jiných subjektů, vydává bezpečnostní opatření, plánuje budoucnost kybernetické bezpečnosti státu a další. Do toho všeho navíc musí provádět kontrolu, informační podporu a další, velmi náročné operace.

Pravděpodobně rozšíření těchto povinností vedlo k oddělení Národního úřadu pro kybernetickou a informační bezpečnost od Národního bezpečnostního úřadu, který má už tak spoustu práce a jeho vytíženost by byla neúnosná. Největším problémem tohoto úřadu je fakt, že vzdělaní pracovníci z rozličných sfér bude velmi těžké sehnat. Finančně to bude také velmi náročná záležitost, proto je také v zákoně uvedeno, že rozpočet tohoto úřadu se vytváří zvlášť.

Pro korektní práci jsou úřadu poskytovány takřka veškeré osobní údaje zaměstnanců dané základní či digitální služby. (jméno, příjmení, rodné číslo, způsobilost, bydliště, rodná země, datová schránka aj.).

7.5.2. Informační servis

Další z povinností tohoto úřadu je poskytovat na svých webových stránkách informační servis o aktuálních bezpečnostních hrozbách. Tuto povinnost v předchozím znění také nenajdeme.

Bohužel její účinek pravděpodobně není tak valný, protože o ní vědí pouze lidé, kteří znají zákon, nebo webové stránky úřadu. Mezi veřejnost se takováto informace dostane málokdy, což je škoda, protože informace v něm uvedené jsou vcelku užitečné i pro někoho, kdo této problematice příliš nerozumí.

Další jeho nevýhodou je to, že není moc často aktualizován. Zpravidla jednou či dvakrát do měsíce, což asi není úplně optimální. Naopak jeho výhodou je, že pro každou hrozbu zvlášť je ve věstníku hrozeb uveden doporučený postup pro její eliminaci.

Strukturováno je to tím způsobem, že v seznamu hrozeb si může každý uživatel danou hrozbu otevřít. V první kapitole se obecně hovoří o dané hrozbě, kdy byla nalezena, co může způsobit atd.

V druhé kapitole se potom uvádí doporučený postup likvidace této hrozby. Na konci článku jsou potom uvedeny další zdroje týkající se dané hrozby.

25.09.2018	Nebezpečná aplikace QRecorder
24.09.2018	Varování před podvodným vyderačským e-mailem
18.09.2018	Varování před cílenými phishingovými útoky na akademickou sféru
29.06.2018	Ransomware je stále aktuální hrozbou
14.05.2018	Efail - kritická zranitelnost postihující PGP a S/MIME
05.01.2018	Meltdown - chyba v moderních procesorech
04.01.2018	Spectre - chyba v moderních procesorech
25.10.2017	Nový ransomware Bad Rabbit
17.10.2017	ROCA - zranitelnost v generování RSA klíčů
16.10.2017	KRACK - zranitelnost protokolu WPA2 umožňuje čtení šifrovaných dat
27.06.2017	Petya/Petrwrap/NotPetya - nová hrozba ransomwaru

Obr 11. – ukázka věštníku bezpečnostních aktualit[134]

7.5.3. Národní CERT

Nové znění také výrazně rozšiřuje povinnosti národního CERTu[135]. Všechny nové body v paragrafu 17 vybízí národní CERT k důkladnější a otevřenější spolupráci[136] mezi členy zahraničních CERTů nacházejících se v EU. Toto lze prokázat několika body: CERT je povinen sdílet informace se zahraničním CERTem týkající se bezpečnostních incidentů přesahující hranice našeho státu. To

[134]Hrozby. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno, 2018 [cit. 2018-12-07]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

[135]Zajímavý potom může být fakt, že podmínky pro to, aby se daný subjekt označoval jako národní CERT jsou totožné jako v původním znění (z roku 2014) i přes to, že má značně rozšířené povinnosti a práva.

[136]Toto jasně říká i bod K v 17 paragrafu, který jednoduše říká: spolupracuje s týmy jiných členských států. Z právního hlediska je toto vcelku obecná informace, která se dá překroutit různými způsoby. Míra této spolupráce není nijak zvláště stanovena.

samozřejmě platí i pro Českou republiku, která má právo si vyžádat tyto informace od zahraničních členských států EU, pokud se týkají naší, vnitrostátní kybernetické bezpečnosti.

