

Zásady ochrany informačních systémů z hlediska implementace GDPR ve veřejné správě

Bc. Jana Rýpalová

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Bc. Jana Rýpalová
Osobní číslo: A17343
Studijní program: N3902 Inženýrská informatika
Studijní obor: Bezpečnostní technologie, systémy a management
Forma studia: Kombinovaná
Téma práce: Zásady ochrany informačních systémů z hlediska implementace GDPR ve veřejné správě
Téma práce anglicky: An Information Systems Protection Policy for the Implementation of GDPR in Public Administration

Zásady pro vypracování

1. Zpracujte rešerši vztahující se k problematice zvoleného tématu včetně legislativních norem.
2. Popište strukturu informačního systému obcí.
3. Analyzujte současná rizika zabezpečení informačního systému obcí s důrazem na osobní údaje.
4. Zhodnoťte současný stav informačního systému.
5. Navrhněte vhodný způsob implementace ochranných mechanismů.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN. Informační technologie ve veřejné správě. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 183 s. ISBN 978-80-7318-607-4.
2. DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.
3. POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice. ISBN 80-86898-38-5.
4. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.
5. BARTÍK Václav, JANEČKOVÁ Eva. Ochrana osobních údajů v aplikační praxi-vybrané problémy. Vyd. 4. Praha: Wolters Kluwer, 2016, 287 s. ISBN:978-80-7552-141-5 EAN:9788075521415.
6. BARTÍK Václav, JANEČKOVÁ Eva. Zpracování osobních údajů obcemi. Vyd. 1 Praha: Wolters Kluwer 173 s. ISBN: 978-80-7357-962-3 EAN 9788073579623

Vedoucí diplomové práce:

doc. Ing. Jiří Gajdošík, CSc.
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: 9. prosince 2019
Termín odevzdání diplomové práce: 29. května 2020



doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem v diplomové práci pracovala samostatně a citovala jsem použitou literaturu. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně dne: 10. 8. 2020

Jméno a příjmení studenta: Bc. Jana Rýpalová

Jana Rýpalová, v.r.

.....

podpis studenta

ABSTRAKT

Tato diplomová práce je zaměřena na otázku ochrany informačních systémů z hlediska implementace GDPR ve veřejné správě. Prostřednictvím rešerše odborné literatury, analýzy současných rizik, vztahujících se ke zvolenému tématu, se práce bude zabývat aktuální právní situací včetně možných problémů, které toto téma přináší. Hlavní pozornost bude soustředěna na obecné nařízení o ochraně osobních údajů s odkazy na předchozí právní úpravy v zákonech a na nařízení o ochraně informačních systémů ve veřejné správě, jež budou porovnávány s novými právními úpravami. Cílem této diplomové práce je zjistit, nakolik rozsáhlé jsou rozdíly v právních úpravách již neplatných zákonů a v nových právních normách. A zároveň, jakým způsobem se tyto změny odrazily v již zavedených systémech zpracování osobních údajů, které musely být revidovány pracovníky ve státní sféře.

Klíčová slova: adaptační zákon, ústava, pověřenec, informační systémy, GDPR, nařízení, ochrana osobních údajů, veřejná správa, legislativní normy, ochranné mechanismy, obec, státní sféra.

ABSTRACT

This diploma thesis deals with the issue of information systems protection in terms of GDPR implementation in public administration. Through the research of professional literature, analysis of current risks to the selected topic, the thesis will deal with the current legal situation, including possible problems that this topic brings. Main attention will be paid to the general regulation on the protection of personal data with reference to the previous legislation in the laws and regulations on the protection of information systems in public administration and to compare it with the new legislation. The aim of this diploma thesis is to find out to what the differences in legal regulations of already invalid laws are in comparison with the new legal regulations. At the same time, how these changes have been reflected in the already established systems of personal data processing, which had to be revised by workers in the state sector.

Keywords: adaptation law, constitution, commissioner, information systems, GDPR, regulations, personal data protection, public administration, legislative standards, protection mechanisms, municipality, state sector.

Na tomto místě bych ráda poděkovala vedoucímu své diplomové práce doc. Ing. Jiřímu Gajdošíkovi, Csc. Za jeho vstřícnost, cenné rady a připomínky, kterými mi pomáhal při psaní této práce. Dále bych chtěla poděkovat své rodině za velkou podporu, kterou mi poskytovali během celého studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD	8
I. TEORETICKÁ ČÁST	9
1 LEGISLATIVNÍ NORMY	10
1.1 OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR)	16
1.2 INFORMAČNÍ ZÁKON	18
2 STRUKTURA INFORMAČNÍCH SYSTÉMŮ OBCE	21
2.1 KOMUNIKACE VE VZTAHU ÚŘAD – OBČAN	22
2.2 KOMUNIKACE VE VZTAHU ÚŘAD – ÚŘAD	25
2.2.1 Datová schránka	26
2.2.1 Registry	26
2.3 KOMUNIKACE VE VZTAHU ÚŘAD – PRÁVNICKÁ OSOBA	28
3 ANALÝZA SOUČASNÝCH RIZIK ZABEZPEČENÍ INFORMAČNÍHO SYSTÉMU OBCÍ S DŮRAZEM NA OSOBNÍ ÚDAJE	29
3.1 POPIS RIZIKA A HODNOCENÍ RIZIK	34
II. PRAKTICKÁ ČÁST	36
4 KRITICKÉ POSOUZENÍ AKTUALNÍHO STAVU INFORMAČNÍHO SYSTÉMU	37
4.1 ÚČETNICTVÍ OBCÍ	40
4.2 MZDY A PERSONALISTIKA	44
4.3 POPLATKY	45
4.4 SPISOVÁ SLUŽBA	45
4.5 ZVEŘEJŇOVÁNÍ DOKUMENTŮ Z JEDNÁNÍ ORGÁNŮ OBCE	49
4.6 ZVEŘEJŇOVÁNÍ INFORMACÍ NA ÚŘEDNÍ DESCE OBCE	54
4.7 REGISTR SMLUV	57
4.8 JEDNÁNÍ ZASTUPITELSTVA A ZVEŘEJŇOVÁNÍ NA INTERNETU	58
4.9 BEZPEČNOST NA INTERNETU	59
5 EVALUACE SOUČASNÉHO STAVU ZABEZPEČENÍ BUDOVY MALÉHO OBECNÍHO ÚŘADU	64
ZÁVĚR	67
SEZNAM POUŽITÉ LITERATURY	69
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	76
SEZNAM OBRÁZKŮ	77
SEZNAM TABULEK	78

ÚVOD

Předkládaná diplomová práce se zabývá zhodnocením Obecného nařízení o ochraně osobních údajů, tzv. GDPR, dva roky po jeho uvedení v platnost v květnu 2018. Práce zkoumá jeho implementaci ve veřejné správě a použití počítačových softwarů s ohledem na kybernetickou bezpečnost. Právo na ochranu osobních údajů patří mezi základní práva člověka a zajištění tohoto práva je jedním ze základních pilířů právního státu. Dané evropské nařízení nahradilo zákon o ochraně osobních údajů přijatý na území České republiky v roce 2000.

Po schválení nařízení v roce 2016 byla členským státům Evropské unie dána dvouletá lhůta na přípravu podmínek pro jeho realizaci v rámci práva každého státu. K přijetí zákona v České republice došlo 27. 5. 2018. Dnes je GDPR plně uplatňované v každodenním dění úřadů a v jiných státních institucích. S dvouletým odstupem je tak možné reálně zhodnotit jeho implementaci.

Práce se snaží obsáhnout, jaké zásadní změny s sebou GDPR přineslo a jak se s ním veřejná správa vyrovnala prakticky během uplynulých dvou let. Práce bude zaměřena zejména na využití softwarů při práci s osobními údaji a jejich ochranou.

Teoretická část diplomové práce obsahuje rešerši zákonů, které v českém právu zaručují právo občana na soukromí, a popis obecné informační struktury veřejné správy na úrovni obcí.

V praktické části je na příkladu obecního úřadu popsána práce se softwarovými programy pracujícími s osobními údaji a také se zabezpečením obecního úřadu. Analýzou bezpečnostních systémů se dopracujeme ke srovnání zabezpečení před přijetím GDPR v platnost a po něm.

Cílem této práce je na praktickém příkladu ukázat, do jaké míry byly tímto novým nařízením ovlivněny zejména malé obce a nakolik zásadní změny u nich nastaly.

I. TEORETICKÁ ČÁST

1 LEGISLATIVNÍ NORMY

Při práci ve veřejné správě je využití informačních a komunikačních technologií důležité, neboť úřady se díky nim více přibližují lidem a jejich služby se stávají dostupnější. Pro lepší informovanost jsou v obcích využívány webové stránky, zpravodaj, místní rozhlas, v některých obcích je to i kabelová televize a také rozvoj vysokorychlostního internetu. V malých obcích není jednoduché, aby informace, které předkládáme občanům, byly aktuální, o aktualizaci webových stránek se většinou starají zaměstnanci obce nebo přímo starosta, případně to mohou být dobrovolníci, kteří tyto služby mají jako koníček a prokázali určité znalosti a dovednosti v tomto oboru. Velká města mají kvalifikované IT pracovníky, kteří se aktualizací informací a informačních systémů zabývají převážnou část své pracovní doby.

V současné době je možné žádat státní dotace podporující výstavbu sítí pro vysokorychlostní internet a stále častěji se mluví o chytrých městech, tzv. Smart City, kde by byly využívány nejmodernější informační a komunikační technologie. Znamenalo by to zjednodušení orientace ve městě, parkování, dopravy, sdílení různých dat, úsporu energie, komunikaci s úřady apod. V ideálním případě by tak v budoucnu vznikl tzv. chytrý stát, v jehož rámci by byla komunikace díky informačním technologiím mnohem snadnější. V České republice je koncept Smart City využíván zejména ve velkých krajských městech. Jako úspěšný příklad projektu jsou uváděna velká města států západní Evropy, např. Holandsko, Skandinávie nebo Rakousko. „Dominantními cílovými oblastmi pro implementaci konceptu Smart City v České republice jsou udržitelná mobilita, oblast informačních a komunikačních technologií a efektivní správa území. Tyto oblasti patří i k nejčastěji uváděným při identifikaci úspěšně implementovaných projektů. Nejčastěji uváděným zdrojem informací o konceptu Smart City/Region jsou tematicky zaměřené konference, internet, příklady dobré praxe z jiných měst a také informace od firem, které působí v dané oblasti.“¹

K modernizaci měst dochází za pomoci RIS3 národní strategie. Název RIS3 je odvozen od anglického *Research and Innovation Strategy for Smart Specialisation*. Vytvoření strategií na podporu zejména ekonomického růstu bylo zadáním Evropské unie všem jejím členům. Tento projekt je financován z evropských strukturálních a investičních fondů (ESIF).

¹ Shrnutí „Analýzy aktuální úrovně zapojení ČR do konceptu SMART city a SMART region v souvislosti s novými trendy, včetně návrhů opatření.“ *Vláda* [online]. Praha: Vláda České republiky, 2018 [cit. 2020-07-22]. Dostupné z: <https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/Shrnuti-Analyzy-aktualni-urovne-zapojeni-CR-do-konceptu-smart-city-a-smart-region-v.pdf>

„Usnesením vlády České republiky ze dne 14. března 2018 č. 168 bylo s účinností k 1. dubnu 2018 schváleno převedení agendy **Národní výzkumné a inovační strategie pro inteligentní specializaci České republiky** (tj. Národní RIS3 strategie) z Úřadu vlády České republiky na Ministerstvo průmyslu a obchodu. Povinnosti uložené bývalému místopředsedovi vlády pro vědu, výzkum a inovace tímto usnesením přecházejí na ministra průmyslu a obchodu.“²

Využívání moderních informačních technologií klade i zvýšené požadavky na uživatele, kteří musí být vybaveni požadovanou technikou a také musí být gramotní v práci s těmito technologiemi. Veškerá práce je omezená nejen možnostmi systému, ale zejména zákony, které zajišťují to, aby nebyly zneužity četné osobní údaje, kterými úřady disponují. Proces ochrany osobních údajů souvisí s ochranou soukromí a základy můžeme nalézt již v **Deklaraci práv člověka a občana**³ z roku 1789. Poprvé v ní byly vyhlášeny zásady, které v současné době pokládáme za samozřejmé. Deklarace obsahuje práva člověka, která označuje jako přirozená, nezczizitelná a posvátná, lidé se rodí a zůstávají svobodnými a rovnými ve svých právech. Přirozenými a nezadatelnými právy jsou svoboda, vlastnictví, bezpečnost a právo na odpor proti útlaku. „Výkonná moc je odvozena z principu svrchovanosti národa. Lidská svoboda spočívá v tom, že každý může činit vše, co neškodí druhému, omezení těchto svobod mohou být ustanovena pouze zákonem.“⁴

Dalším významným dokumentem, který zaručuje právo na soukromí, je **Všeobecná deklarace lidských práv**⁵, přijatá Valným shromážděním OSN v roce 1948, která byla přeložena do více než 500 jazyků. Oproti české Listině základních práv, která je vedle Ústavy České republiky nejvyšší právní normou, jsou jí podřízeny všechny členské státy OSN. Všeobecná deklarace lidských práv je dokumentem, který funguje jako globální mapa svobody a rovnosti. Uvedená deklarace je dodnes nejenom živoucím legislativním dokumentem, ale na jeho základě se vyvíjí další pohled na rozvoj lidských práv a jejich chápání, například v případě dětí, sexuálních menšin nebo tělesně či duševně postižených.

² VŠETEČKA, Daniel. RIS3 strategie. *MPO* [online]. Praha: Ministerstvo průmyslu a obchodu, 2019 [cit. 2020-07-22]. Dostupné z: <https://www.mpo.cz/cz/podnikani/ris3-strategie/>

³ SKOUPÝ, Arnošt. *Texty k obecným dějinám kapitalismu I.* Olomouc: Vydavatelství Univerzity Palackého, 1989.

⁴ Deklarace práv člověka a občana. *Informační centrum vlády* [online]. Praha: Vláda České republiky, 24. 8. 2009 [cit. 2020-03-10]. Dostupné z: <https://icv.vlada.cz/cz/tema/deklarace-prav-cloveka-a-obcana-60939/>

⁵ *Všeobecná deklarace lidských práv*. Ilustroval Yacine AÏT KACI. Praha: Informační centrum OSN, [2015]. ISBN 978-80-86348-42-1.

Z práce Ústavního soudu České republiky je patrné dlouhodobé zabývání se rámcem lidských práv, která se promítají do jeho konečných rozhodnutí. Z doby nedávné lze uvést např. judikát Ústavního soudu České republiky (II. ÚS 3169) ze dne 23. 1. 2018, který ukládá povinnost v obecných termínech pro péči o osoby postižené autistickým spektrem. Tímto judikátem bylo potvrzeno, že osoba se zdravotním postižením má právo na dostupnost sociálních služeb.

Na evropské úrovni můžeme ještě připomenout **Úmluvu o ochraně lidských práv a základních svobod**⁶, zkráceně Evropská úmluva o lidských právech, která byla podepsána v Římě v roce 1950. Československo ji ratifikovalo v roce 1992, jako první stát východní Evropy a publikovalo pod č. 209/1992 Sb.

Jedním ze základních pilířů smluvního systému ochrany lidských práv v Evropské unii je Evropská sociální charta, v našem právním systému vedená jako Sdělení č. 14/2000 Sb. m. s. Charta byla přijata dne 18. října 1961 a Československá federativní republika ji podepsala 27. května 1992. „Oproti Evropské úmluvě o ochraně lidských práv a základních svobod bere Evropská sociální charta v úvahu odlišnosti sociálních práv od práv občanských či politických a také i možné ekonomické rozdíly v jednotlivých zemích.“⁷

Dalším počinem Rady Evropy bylo v roce 1981 ve Štrasburku přijetí **Úmluvy o ochraně osob**⁸ se zřetelem na automatizované zpracování osobních dat (č. 115/2001 Sb.). Dnem přijetí této Úmluvy je 28. leden a tento den se stal mezinárodním dnem ochrany osobních údajů a můžeme ho také označit jako počátek ochrany osobních údajů. Poprvé je zde definován pojem osobní údaj a další pojmy týkající se identifikovatelné osoby. „Účelem této Úmluvy je zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoliv národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám a zejména k jejímu právu na soukromý život se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují („ochrana údajů“).“

„Jménem České republiky byla Úmluva podepsána ve Štrasburku dne 8. září 2000. S Úmluvou vyslovil souhlas Parlament České republiky a prezident republiky Úmluvu ratifikoval. Ratifikační listina České republiky byla uložena u generálního tajemníka Rady Evropy,

⁶ *Správní právo: (soubor zákonů)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, [2016]. ISBN 978-80-7380-649-1.