V porovnání s původním zněním, kde žádná spolupráce, ani ve své nejjednodušší formě zmíněné v bodu K paragrafu 17 (viz. poznámka pod čarou) není nikde zmíněna. Spolupráce tedy „fungovala“ čistě na dobrovolné bázi.

Tato informační pomoc není navíc nijak financována státem, který o ní žádá. *„Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 nezbytné náklady.“*[137]

Spolupráce mezi členskými státy sice není dokonalá (viz. předchozí kapitoly zabývající se úrovněmi implementace NISu), definice v zákoně také není úplně jednoznačná (viz. poznámka pod čarou č. 53), ale i přes to se dá říci, že se jedná o správný krok v bezpečnosti kyberprostoru. Ještě je ale příliš brzy činit nějaký závěr, protože jsme teprve v začátcích. Za několik let by bylo zajímavé vytvořit nějakou analýzu (například i grafickou mapu doplněnou o grafy) zabývající se případy, kdy byla tato spolupráce využita.

7.5.4. Kontrolní činnost úřadu

Samotný úřad, jelikož má takto silné pravomoci, podléhá také nově kontrole, která je vybrána členy poslanecké sněmovny. Kontrola je také mnohem přísnější, než když byla kontrolována sekce kybernetické bezpečnosti pod NBÚ.

Hlavní rozdíl mezi minulým a nynějším zněním zákona je dopad takové kontroly. V novém znění je přesně definováno, co a jak se trestá a obecně vzato se podmínky této kontroly a následných trestů velmi zvyšují.

Velmi je například trestáno, pokud daná pověřená osoba neohlásí bezpečnostní incident úřadu. Dalším, velmi závažným přestupkem, je situace, kdy postižený subjekt nepředá všechna data o incidentu úřadu anebo tyto data po předání bezpečně a kompletně nezlikviduje.

---

[137] Zákon č. 205/2017 Sb. *Zákony pro lidi.cz* [online]. Praha, 2017, 2017 [cit. 2018-12-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205/zneni-20170801#cast1

Zásadní rozdíl potom činí slovíčko může. V původním znění je jasně psáno, že úřad uloží v případě provinění se pokutu v řádech X korun. V novém znění jsou tyto řády sice výrazně zvýšeny, ale zato zde existuje více prostoru pro benevolenci samotného úřadu, protože se zde objevuje slovíčko lze. Pokuta tedy vůbec nemusí být vydána. *„Se slova „se uloží pokuta“ nahrazují slovy „lze uložit pokutu““*[138]

Toto je velmi sporná část; pokuta může, ale nemusí být udělena. To samo o sobě na jednu stranu dovoluje úřadu nedávat pokuty menším prohřeškům, ale na druhou stranu může být tato definice zneužita. Jako možné řešení by se nabízelo vrátit se v tomto případě k původnímu znění a snížit minimální hranici pokut, což ale situaci nemusí nijak zásadně zlepšit, záleželo by na výši této hranice.

Nejlepším řešením by bylo naopak zvýšit tuto hranici na nezanedbatelnou úroveň pro všechny. Řešit to procentuálně, nikoliv fixní částkou. Například nastavit nejnižší hranici pokuty na X % z ročního obratu. Pokud by byly pokuty uvedeny v procentech za různé prohřešky, tak by byly tyto částky nezanedbatelné jak pro menší, tak i větší subjekty.

Toto platí i na „druhém vrcholu“. Nejvyšší částky by si také zasloužili tuto úpravu, kdy některé pokuty jsou pro velké subjekty nevýznamné[139]. V případě státních institucí, které nemají vysoký obrat nebo ho mají mizivý či neexistující by se určitě dala vymyslet jiná forma pokutování, například ne finančního rázu, ale spíše personálního. V případě státních institucí by se určitě dali tyto pokuty dále vydávat i fixní částkou.

7.6. Přechodná ustanovení

Je potřeba také zmínit přechodná ustanovení, která se do nového zákona zavádí pouze dočasně. Jejich působnost skončila 8. listopadu 2018 a dnes již nejsou aktuální. Umožňovala subjektům, kterých se novela ZKB týkala se na ni připravit

[138]Zákon č. 205/2017 Sb. *Zákony pro lidi.cz* [online]. Praha, 2017, 2017 [cit. 2018-12-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205/zneni-20170801#cast1

[139]Toto je obecně problém ve spoustě státních odvětvích, například ve Spisové službě jsou tyto pokuty až směšně nízké pro velké firmy s vysokým obratem; fungují pouze v případě menších firem a institucích, které mají nižší obrat.

a dát si do pořádku veškeré náležitosti, které s ním jsou spojené. V této části zákona je definováno do kdy a co se musí úřadu ohlásit a jak se musí změnit jejich současná bezpečnostní politika. V původním znění tohle samozřejmě není.