⁷ LINHART, Jan. *Základní lidská práva a svobody a jejich procesní ochrana*. Brno, 2008. Diplomová práce. Masarykova univerzita, Právnická fakulta, Katedra právní teorie.

⁸ DITRICHOVÁ, Petra a Marek JUKL. *Základní prameny mezinárodního humanitárního práva*. Praha: Ministerstvo obrany České republiky – VHÚ Praha, 2017. ISBN 978-80-7278-698-5.

depozitáře Úmluvy, dne 9. července 2001. Při ratifikaci Úmluvy bylo v souladu s článkem 13 Úmluvy učiněno oznámení České republiky, že pověřeným úřadem je Úřad pro ochranu osobních údajů, Havelkova 22, 130 00 Praha 3. Úmluva vstoupila v platnost na základě svého článku 22 odst. 2 dne 1. října 1985. Pro Českou republiku vstoupila v platnost podle odstavce 3 téhož článku dne 1. listopadu 2001.⁹

Na dodržování lidských práv dohlíží kromě států také spolky a organizace. Mezi významné světové organizace se řadí například:

- Human Rights Watch (v překladu Dohlížení na lidská práva) se sídlem v New Yorku,
- Amnesty International, jejímž cílem je prosazování lidských práv, a to např. za pomoci kampaní proti porušování lidských práv,
- Úřad vysokého komisaře OSN pro lidská práva (OHCHR),
- Informační a dokumentační systémy o lidských právech (HURIDOCS),
- Informační síť o právech dětí (CRIN), která se zaměřuje zejména na práva dětí v afrických zemích,
- Asociace pro práva žen v rozvoji (AWID).

V České republice jsou to státní úřady Rada vlády ČR pro lidská práva a Veřejný ochránce práv – ombudsman. Neziskové organizace působící na území ČR jsou Český helsinský výbor, Člověk v tísni, Liga lidských práv a mnoho dalších.

V České republice je právo na ochranu osobních údajů garantováno **Listinou základních práv a svobod České republiky**.¹⁰ „Preambule Listiny představuje hodnotová východiska, na nichž stojí Česká republika. Jedná se o zásadu respektu k přirozeným právům člověka, respektu k právům občana, uznání svrchovanosti zákona a návaznost na tradice humanismu, demokracie a samosprávy.“¹¹ V preambuli nejsou ani opomenuty zkušenosti z dob minulých, kdy lidská práva a základní svobody byly potlačovány.

⁹ Sdělení č. 115/2001 Sb. m. s., Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-21]. Dostupné z: <https://www.zakonyprolidi.cz/ms/2001-115>

¹⁰ *Úplné znění Ústavního zákona České národní rady č. 1/1993 Sb., Ústava České republiky: Úplné znění Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky; některé další související právní předpisy*. 14. vydání. Praha: Armex Publishing, 2019. Edice kapesních zákonů. ISBN 978-80-87451-66-3.

¹¹ KLÍMA, Karel a kol. *Komentář k Ústavě a Listině*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-44-X, s. 595

Podle čl. 10 odst. 1 Listiny má každý právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Podle odst. 2 téhož ustanovení má každý právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. V Listině základních práv a svobod je čl. 7 odst. 1, kde je uvedeno: „Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“¹² Možným protikladem k ochraně soukromí a tím i ochraně osobních údajů je právo na informace čl. 17 Listiny základních práv a svobod. V takovýchto případech musí rozhodnout soud, které právo bude upřednostněno.

Do dubna 2019 byl článek č. 10 odst. 3 Listiny základních práv a svobod ošetřen **zákonem č. 101/2000 Sb., o ochraně osobních údajů**¹³ a o změně některých zákonů, kterým byl také zřízen Úřad pro ochranu osobních údajů. Tento zákon v souladu s právem Evropské unie a také v souladu s ratifikovanými mezinárodními smlouvami upravoval vše, s čím je možné se setkat při zpracování a předávání osobních údajů až do roku 2019, kdy vstoupil v platnost nový **zákon č. 110/2019 Sb., o zpracování osobních údajů**.¹⁴ Přijetí tohoto zákona však předcházelo nabytí účinnosti **Nařízení Evropského parlamentu a Rady (EU) č. 2016/679**¹⁵, často označované jako GDPR (General Data Protection Regulation).

Kromě uvedených zákonů jsou informační systémy veřejné správy ovlivněny dalšími předpisy. Těmito předpisy jsou **zákon č. 365/2000 Sb., o informačních systémech veřejné správy**.¹⁶ Vymezuje základní pojmy týkající se informačních systémů, říká nám, jaké informace budeme evidovat, zpracovávat.

Dalším zákonem je **zákon č. 89/2009 Sb., občanský zákoník**¹⁷ a **zákon č. 40/2009 Sb., trestní zákoník**¹⁸, ve znění pozdějších předpisů. V něm je možné najít dvě skutkové podstaty věnované ochraně osobních údajů. Odst. 1 a 2 § 180 „Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí,

¹² Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součástí ústavního pořádku České republiky. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-21]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1993-2>

¹³ BARTÍK, Václav. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: ANAG, 2010. Právo (ANAG). ISBN 978-80-7263-613-6.

¹⁴ PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): Zákon o zpracování osobních údajů: komentář*. 2. aktualizované a doplněné vydání. Praha: Leges, 2019. ISBN 978-80-7502-396-4.

¹⁵ Tamtéž.

¹⁶ Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákon. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-04]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-365>

¹⁷ Zákon č. 89/2009 Sb., občanský zákoník. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-12]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-89>

¹⁸ Zákon č. 40/2009 Sb., trestní zákoník. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-06-02]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40?>

zpřístupní, jinak zpracovává nebo si присvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci.“¹⁹

Součástí naší legislativy jsou také ratifikované a vyhlášené mezinárodní smlouvy o lidských právech a svobodách. Patří sem například Mezinárodní pakt o občanských a politických právech, který převzal znění článku 12 Všeobecné deklarace lidských práv.

Protiváhou zákonných omezení na ochranu soukromí a osobních údajů máme garantované právo na informace **zákonem č. 106/1999Sb., o svobodném přístupu k informacím**²⁰, tzv. informační zákon, který vychází z Listiny základních práv a svobod.

Do historického vývoje budování informačních systémů veřejné správy patří také **zákon č. 111/2009 Sb., o základních registrech**.²¹

Po vzniku samostatných obecních úřadů v 90. letech minulého století došlo k velkému rozmachu informačních a komunikačních technologií. Úřady, občané i podnikatelé se snaží ulehčit si a zjednodušit komunikaci mezi sebou. Nahrává tomu masivní rozšíření internetu. Začínají se používat elektronické formuláře, vznikají centrální evidence, tzv. registry, jsou to centrální databáze, které obsahují různé informace. Shromažďují se zde informace o osobách, majetku, veřejných zakázkách, osobách podnikajících a jiných centrálně evidovaných skutečnostech. Registry vedou různé instituce a chybí jejich vzájemné propojení.

V roce 1999 vláda přijímá strategický dokument „Státní informační politika – cesta k informační společnosti“.²² Rok po přijetí tohoto dokumentu zřizuje nový úřad, Úřad pro veřejné informační systémy zvaný ÚVIS. Má za úkol vytvářet pravidla pro budování informačních systémů veřejné správy. V souvislosti s rozvojem informačních systémů a zjednodušením komunikace je přijat **zákon č. 227/2000 Sb., o elektronickém podpisu**²³ a **zákon č. 133/2008 Sb., o evidenci obyvatel a rodných číslech**.²⁴

¹⁹ Tamtéž.

²⁰ Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-18]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106>

²¹ Zákon č. 111/2009 Sb., o základních registrech. In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-04-23]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-111>

²² Státní informační politika – cesta k informační společnosti. *Vláda* [online]. Praha: Vláda České republiky [cit. 2020-03-19]. Dostupné z: <https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/>

²³ Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-18]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-227>

²⁴ Zákon č. 133/2008 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-04]. Dostupné z:

Nesmíme zapomenout na **zákon č. 128/2000 Sb., o obcích**.²⁵ Tento zákon vymezuje a upravuje vše, co souvisí s činností obce. Obec spravuje své záležitosti samostatně, v samostatné působnosti nebo je na obec přenesena působnost státu – tzv. přenesená působnost, kterou obec vykonává za stát. Mezi tuto působnost patří matrika, evidence obyvatel a činnost stavebních úřadů. Zákon o obcích také určuje, jaké má kdo pravomoci, jak se postupuje při dispozici s obecním majetkem, do jaké finanční výše plnění může rozhodnout starosta, jak svolat zastupitelstvo atd.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti²⁶ upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

1.1 Obecné nařízení o ochraně osobních údajů (GDPR)

Celý název je Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů), v odborných textech se běžně objevuje označení GDPR, což je zkratka z anglického General Data Protection Regulation). Toto nařízení je velice významný a komplexní právní rámec, jehož podstatou je zabezpečit osobní údaje při jejich zpracování proti jejich zneužívání, nařizuje údaje shromažďovat a uchovávat.

Nařízení kategorizuje údaje na:

- **Citlivé osobní údaje**, mezi které se řadí údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech, o pravomocném odsouzení osob, genetické a biometrické. Jedná se o údaje, které podléhají velmi přísnému režimu, neboť informace, kterou nesou, by mohla konkrétní osobu poškodit ve společnosti nebo ji diskriminovat.
- **Osobní údaje** jsou ve směrnici definovány jako veškeré informace vztahující se k identifikované či identifikovatelné fyzické osobě. Mezi základní osobní údaje

<https://www.zakonyprolidi.cz/cs/2000-133>

²⁵ Zákon č. 128/2000 Sb., o obcích (obecní zřízení). In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-06-30]. <https://www.zakonyprolidi.cz/cs/2000-128>

²⁶ Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-04-29]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>

se řadí pohlaví, věk a datum narození, jméno a příjmení, osobní stav a např. fotografii nebo videozáznam.

Nařízení reaguje na technologické změny posledních let, kdy roste vnitřní propojení trhů evropského hospodářského prostoru. Toto nařízení se dotýká opravdu každého z nás. Těmito nařízeními získala EU účinný nástroj k ochraně osobních údajů.

Nařízení se stalo účinné především kvůli vysokým pokutám, které za jeho porušení hrozí. Velké hysterie kolem přijetí tohoto zákona využilo velké množství poradenských společností. Určitě není příliš troufalé tvrdit, že s vidinou výdělku konzultanti záměrně v mediích dramatizovali změny, které s sebou nové nařízení přineslo.

Současně se objevily i názory protichůdné, prohlašující, že nařízení je významné, ale nedá se říct, že by přineslo přímo zvrát v oblasti ochrany osobních údajů. Hlavním důvodem je to, že tuto oblast upravují ještě další právní dokumenty. Pokud jsme doposud zpracovávali osobní údaje v souladu s českým **zákonem č. 101/2000 Sb., o ochraně osobních údajů**, tak ve své podstatě se příliš nemění. Nařízení vychází ze stejných zásad, jako tento zákon²⁷:

- Zásada zákonnosti,
- Zásada korektnosti a zásada transparentnosti,
- Zásada omezení účelu,
- Zásada přesnosti,
- Zásada omezení uložení,
- Zásada integrity a důvěrnosti.

Podstatou a hlavním důvodem, proč nařízení vzniklo, bylo poskytnout soubor standardizovaných zákonů o ochraně údajů ve všech členských zemích EU. To by mělo občanům EU usnadnit pochopení způsobu využití jejich údajů a možnosti chránit své osobní údaje, a to ve všech zemích EU. Zásadním rozdílem, při srovnání s českým zákonem o ochraně osobních údajů, je tak jeho obšírná územní platnost.

²⁷ ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

1.2 Informační zákon

Na základě **zákona č. 106/1999Sb., o svobodném přístupu k informacím**²⁸, tzv. informační zákon, jsou státní orgány, mezi které se řadí např. ministerstva, kraje, obce a také veřejné instituce, kterými jsou státní společnosti, příspěvkové organizace a další, povinny poskytovat informace, na které se občané dotazují.

„Povinnými subjekty, které mají podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím povinnost poskytovat informace vztahující se k jejich působnosti, jsou státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce. Povinnými subjekty jsou dále ty subjekty, kterým zákon svěřil rozhodování o právech, právem chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti.“²⁹ V praxi to znamená, že dotaz se může týkat jakékoliv sféry, např. nakládání s finančními prostředky, stavebními plány, smlouvami apod.

„Žádost o poskytnutí informace se podává ústně nebo písemně, a to i prostřednictvím elektronické komunikace (e-mail doručený na adresu elektronické podatelny obce, a to i bez elektronického podpisu). Není-li žadateli na ústně podanou žádost informace poskytnuta, anebo nepovažuje-li žadatel informaci poskytnutou na ústně podanou žádost za dostačující, je třeba podat žádost písemně. Abychom žádost mohli posuzovat jako žádost dle informačního zákona, musí splňovat konkrétní obsahové náležitosti. Pokud by žádost o informaci neobsahovala sdělení, že jde o žádost dle zákona 106 a adresu pro doručování, a v případě elektronicky podaných žádostí nebyla podána na adresu elektronické podatelny, nejednalo by se o žádost dle příslušného zákona a správní subjekt by žádost nevyřizoval dle daného zákona.“³⁰

Právo na ochranu osobních údajů je zařazeno mezi základní lidská práva, zatímco právo na informace je řazeno mezi tzv. politická práva. Tento zákon dává širokému počtu žadatelů možnost zeptat se státních institucí na vše co je spojené s jejich činností a státní instituce jsou povinny informace poskytnout, nově pod hrozbou vysoké pokuty za neposkytnutí žádaných

²⁸ Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-18]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106>

²⁹ PASEKOVÁ, Eva. Svobodný přístup k informacím? Soudy jsou zahlceny žádostmi i šikanózními dotazy. *Česká justice* [online]. Praha: Ministerstvo vnitra České republiky 2016 [cit. 2020-04-23]. Dostupné z: <https://www.ceska-justice.cz/2016/12/svobodny-pristup-k-informacim-soudy-jsou-zahlceny-zadostmi-sikanoznimi-dotazy/>

³⁰ Manuál pro obce k zákonu o svobodném přístupu k informacím. *MV ČR* [online]. Praha: Ministerstvo vnitra České republiky, 2017 [cit. 2020-04-23]. Dostupné z: <https://www.mvcr.cz/odk2/soubor/manual-pro-obce-k-zakonu-o-svobodnem-pristupu-k-informacim.aspx>

informací. Subjekt, který informace poskytuje, dotazy i odpovědi povinně zveřejňuje na svých webových stránkách.

Tento zákon je možné doslova zneužít a svými dotazy doslova ochromit činnost malých obecních úřadů neustálými dotazy, což může hraničit se šikanou. Obce mají v takových případech jen velmi omezené možnosti, jak se s takovou situací vyrovnat. „Zákon je napsán velmi nevyváženě ve prospěch těch žadatelů, kteří si jej zvolili jako svoji zbraň či nástroj pomsty vůči povinným subjektům, např. vůči soudům. Jeden z žadatelů, nespokojený s délkou svého řízení u Nejvyššího soudu, dokonce neváhal napsat, že až do vydání rozhodnutí v jeho věci bude „za trest“ Nejvyššímu soudu denně posílat novou žádost podle informačního zákona – a skutečně zhruba desítku žádostí takto poslal (každou s pěti základními otázkami a řadou dílčích podotázek).“³¹ Momentálně vláda zpracovává novelu zákona o volném přístupu k informacím. V podstatě momentálně neexistuje omezení pro žadatele o informaci. Pokud je splněna forma žádosti, je velmi těžké vyhnout se odpovědi na všetečné otázky různého charakteru.