7.7. Zákon č. 104/2017 Sb.

Tento zákon také upravuje původní znění zákona z roku 2014. Ne však do takové míry jako zákon č. 181/2017 Sb. který je mnohem obsáhlejší. Tento zákon spíše provádí menší změny, které nemají takový význam jako výše zmíněný zákon. Nejdůležitější změnou, kterou přináší je zvýšení pokutové sazby ze stovek tisíc korun na jednotky milionů. Zpřesňuje definice majitele a správce základní / digitální služby, zavádí nová ustanovení týkající se způsobu předávání dat NÚKIB a jiné.

Závěr

Nová nařízení Evropské Unie v podobě GDPR, eIDAS a NIS velmi zásadně upravují dosavadní stav eGovernmentu a eDokumentů obecně v našem prostředí. Tato legislativní opatření jsou obecně i přes své některé nedostatky, jako jsou jejich pomalé zavádění a nízký ohlas občanů (Datové schránky, eOP) dobrým krokem k bezpečnější digitální budoucnosti České republiky. Lze předpokládat, že se tato oblast bude v budoucích letech velmi rychle rozvíjet, stejně jako tomu bylo doposud, a reakcí státu (nebo Evropské Unie) budou stále nová a nová legislativní opatření. Bude docházet k zásadním změnám, nejen právního rámce, ale ke komplexním změnám v problematice bezpečnosti kyberprostoru, a tedy i eDokumentů, které se v něm pohybují.

Možná neprávem jsou veřejností vnímána tato legislativní nařízení přicházející z Evropské unie spíše v negativní světle, ač přináší mnoho dobrého, a nakonec by se dalo říci, že z Evropy pomáhají dělat lepší, bezpečnější a přístupnější místo pro život. Při zkoumání těchto nařízení jako celku v nich lze spatřit určitý obraz budoucnosti Evropy, která je jistojistě digitální a poněkud bezpečnější. Samozřejmě jsou zatím všechna tato nařízení příliš nová a až čas ukáže, jestli budou mít dlouhodobý efekt na naši společnost a její bezpečnost.

Tato práce si kladla za cíl poskytnout relativně podrobný přehled o eDokumentu samotném, o základech informační bezpečnosti a jednotlivých prvcích českého eGovernmentu (Datová schránka, CzechPOINT, Základní registry, eSSL, Portál veřejné správy) a jednotlivých nařízení z Evropské Unie implementovaných do prostředí České republiky různými legislativními opatřeními. Především se jedná o Obecné nařízení o ochraně osobních údajů (GDPR), novely Zákona o kybernetické bezpečnosti (ZKB), které zavádí směrnici NIS a zákony č. 250/2017 Sb. o elektronické identifikaci a 297/2016 Sb. o službách vytvářejících důvěru, které zavádějí eIDAS. V praktické části práce, které je věnována 7. kapitola, bylo provedeno srovnání Zákona o kybernetické bezpečnosti ve svém původním znění s novelami zavádějícími směrnici Evropské Unie NIS.

Bakalářská práce poskytuje jednotný přehled důležitých prvků eGovernmentu a těch nejdůležitějších legislativních změn týkajících se eDokumentů a kyberprostoru obecně. Výsledná komparace Zákona o kybernetické bezpečnosti poukazuje na to, jak velkým krokem bylo zavedení směrnice NIS do právního rámce České republiky. Zároveň poskytuje přehled jednotlivých změn a některé jejich dopady. Cílem bakalářské práce nebylo poskytnout úplný a detailní pohled na celý eGovernment České republiky, ale spíše umožnit čtenáři utvořit si jednotnou obecnou představu o českém eGovernmentu a seznámit jej se základními východisky a nejdůležitějšími prvky eGovernmentu a kyberprostoru obecně.

Ze zmíněných legislativních opatření, které jsou aplikovány do právního rámce České republiky, lze vysledovat některé společné prvky, protínající všechna tato opatření. Jsou jimi především snaha o vytvoření co nejuniverzálnějšího legislativního rámce pro všechny členské země EU. Z nařízení eIDAS, GDPR a směrnice NIS lze vysledovat snahu o sjednocení jednotlivých národních právních rámců a jejich vzájemnou kompatibilitu. Dalším společným znakem všech těchto opatření je snaha o provázání spolupráce v oblastech daných legislativ mezi jednotlivými členskými státy. Společné mají také to, že oproti starším legislativám, kladou důraz především na rychlost nahlašování jednotlivých incidentů, což byl obecně jeden z větších nedostatků minulých legislativních opatření. Ve zmíněných opatřeních vesměs také platí, že brzké nahlášení incidentu je polehčující okolností při pochybení. Dalším společným prvkem všech nařízení je obecné, velmi razantní, zvýšení sankcí a pokut při jejich porušení.

Do budoucna by určitě bylo zajímavé zanalyzovat konkrétní praktické dopady těchto legislativních opatření, jakých výsledků bylo dosaženo či naopak, v čem tato legislativní opatření selhala a v čem by byl ještě prostor k úpravám a doplňkům.

Použité zdroje a literatura

BARTOŠEK, Miroslav. Digitální knihovny - teorie a praxe. Národní knihovna: knihovnická revue[online]. Praha: Národní knihovna ČR, 2004. 2004, roč. 15, č. 4 [cit. 2019-04-19], s. 233. Dostupný z WWW: < http://eprints.rclis.org/6901/1/DL-Bartosek-final2.pdf>. ISSN 1214-0678

BÍLÝ, Radek. Elektronický podpis – k čemu je dobrý a jak jej získat?. Portál.pohoda [online]. 2016 [cit. 2019-04-19]. Dostupné z: https://portal.pohoda.cz/pro-podnikatele/uz-podnikam/elektronicky-podpis-%E2%80%93-k-cemu-je-dobry-a-jak-jej-zi/

Co je eGovernment?. *Ministerstvo vnitra České republiky* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

Co je GDPR?. KYBEZ [online]. 2018 [cit. 2018-07-28]. Dostupné z: https://www.kybez.cz/gdpr

CO JE NÚKIB. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB [online]. Brno, 2017 [cit. 2018-07-26]. Dostupné z: https://www.govcert.cz/

Co považuje GDPR za osobní údaje. GDPR: Obecné nařízení o ochraně osobních údajů [online]. Praha, 2017 [cit. 2018-07-25]. Dostupné z: https://www.gdpr.cz/gdpr/osobni-udaje/

CUBR, Ladislav. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5.

Data corruption. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2019-04-19]. Dostupné z: https://en.wikipedia.org/wiki/Data_corruption

Data loss of image: Data Corruption. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-19]. Dostupné z: https://en.wikipedia.org/wiki/Data_corruption#/media/File:Data_loss_of_image_file.JPG

Datové schránky. In: Město Broumov [online]. [cit. 2018-07-23]. Dostupné z: http://m.broumov-mesto.cz/datove-schranky/d-2525

Datové schránky jako součást eGovernmentu. *Datové schránky* [online]. [cit. 2019-04-19]. Dostupné z: https://www.datoveschranky.info/o-datovych-schrankach/datove-schranky-jako-soucast-egovernmentu

DPO čili Pověřenec pro ochranu osobních údajů. *GDPR Obecné nařízení o ochraně osobních údajů prakticky* [online]. 2016 [cit. 2019-02-11]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/

Dublin Core. Wiki knihovna.cz [online]. 2012 [cit. 2019-04-19]. Dostupné z: http://wiki.knihovna.cz/index.php/Dublin_Core

EDMS - Electronic Document Management System. *EDMS* [online]. 2014 [cit. 2019-04-20]. Dostupné z: http://www.edms.net/

EIDAS: Elektronické značky a pečetě a rekviem za datovou zprávu. Lupa.cz [online]. [cit. 2018-07-22]. Dostupné z:

https://www.lupa.cz/clanky/eidas-elektronicke-znacky-a-pecete-a-rekviem-za-datovou-zpravu/

EIDAS, ELEKTRONICKÝ PODPIS. Ministerstvo vnitra České republiky [online]. Praha: Odbor eGovernmentu, 2016 [cit. 2018-07-24]. Dostupné z: http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx

Elektronická časová razítka. První certifikační autorita [online]. [cit. 2018-07-21]. Dostupné z: http://www.ica.cz/elektronicka-casova-razitka