„Jediný občan dokázal přimět spoustou žádostí o informace celé zastupitelstvo obce k rezignaci. Teď se stohy jeho podání musí prokousávat ministerstvem dosazený správce.“³² Takovým správcem je úředník, kterého pověřil ministerstvo vnitra vedením obce po celou dobu, kdy obec nemá volený zastupitelský orgán. Správce má omezené pravomoci, proto pod jeho vedením nedochází k rozvoji obce, ale spíše udržování nezbytného chodu úřadu.

Při práci ve veřejné správě není jedinou těžkou zkouškou uvedený informační zákon. Stále se zvyšující nároky, které se stupňují na základě vršících se nařízení a zákonů, a s tím související obrovská zodpovědnost vedou k tomu, že mnohé obce zůstávají bez vedení. To dokazují údaje z posledních komunálních voleb v roce 2018.³³

Ve volbách kandidovalo o 17 tisíc méně osob, než při předešlých komunálních volbách o čtyři roky dříve. Celkem v 17 obcích se kvůli nedostatečnému zájmu jejich občanů volby nemohly

³¹ PASEKOVÁ, Eva. Svobodný přístup k informacím? Soudy jsou zahlceny žádostmi i šikanózními dotazy. *Česká justice* [online]. Praha: Ministerstvo vnitra České republiky 2016 [cit. 2020-04-23]. Dostupné z: <https://www.ceska-justice.cz/2016/12/svobodny-pristup-k-informacim-soudy-jsou-zahlceny-zadostmi-sikanoznimi-dotazy/>

³² ŤOPEK, Martin. Správce převzal řízení obce, jejíž zastupitele vyhnaly stohy žádostí. *IDnes* [online]. 28. 1. 2014 [cit. 2020-05-18]. Dostupné z: https://www.idnes.cz/pardubice/zpravy/spravce-obec-sec-zastupitelstvo-zadosti.A140128_2027379_pardubice-zpravy_mt

³³ NOVOTNÝ, Jan. Hledá se starosta. *Euro* [online]. 5. 10. 2018 [cit. 2020-05-18]. Dostupné z: <https://www.euro.cz/politika/hleda-se-starosta-spravu-nad-radou-obci-prevezme-ministerstvo-vnitra-1423046>

uskutečnit. Ve většině obcí kandidovalo předně tolik osob, kolik je potřeba na sestavení zastupitelstva.

Na závěr této kapitoly můžeme uvést, že normativní regulace a správní řád nepatří zrovna mezi jednoduchou četbu. Kromě toho dochází k častým změnám a novelizacím, ve kterých se volení zástupci obcí musí velmi dobře orientovat, protože na sebe v moment nastoupení do funkce přebírají nemalou zodpovědnost. Proto je nedílnou součástí i účast na školeních a samovzdělávání. Za poslední desetiletí se velké množství školení zaměřuje také na výuku v oblasti informačních technologií. Zásadami využívání informačních technologií ve státní správě, zejména se zaměřením na kybernetickou bezpečnost, se budeme zabývat v dalších kapitolách.

2 STRUKTURA INFORMAČNÍCH SYSTÉMŮ OBCE

Základním předpokladem každého informačního systému je informace. Význam informace a informovanosti je v dnešní době nedocenitelný. Informace zastarávají mnohem rychleji než v minulosti a lze předpokládat, že tento trend bude neustále pokračovat. Zakladatel kybernetiky Norbert Wiener v jednom ze svých děl uvedl, že pokud chce člověk aktivně žít, musí žít s přiměřenými informacemi. Wiener označil informaci jako „to, co si vyměňujeme s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.“³⁴

Informace je velmi široký, mnohoznačný pojem, který se užívá v různých významech. V nejobecnějším smyslu je informace chápána jako údaj o prostředí, jeho stavu a procesech v něm probíhajících. Informace snižuje nebo odstraňuje neurčitost (entropii) systému (např. příjemce / uživatele informace). Množství informací lze charakterizovat tím, jak se jejím přijetím změnila míra neurčitosti přijímajícího systému.³⁵ Jako příklad si můžeme uvést následující tabulku, kde jsou vyobrazeny základní funkce informačních a komunikačních technologií ve vztahu k informačním technologiím.

FUNKCE	DEFINICE	PŘÍKLADY
Zachycení informací	Získávání a vyjadřování informací ve formě umožňující přenos, zpracování a uchování informací.	Klávesnice počítače, magnetofon, telefonní přístroj.
Přenos informací	Přenos informací z jednoho místa na druhé – od zdroje k příjemci.	Telefonní síť, televizní vysílač, novinová distribuční síť, pošta (doručující dopisy).
Uchování informací	Přesun informací na místo, kde budou uchovány a později zpřístupněny.	Papír, magnetická páska, CD – ROM, disketa, fotografický film.
Vyhledávání informací	Hledání a zpřístupnění konkrétních informací požadovaných příjemcem.	Hledání v kartotéce, některé počítačové programy spolu s organizací dat v paměti.
Zpracování informací	Vytváření nových informací (s novým významem) z dostupných informací.	Počítačové programy, založené na znalostech, vyjádřených ve vhodné formě.
Zobrazování informací	Prezentace informací ve formě, kterou je člověk schopen vnímat.	Obrazovka počítače, tiskárny, magnetofon, multimedia.

Obrázek č. 1 Základní funkce informačních a komunikačních technologií³⁶

³⁴ Teorie informace. *IS Mendelu* [online]. Brno: Mendelova univerzita [cit. 2020-06-07]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7017

³⁵ JONÁK, Zdeněk. Informace. *Databáze Národní knihovny ČR* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2020-07-07]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD

³⁶ TRUNEČEK, Jan. *Management v informační společnosti*. 2. vydání. Praha: Vysoká škola ekonomická, 1999. ISBN 80-7079-683-9, s. 139

V kybernetickém slovníku je informace definována jako „abstraktní pojem, označující obsah neboli význam sdělení, něco, co snižuje neurčitost a naopak zvyšuje pravděpodobnost předvídat nebo přesně poznat výsledky určité události. Má nehmotný charakter, ale je vždy spojena s nějakým fyzickým pochodem, který ji nese. Informacemi mohou být např. údaje, čísla, znaky, povely, instrukce, příkazy, zprávy apod. Nositelům informace je signál. Je to časově proměnná fyzikální veličina, jíž jsou zobrazeny údaje. Signál umožňuje získání informace, její přenos na dálku, uchování v paměti a zpracování v počítači.“³⁷

„Jedním ze základních předpokladů života v informační společnosti je neomezený přístup k veřejně dostupným informacím, zejména pak k těm, které plynou z veřejné správy. Mají-li být informační potřeby veřejnosti v tomto směru dostatečně uspokojovány, je zapotřebí, aby struktura veřejného informačního systému obce zahrnovala co nejvíce informačních zdrojů. Cílem této kapitoly je tedy podrobněji se věnovat jednotlivým prostředkům jednosměrné komunikace, formám obousměrné komunikace, ale také dalšímu informačnímu zdroji, kterým mohou být veřejné informační služby.“³⁸

Obecní úřad je povinen pravidelně informovat o své aktuální činnosti. Způsob poskytování informací se odvíjí od jejího typu a také od jejího příjemce. Tlak na obec se zvyšuje současně s dobou. Kromě informovanosti občanů je důležité zároveň slyšet zpětnou vazbu. Zaměstnanci obce by neměli zapomínat, že právě občan rozhoduje o tom, kdo obec povede.

Z historie obecní komunikace jsou známí hudebníci a ponocní, kteří ohlašovali aktuality na některých místech ještě začátkem 20. století. Tento přenos informací s sebou nesl nepřesnost informací a především stručnost. Činnost těchto lidových zpravodajů vystřídaly první tištěné noviny, které umožňovaly plošné oslovení velkého počtu obyvatel. S rozvojem techniky se na konci 20. století stal významným pomocníkem internet. Způsoby a možnosti komunikace současnosti budou podrobněji rozepsány v následující podkapitole.

2.1 Komunikace ve vztahu úřad – občan

Poskytování informace orgány obce bez předchozí žádosti se nazývá jednosměrnou komunikací a nedochází k cílené odpovědi ze strany veřejné správy. Občané si vyberou z dostupných

³⁷ JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN. *Informační technologie ve veřejné správě*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. ISBN 978-80-7318-607-4, s 14.

³⁸ ZOBAL, Jaroslav. *Informační systém města či obce*. Brno, 2006. Diplomová práce. Masarykova univerzita, Ekonomicko-správní fakulta. Vedoucí práce Mgr. Jiří Špalek, Ph.D.

informačních prostředků ten, který jim nejlépe vyhovuje a je pro ně nejvhodnější. Požadované informace se sám pokusí vyhledat.

Mezi tyto prostředky patří:

- webové stránky,
- informační kanál kabelové televize,
- místní rozhlas,
- úřední deska,
- obecní zpravodaj,
- tištěné materiály a publikace,
- informační letáky,
- informační vývěsní skřínky,
- informační SMS zprávy a e-maily.

Okruh zveřejňovaných informací je možné také rozdělit na:

- **Povinné** – ty jsou stanoveny zákonem č. 106/1999 Sb., o svobodném přístupu k informacím a standardy informačních systémů veřejné správy (informace musí být přístupné v sídle obecního úřadu a také způsobem umožňujícím dálkový přístup).
- **Dobrovolné** – rozsah informací je ponechán na uvážení příslušného úřadu, který si množství, okruh a formu volí podle svého uvážení. S ohledem na zákony o ochraně osobních údajů se dá zveřejňováním velkého množství informací předejít dotazování veřejnosti.

Pokud občan nenalezl požadované informace prostřednictvím jednosměrné komunikace, může se obrátit na příslušný úřad s konkrétní žádostí o informace. V takovém případě mluvíme o obousměrné komunikaci. Zde již existuje zpětná vazba, kdy kompetentní úředník odpovídá na občanův dotaz. Ten může být podán ústně nebo písemně a v obou případech prostřednictvím telekomunikačního zařízení.

Mezi prostředky obousměrné komunikace můžeme zahrnout:

- osobní kontakt,
- telefonický kontakt,
- poštovní korespondence,

- elektronická pošta (e-mail),
- datová schránka.

Pokud žádost směřuje k poskytnutí informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, jsou dodržovány stanovené lhůty. Konkrétně se jedná o 5 kalendářních dnů v případě, že informace již byla zveřejněna, žadatel je pak naveden, aby si údaj samostatně vyhledal, a 15 kalendářních dnů tehdy, pokud žadatel trvá na přímém poskytnutí informací. To platí pouze v rovině povinné komunikace a týká se zejména povinně zveřejňovaných informací. Poskytnuté informace subjekt zveřejní způsobem umožňujícím dálkový přístup. V praxi platí, že úředník v zásadě reaguje na žádost občana o poskytnutí informací stejnou formou, jakou se občan na daný úřad obrátil.

Komunikace úřadu a občana prostřednictvím veřejného informačního systému je podstatou informační činnosti každého úřadu. Způsob informování je upravován zákony. V kompetenci každého úřadu je forma, jakou při komunikaci zvolí. V této souvislosti lze říct, že představitelé obce mají zájem na co nejširším využití informačních prostředků. Vede je k tomu mnoho různých důvodů, mohou být politické, snaha plnit předvolební sliby nebo se také blíží nové volby. Dalšími důvody může být tlak ze strany společnosti, která má rostoucí potřebu informovanosti, také může mít potřebu držet krok s okolními vesnicemi.

Dnešní doba přináší obrovský boom v oblasti informačních technologií, které usnadňují komunikaci, ale objevují se i nové informační prostředky a formy komunikace. Vyšší finanční prostředky a kvalita moderních technologií způsobují, že i menší obce modernizují veřejný informační systém. Při modernizaci se nesmí zapomínat, že struktura informačního systému se musí přizpůsobit nejen mladé generaci, ale také starším spoluobčanům.

Poskytování a předávání informací veřejnosti má být především objektivní a včasné. Veřejná správa není pouze výkonným orgánem, ale je především službou občanům. Každý občan by měl vědět, kde je možné potřebné informace získat a měl by také vědět, proč je užitečné tyto informace znát a využívat.

Ke spokojenosti veřejnosti přispěje, když poskytované informace splňují následující kritéria:

- Pravdivost – pravdivé informace jsou základním předpokladem pro důvěru občana ve veřejnou správu (využití nepravdivých informací by vedlo ke konkrétním škodám na straně uživatele a v konečném důsledku by byl efekt zveřejňování informací negativní).

- Aktuálnost – základní podmínka pro zajištění pravdivosti (neaktuální a zastaralá informace se totiž stává informací nesprávnou a nepravdivou).
- Srozumitelnost – informace musí být naformulována s ohledem na vzdělání, schopnosti i potřeby občanů. V tomto případě je také důležité rozlišit činnosti územní samosprávy, které spadají do oblasti přenesené působnosti státní správy dané platnou legislativou, a činnosti územní samosprávy, sem patří záměry zastupitelstva, priority a plány. Občan jako volič je může významným způsobem ovlivnit.
- Věrohodnost – na první pohled musí být zřejmé, že poskytované informace pocházejí z veřejné správy a jsou tedy identifikovatelné (jednoznačně lze dohledat původce informace).
- Srovnatelnost – poskytované údaje by mělo být možné sumarizovat a porovnat podle stanovených kritérií (např. s jinými obcemi).
- Přiměřenost – informace by měly být skutečně požadované a jejich poskytnutí by mělo být adekvátní dané situaci a nemělo by docházet k vyhýbání se řešení konkrétních problémů.

Vedle vyjmenovaných požadavků na kvalitu poskytovaných informací by orgány veřejné správy měly dále respektovat potřeby, možnosti a zvyklosti příjemců informace, v tomto případě zejména obyvatel dané obce. Volbou vhodných informačních prostředků a komunikačních forem s ohledem na velikost obce a místní zvyklosti by měla být zajištěna bezproblémová dostupnost informací, případně i možnost jejich uchování. Při poskytování informací musíme mít na paměti ochranu osobních údajů a jejich zabezpečení.

2.2 Komunikace ve vztahu úřad – úřad

Komunikace mezi úřady je velice důležitá, oceňuje se především rychlost při různých povolovacích a schvalovacích procesech. Nadřízené úřady, úřad s rozšířenou působností a krajský úřad se vyjadřují k záměrům obce, které musí být v souladu s tzv. nadřazenou dokumentací, jež se týká např. plánu rozvoje a kanalizací, územního plánování, dopravy aj.

Komunikace mezi úřady může probíhat stejně jako mezi úřadem a občanem následující formou:

- osobní kontakt,
- telefonický kontakt,
- poštovní korespondence,

- elektronická pošta (e-mail),
- datové schránky.

2.2.1 Datová schránka

Komunikace prostřednictvím datových schránek nahrazuje klasické doručování v listinné podobě, protože podle zákona je zrovnoprávněna papírová a elektronická verze zasílaných dokumentů. „Dokument (datová zpráva), který je dodán do datové schránky, je doručen okamžikem přihlášení do datové schránky oprávněnou osobou. Obdobně jako u listovních zásilek funguje fikce doručení: nepřihlásíte-li se do datové schránky ve lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, považuje se tento dokument za doručенý.“³⁹

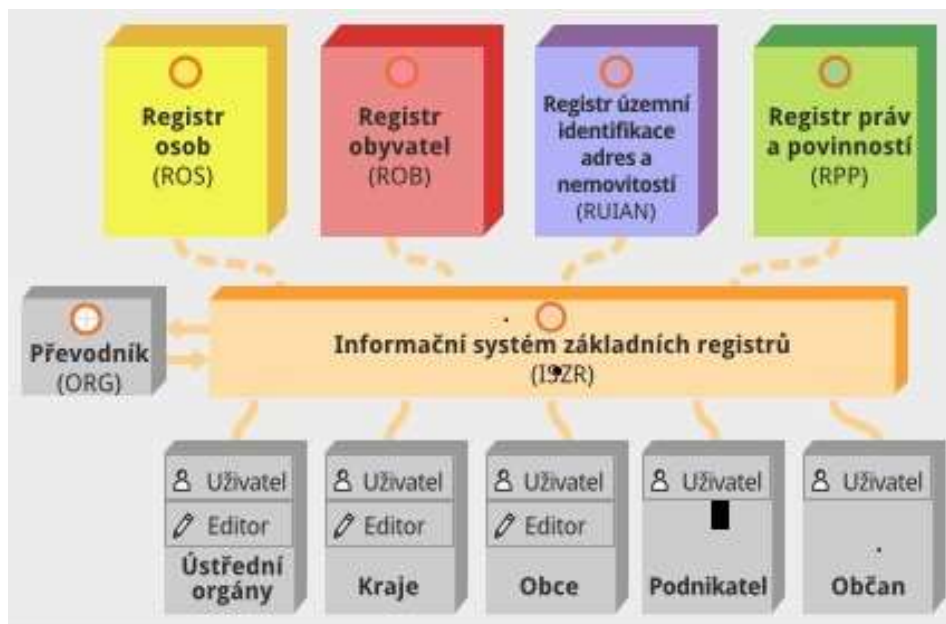
Zřízení datové schránky je povinné pro orgány státní moci a právnické osoby zapsané v obchodním rejstříku, pro ostatní podnikající i nepodnikající fyzické osoby je zřízení datové schránky dobrovolné. Orgány veřejné moci jsou povinny posílat dokumenty adresátům přednostně do datové schránky, pokud ji mají zřízenou. V roce 2010 se uvažovalo o zpoplatnění datových schránek. Ministerstvo vnitra tehdy navrhlo, aby odesílatel zaplatil 15 Kč za poslání úředního dokumentu. Takto by celý projekt ztratil jednu ze svých hlavních výhod, kterou byla bezplatnost.