Elektronické značky. Earchiv.cz [online]. [cit. 2018-07-22]. Dostupné z: http://www.earchiv.cz/b12/b0309001.php3

Elektronický podpis. In: Wikipedia [online]. [cit. 2018-07-24]. Dostupné z: https://cs.wikipedia.org/wiki/Elektronick%C3%BD_podpis#/media/File:Digital_Signature_diagram_cs.svg

ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA: DŮVĚRYHODNÉ ÚLOŽIŠTĚ. *M.I.T Consulting* [online]. [cit. 2018-11-10]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA. *M.I.T Consulting* [online]. [cit. 2019-04-29]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA: HLAVNÍ RYSY ŘEŠENÍ. *M.I.T Consulting* [online]. [cit. 2018-11-10]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

ERMS – ELEKTRONICKÁ SPISOVÁ SLUŽBA: KOMU JE APLIKACE ERMS URČENA? *M.I.T Consulting* [online]. [cit. 2018-11-10]. Dostupné z: http://www.mit-consulting.cz/produkty/elektronicka-spisova-sluzba/

GDPR stručně: O ochraně osobních údajů stručně a jasně. *Úřad pro ochranu osobních údajů: The office for personal data protection* [online]. [cit. 2019-02-07]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

General Data Protection Regulation (GDPR). *EARCHIVACE.CZ* [online]. [cit. 2019-04-29]. Dostupné z: http://www.earchivace.cz/clanky/general-data-protection-regulation-gdpr/

GDPR telefonní linka. *Úřad pro ochranu osobních údajů* [online]. Praha, 2016 [cit. 2019-02-10]. Dostupné z: https://www.uoou.cz/gdpr-telefonni-linka/ds-5287/archiv=0&p1=1059

Gordic spol. s.r.o.: TOP 10 ZADAVATELŮ. VsechnyZakazky.cz [online]. Praha, 2018 [cit. 2018-10-13]. Dostupné z: https://www.vsechnyzakazky.cz/supplier/detail/396115/GORDIC-spol-s-ro

GUTTENBRUNNER, Mark; RAUBER, Andreas. Evaluating Emulation and Migration: Birds of a Feather?. In: International Conference on Asian Digital Libraries. Springer Berlin Heidelberg, 2012. p. 158.

Hostovaná elektronická spisová služba [online]. 2018 [cit. 2018-10-13]. Dostupné z: https://www.kraj-jihocesky.cz/tck/espis/files/e-learning/2_6_0_UzivatelskaDokumentace_spslite.pdf

HOUŠKA a KUNC. COBIT: Co je to COBIT?. Underground ÚAI [online]. [cit. 2019-04-19]. Dostupné z: http://www.uai.tode.cz/stud_mat/Management_IS/Cobit.pdf

Hrozby. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno, 2018 [cit. 2018-12-07]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

ICZ e-spis® LITE: Produktový list. ICZ [online]. Praha, 2018 [cit. 2018-10-13]. Dostupné z: https://www.iczgroup.com/wp-content/uploads/2017/08/PL_e-spis-LITE.pdf

Incidenty, Úniky dat: Hlášení incidentů. *Národní platforma pro GDPR* [online]. [cit. 2019-04-20]. Dostupné z: http://www.gdpr-platforma.cz/index.php/gdpr/hlaseni-incidentu

ISMS. WikiSofia [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/ISMS

ISMS: normy ISO 27001 a ISO 27002. *RiskAnalysisConsultants* [online]. 2018, 2018 [cit. 2019-02-12]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/BS7799

JIROTKA, Tomáš. Slovníček pojmů. Digipodpis [online]. [cit. 2018-07-23]. Dostupné z: http://www.digipodpis.cz/slovnicek.php

Kauza DigiNotar, aneb: když certifikační autorita ztratí důvěru. Lupa.cz [online]. 2011 [cit. 2019-04-19]. Dostupné z: https://www.lupa.cz/clanky/kauza-diginotar-aneb-kdyz-certifikacni-autorita-ztrati-duveru/

KUNT, Miroslav. Novela národního standardu pro elektronické systémy spisové služby. *ISSS* [online]. 2017 [cit. 2019-04-20]. Dostupné z: https://www.isss.cz/archiv/2017/download/prezentace/na_kunt.pdf

Kvalifikovaný certifikát pro elektronický podpis. I. Certification Authority: První certifikační autorita [online]. [cit. 2019-04-19]. Dostupné z: https://www.ica.cz/kvalifikovany-certifikat-pro-epodpis