Kvůli výše uvedeným důvodům je datová schránka preferovaným způsobem komunikace ve státní sféře.

2.2.1 Registry

Dalším významným způsobem komunikace úřadů mezi sebou jsou tzv. registry. Registr je v podstatě centrální databáze, která obsahuje informace týkající se osob, majetku, veřejných zakázek, ekonomických subjektů, územní identifikace nemovitostí. V registrech jsou využívány inteligentní elektronické formuláře, jejichž prostřednictvím mohou být úřední záležitosti vyřízeny kdykoli a odkudkoli za předpokladu, že je v místě dostupné internetové připojení. K takovému vyřízení záležitostí je potřebná elektronická identita a tou je elektronický podpis.

³⁹ *Datové schránky* [online]. Praha: Ministerstvo vnitra České republiky, 2019 [cit. 2020-04-16]. Dostupné z: <https://www.datoveschranky.info/>



Obrázek č. 2 Schéma fungování základních registrů⁴⁰

„Základní registry představují mozek eGovernmentu v České republice a všech souvisejících projektů elektronizace veřejné správy. Zavedením základních registrů dochází k odstranění duplicitních a neaktuálních údajů a k daleko vyšší míře efektivity všech souvisejících procesů. Jedná se o čtyři základní registry.“⁴¹

- Registr obyvatel (ROB) – správa ministerstva vnitra,
- Registr osob (ROS),
- Registr územní identifikace, adres a nemovitostí (RUIAN),
- Registr práv a povinností (RPP).

„Za kontrolu a především bezpečnost údajů v základních registrech je zodpovědný Úřad pro ochranu osobních údajů, do jehož gesce spadá i podstatný stavební kámen celého systému – převodník identifikátorů fyzických osob – tzv. ORG.“⁴²

Údaje z registrů obyvatel si obec musí vyžádat každý kalendářní měsíc v centrální evidenci obyvatel. Poskytují se údaje o změně trvalého pobytu, o úmrtí a narození. Takto získané údaje vkládá do své evidence obyvatel a aktualizuje si ji.

⁴⁰ Základní registry. *OSF MV ČR* [online]. Praha: Odbor strukturálních fondů Ministerstva vnitra České republiky [cit. 2020-04-23]. Dostupné z: <http://www.osf-mvcr.cz/zakladni-registry>

⁴¹ Tamtéž.

⁴² Tamtéž.

Registr územní identifikace adres a nemovitostí je spravován příslušným stavebním úřadem, který vkládá do tohoto registru nově přidělená čísla popisná po kolaudaci staveb. Registr má využití pro vytváření volebních okrsků a volebních seznamů.

Do registrů vstupujeme pomocí přihlašovacích hesel a je také nutné uvést, za jakým účelem do databází vstupujeme.

2.3 Komunikace ve vztahu úřad – právnická osoba

Právnické osoby zapsané v obchodním rejstříku mají povinnost podle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů mít zřízenou datovou schránku, tudíž komunikace musí přednostně probíhat touto cestou. V případě neúředních záležitostí může komunikace probíhat i méně formálně. Další možnosti komunikace:

- osobní kontakt,
- telefonický kontakt,
- poštovní korespondence,
- elektronická pošta (e-mail).

3 ANALÝZA SOUČASNÝCH RIZIK ZABEZPEČENÍ INFORMAČNÍHO SYSTÉMU OBCÍ S DŮRAZEM NA OSOBNÍ ÚDAJE

Obec je spravována zastupitelstvem. Dalšími orgány správy obce je rada obce, starosta, obecní úřad a zvláštní orgány obce. Obec si své záležitosti spravuje nezávisle v samostatné působnosti, v tomto případě do činnosti obce může zasahovat stát a kraj v případě porušení zákona. Do samostatné působnosti obce patří všechny záležitosti, které jsou v zájmu obce a především v zájmu občanů. Obec má za povinnost pečovat a uspokojovat potřeby svých občanů. Jedná se především o uspokojování potřeb týkajících se rozvoje zdraví, vzdělávání, dopravy, bydlení, informovanosti, ochrany přírody, veřejného pořádku. Obec má své katastrální území a také svůj majetek, se kterým hospodaří jako správný hospodář. Dispozice s obecním majetkem podléhá veřejné kontrole. Prodej, směna, pronájem musí být předem oznámena a zveřejněna na elektronické úřední desce po dobu nejméně 15 dní a občané se mohou k plánované dispozici vyjádřit.

Každý orgán obce má určeny v zákoně o obcích své pravomoci a povinnosti, které musí dodržovat. K plnění povinností zastupitelstvo vydá obecně závaznou vyhlášku či nařízení.

Dále má obec přenesenou působnost. Přenesenou působností rozumíme výkon státní správy, kterou stát část své státní moci přenáší na obec, a její rozsah je určen zákonem. Na přenesenou působnost dostává obec příslušný finanční příspěvek od státu. V České republice je uplatňován princip smíšeného modelu veřejné správy, jehož cílem je přiblížit státní správu občanům. V přenesené působnosti záleží na velikosti obce, v případě menších obcí je možno vydávat nařízení, vede evidenci obyvatel, větší obce s tzv. rozšířenou působností mají matriky, oprávnění vydávat občanské průkazy a cestovní pasy, stavební povolení aj.

Mimo zajištění výše uvedeného má také veřejná budova úřadu splňovat požadavky na bezpečnost pohybujících se občanů, zaměstnanců úřadu a zabezpečení informací. V dnešní době je slovo bezpečnost dosti používané vzhledem k nestabilní situaci v některých státech. K bezpečné situaci dnešní doby nepřispívá ani současná ekonomická krize, způsobená koronavirovou situací, provázená uzavíráním firem a ztrátou zaměstnání. Vše může mít za následek zvýšení agresivity a přibývání útoků psychicky narušených jedinců. „Veřejné budovy se už v dřívějších dobách stavěly tak, aby splňovaly určité stavební a bezpečnostní standardy a vzbuzovaly v návštěvnických pocit bezpečí. Proto jsou zpravidla pevné stavební

konstrukce, které mají široký rozsah odporové odolnosti, a stavební materiály jsou voleny s ohledem na potřebnou bezpečnost. Dodatečnou bezpečnost zajistí zdivo z plných pálených cihel min. tloušťka 300 mm (pevnost v tlaku více než 15 MPa) nebo beton se statickou výztuží s minimální tloušťkou 150 mm.⁴³

„Aby bylo možné nalézt kritická místa v zabezpečení a ochraně objektů místní samosprávy, je nutné zpracovat bezpečnostní analýzu. Pro tyto účely je například používána SWOT analýza pro formulování strategického plánu. Hodnotí silné a slabé stránky situace uvnitř společnosti, příležitosti a posuzuje hrozby okolí. Analýza rizika je potřebná pro zajištění bezpečnosti objektu veřejné správy. Pomáhá určit rizika, stanovit jejich velikost a na základě toho se rozhodnout v jakém pořadí řešit jejich redukci či úplnou eliminaci.“⁴⁴

SWOT analýza

Tabulka č. 1 SWOT analýza zabezpečení

Silné stránky	Slabé stránky
mechanické zabezpečení budovy rozmístění hasicích přístrojů vzdělávání zaměstnanců	zabezpečení budovy proti vstupu nepovolených osob zabezpečení oken a dveří instalace kamerového systému v budově instalace požárních hlásičů v budově rostoucí náklady
Příležitosti	Hrozby
instalace kamerového systému výměna okenních prvků zajištění skleněných výplní instalace požárních hlásičů dostatek kvalifikovaného personálu	volný pohyb osob po budově selhání lidského faktoru selhání techniky vandalismus loupežné přepadení v nočních hodinách

⁴³ UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2004. ISBN 80-7251-172-6.