Kvalifikovaný Dublin Core: Dublin Core Qualified, DCQ. *KTD - Česká terminologická databáze knihovnictví a informační vědy (TDKIV)*[online]. 2012 [cit. 2019-04-02]. Dostupné z: http://aleph.nkp.cz/publ/ktd/00000/08/000000895.htm

Malá novela Zákona o kybernetické bezpečnosti. *CZ.NIC* [online]. 2017 [cit. 2019-04-20]. Dostupné z: https://www.csirt.cz/page/3581/mala-novela-zakona-o-kyberneticke-bezpecnosti/

MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. Praha: Leges, 2012. Teoretik. ISBN 978-80-87576-36-6.

Metadata. *Wikisofia* [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/Metadata

Metadata: Typy metadat. *Wikisofia* [online]. 2013 [cit. 2019-04-19]. Dostupné z: https://wikisofia.cz/wiki/Metadata

Ministerstvo Vnitra České republiky [online]. Praha: Ministerstvo Vnitra, 2018 [cit. 2018-10-11]. Dostupné z: http://www.mvcr.cz/clanek/spisova-sluzba-metodiky.aspx

Ministerstvo vnitra České republiky: Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb. Mvcr[online]. [cit. 2018-07-20]. Dostupné z: http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx

Mobilní aplikace. Datovka [online]. [cit. 2018-07-23]. Dostupné z: https://www.datovka.cz/cs/pages/mobilni-datovka.html

Návrh čtvrtého znění NSESSS. *CNZ.cz* [online]. 2017 [cit. 2019-04-20]. Dostupné z: http://www.cnz.cz/odborne-aktivity/pracovni-skupina-nsesss/aktualni-zneni-nsesss/ctvrte-zneni-nsesss/

Normy ETSI: Vznik standardů. *EARCHIVACE.CZ* [online]. 2014 [cit. 2019-03-19]. Dostupné z: http://www.earchivace.cz/legislativa-a-normy/aplikace-norem-pro-elektronickou-archivaci/

Platforma GINIS. *Gordic* [online]. [cit. 2019-04-29]. Dostupné z: https://www.gordic.cz/produkty/ginis/

Portál veřejné správy. *Ministerstvo vnitra České republiky* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.mvcr.cz/clanek/portal-verejne-spravy.aspx

PREMIS. PREMIS Preservation Metadata Maintenance Activity [online]. 2018 [cit. 2019-04-19]. Dostupné z: https://www.loc.gov/standards/premis/

Práva subjektu údajů: Co znamená právo být zapomenut?. *Úřad pro ochranu osobních údajů: The office for personal data protection* [online]. Praha, 2018 [cit. 2019-02-08]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744

Pseudonymizace osobních údajů. *GDPR: Obecné nařízení o ochraně osobních údajů: prakticky* [online]. [cit. 2019-04-20]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/

ROSER, Max a Hannah RITCHIE. Technological Progress: Moore's Law - exponential increase of the number of transistors on integrated circuits. *Our World In Data* [online]. 2019 [cit. 2019-04-19]. Dostupné z: https://ourworldindata.org/technological-progress

Slovníček pojmů. PostSignum [online]. Praha: Česká Pošta, 2010 [cit. 2018-07-23]. Dostupné z: http://www.postsignum.cz/slovnicek_pojmu.html

SNÍŽKOVÁ, Martina. METS. *Wikiknihovna.cz* [online]. 2012 [cit. 2019-04-13]. Dostupné z: http://wiki.knihovna.cz/index.php/METS

Spisová služba, archivace, skartace: Dlouhodobá archivace a skartace. Software 602 [online]. [cit. 2019-01-11]. Dostupné z: https://www.602.cz/reseni/spisova-sluzba-archivace-skartace/

Standardy pro metadata. NDK Národní digitální knihovna [online]. 2018 [cit. 2019-04-19]. Dostupné z: https://www.ndk.cz/standardy-digitalizace/metadata

Šifrování dat. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2017 [cit. 2019-04-19]. Dostupné z: https://cs.wikipedia.org/wiki/%C5%A0ifrov%C3%A1n%C3%AD_dat

ŠPAČEK, David. EGovernment: cíle, trendy a přístupy k jeho hodnocení. V Praze: C.H. Beck, 2012. Beckova edice ekonomie. ISBN 978-80-7400-261-8.

ŠULC, Roman. EVROPSKÁ UNIE PŘIJALA KYBERSMĚRNICI NIS. Evropský bezpečnostní žurnál [online]. Praha, 2016, 7.7.2016 [cit. 2018-12-06]. Dostupné z: https://www.esjnews.com/cs/evropska-unie-schvalila-kybersmernici-nis

T-Mobile dostal pokutu za obří únik dat o klientech. Utekly adresy nebo výše plateb. *Aktuálně.cz* [online]. 2016 [cit. 2019-02-11]. Dostupné z: https://zpravy.aktualne.cz/ekonomika/t-mobile-dostal-pokutu-za-obri-unik-nezabezpecil-data-uvedl/r~0dc2bc1c63c011e6bc7c0025900fea04/?redirected=1549900938

Úřad pro ochranu osobních údajů. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation [cit. 2019-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/%C3%9A%C5%99ad_pro_ochranu_osobn%C3%ADch_%C3%BAdaj%C5%AF

Vydání certifikátu pro elektronickou pečeť. PostSignum [online]. [cit. 2018-07-21]. Dostupné z: http://www.postsignum.cz/vydani_prvotniho_certifikatu_pro_elektronickou_pecet.html

Vztah ITIL® a CobiT. *BESTPRACTICE.CZ: IT Management Knowledge Base* [online]. [cit. 2019-02-12]. Dostupné z: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Vztah-ITIL-a-dalsich-pristupu/Vztah-ITIL-a-CobiT.alej

Zaručený elektronický podpis. První certifikační autorita [online]. [cit. 2018-07-20]. Dostupné z: http://www.ica.cz/Zaruceny-a-uznavany-ep

Základní informace. CzechPOINT [online]. [cit. 2018-07-23]. Dostupné z: http://www.czechpoint.cz/public/kontaktni-misto/zakladni-informace-kmvs/

ZÁKLADNÍ POJMY. *KYBEZ Platforma kybernetické bezpečnosti* [online]. 2018 [cit. 2019-02-12]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

Základní registry veřejné správy. *BusinessInfo.cz* [online]. 2016 [cit. 2019-04-20]. Dostupné z: https://www.businessinfo.cz/cs/clanky/zakladni-registry-verejne-spravy-ppbi-82624.html#!&chapter=1

Základní registry. *Management Mania* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://managementmania.com/cs/zakladni-registry

Základní registry. Ministerstvo vnitra České republiky [online]. [cit. 2019-04-20]. Dostupné z: https://www.mvcr.cz/clanek/zakladni-registry-zakladni-registry.aspx

Zákon o kybernetické bezpečnosti a jeho aktuální novelizace. *Epravo.cz* [online]. [cit. 2019-04-20]. Dostupné z: https://www.epravo.cz/top/clanky/zakon-o-kyberneticke-bezpecnosti-a-jeho-aktualni-novelizace-106268.html

Zákon č. 104/2017 Sb. Zákony pro Lidi.cz [online]. [cit. 2018-07-26]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104#cast2

Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Zákony pro lidi.cz* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Zákon č. 205/2017 Sb. Zákony pro lidi.cz [online]. Praha, 2017, 2017 [cit. 2018-12-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205/zneni-20170801#cast1

Zákon č. 227/2000 Sb.: Zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). Zakonyprolidi.cz [online]. [cit. 2018-07-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-227

Zákon č. 297/2016 Sb.: Zákon o službách vytvářejících důvěru pro elektronické transakce. Zákony pro lidi.cz [online]. 2016 [cit. 2018-07-24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2016-297

Zákon č. 300/2008 Sb.: Zákon o elektronických úkonech a autorizované konverzi dokumentů. Zakonyprolidi.cz [online]. 2009 [cit. 2019-04-24]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-300

Zákon č. 365/2000 Sb.: Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. *Zakonyprolidi.cz* [online]. 2019 [cit. 2019-04-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365

Zákon č. 499/2004 Sb.: Zákon o archivnictví a spisové službě a o změně některých zákonů. Zakonyprolidi.cz [online]. [cit. 2018-07-20]. Dostupné z: https://www.zakonyprolidi.cz/cs/2004-499

6. Práva subjektu údajů. *Úřad pro ochranu osobních údajů* [online]. 2018 [cit. 2019-04-20]. Dostupné z: https://www.uoou.cz/6-prava-subjektu-udaju/d-27276/p1=4744