⁴⁴ GERŽA, Michal. *Posouzení bezpečnosti a ochrany objektu Městského úřadu Kunovice*. Zlín, 2013. Bakalářské práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce doc. Ing. Miroslav Tomek, Ph.D.

Pro analýzu bezpečnostních rizik na obecním úřadě je možné využít i metodu PNH. „Zmiňovaná metoda patří mezi jednodušší nástroje pro hodnocení rizik. Jedná se o bodovou polokvantitativní metodu, kdy postupně bodujeme (hodnotíme) jednotlivé kroky metody. Tyto kroky jsou P – pravděpodobnost, N – následky a H – názor hodnotitele. Bodovou škálu si určujeme sami podle našich potřeb. Nejčastěji se boduje na stupnici od 1 do 5, popřípadě od 1 do 10. Až jsou jednotlivé kroky obodovány, vynásobíme je mezi sebou podle vzorce $R = P \times N \times H$. Získáme tak výsledek, který podle své hodnoty spadne do některé s kategorií, a my zjistíme, zdali je riziko přijatelné či nikoli a přijmeme nápravná opatření. Můžeme riziko buďto zmírnit na přijatelnou úroveň nebo ho odstranit úplně.“⁴⁵

Tabulka č. 2 Analýza PNH

P – pravděpodobnost vzniku a existence nebezpečí	
Minimální	1
Nepřavděpodobná	2
Pravděpodobná	3
Téměř jistá	4
Dlouhodobá	5

N – možné následky ohrožení	
Vandalismus	1
Loupežné přepadení v nočních hodinách	2
Selhání techniky	3
Volný pohyb osob po budově	4
Selhání lidského faktoru	5

H – názor hodnotitelů	
Téměř žádný vliv na bezpečnostní situaci	1
Nízký podíl na míře nebezpečí	2
Znatelný podíl vlivu na míře nebezpečí	3
Vysoký podíl vlivu na nebezpečné situaci	4
Velmi významný podíl vlivu na míře nebezpečí	5

⁴⁵ ZAHÁLKA, Jiří. *Analýza rizik v průmyslovém podniku*. Brno, 2012. Diplomová práce. Vysoké učení technické, Fakulta strojního inženýrství, Ústav výrobních strojů, systémů a robotiky. Vedoucí práce Ing. Luboš Kotek, Ph.D.

Míra rizika se v tomto případě počítá pomocí vzorce $R=P \times N \times H$.⁴⁶

Tabulka č. 3 Rizikový stupeň a míra rizika

Rizikový stupeň	R	Míra rizika
I.	> 100	Nepřijatelné riziko
II.	51 > 100	Nežádoucí riziko
III.	11 > 50	Mírné riziko
IV.	3 > 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

„Bodové rozpětí vyjadřuje naléhavost úkolů přijetí opatření ke snížení rizika a prioritu bezpečnostních opatření. Mělo by být obsaženo v plánu zvýšení úrovně bezpečnosti, jenž by měl být součástí vyhodnocení a dokumentace rizik. Při stanovení kategorie závažnosti vyhodnocených rizik je možné rozdělení do pěti rizikových stupňů (I. až V.) a celkové hodnocení míry rizika (R) je pak následující:

- Nepřijatelné riziko s katastrofickými důsledky, vyžadující okamžité zastavení činnosti, odstavení z provozu do doby realizace nezbytných opatření a nového vyhodnocení rizik. Práce nesmí být zahájena, nebo v ní nesmí být pokračováno, dokud se riziko nesníží.
- Nežádoucí riziko vyžadující urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnou úroveň. Na snížení rizika se musí přidělit potřebné zdroje.
- Mírné riziko, i když není nutnost opatření tak závažná jako u rizik kategorie II. Bezpečnostní opatření nutno zpravidla realizovat dle zpracovaného plánu podle rozhodnutí vedení podniku. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období. Je-li toto riziko spojeno se značnými nebezpečnými následky, musí se provést další zhodnocení, aby se přesněji stanovila pravděpodobnost vzniku úrazu, jako podklad pro stanovení potřeby dosažení zlepšení a snížení rizika.
- Akceptovatelné riziko, riziko přijatelné se souhlasem vedení. Je nutno zvážit náklady na případné řešení nebo zlepšení. V případě, že se nepodaří provést technická

⁴⁶ KOUDELKA, Ctirad a Václav VRÁNA. Rizika a jejich analýza. *VŠB* [online]. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, 2006 [cit. 2020-04-26]. Dostupné také z: <https://feil.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf>

bezpečnostní opatření ke snížení rizika, je třeba zavést vhodná opatření organizační. Většinou postačuje školení obsluhy, běžný dozor apod.

- Bezvýznamné riziko, není vyžadováno žádné zvláštní opatření. Nejedná se však o 100% bezpečnost, proto je nutno na existující riziko upozornit a uvést např. jaká organizační a výchovná opatření je třeba realizovat.⁴⁷

Způsob zajištění bezpečnosti malých úřadů dokazuje následující anketa. Dotazník s deseti otázkami ohledně zabezpečení obecního úřadu, byl odeslán 20 obcím s počtem do jednoho tisíce obyvatel. Dotazník vyplnilo 12 respondentů.

Tabulka č. 4 Dotazník pro obce

Vybavení prostoru obecního úřadu		ANO*	NE*
1.	Nachází se u vstupu do budovy kamerový systém?	2	10
2.	Je v prostorách obecního úřadu umístěn kamerový systém k ochraně a monitorování budovy?	1	11
3.	Jsou skleněné výplně zabezpečeny bezpečnostní fólií?	0	12
4.	Jsou vstupní dveře zabezpečeny bezpečnostním kováním a cylindrickou vložkou?	6	6
5.	Je v budově instalován elektronický poplašný systém proti neoprávněnému vstupu?	7	5
6.	Jsou v budově instalovány požární hlásiče?	3	9
7.	Jsou v budově instalovány hasicí přístroje?	12	0
8.	Jsou v budově uzamykatelné skříně?	12	0
9.	Je v budově umístěn trezor na ukládání peněžní hotovosti?	12	0
10.	Je v budově umístěn trezor na ukládání utajovaných dokumentů?	4	6

* Počet obcí

Z odevzdaných odpovědí vyplývá, že na dotazovaných úřadech se nachází pouze uzamykatelné skříně, do kterých pracovníci ukládají citlivé a utajované informace a na některých úřadech

⁴⁷ KOUDELKA, Ctirad a Václav VRÁNA. Rizika a jejich analýza. *VŠB* [online]. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, 2006 [cit. 2020-04-26]. Dostupné také z: <https://feil.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf>

malé trezory k ukládání finanční hotovosti. V případě požáru by mohly být použity hasicí přístroje a nanejvýš se vstupní dveře zamykají klíčem, který lze vyrobit na základě speciální karty.

3.1 Popis rizika a hodnocení rizik

Analýzou bezpečnosti organizace lze získat informace o stavu zranitelnosti, hrozeb a vytvoření komplexních protipatření vedoucích k celistvé ochraně organizace.

Z výše uvedeného vyplývá, že budovy malých obecních úřadů nejsou téměř vůbec zabezpečeny. Velká pozornost se věnuje spíše zabezpečení z hlediska úniku informací než samotnému zabezpečení budovy. Důvodem může být skutečnost, že v malé vesnici je velmi malá kriminalita a k útokům na nemovitosti obce nedochází tak často, spíše se řeší občasné útoky vandalů.

Po přijetí evropského nařízení GDPR musí mít každý subjekt zpracovávající osobní údaje povinnost ustanovit pověřence pro ochranu osobních údajů. V případě malých obcí se jedná o jednu osobu pro několik obcí. V této souvislosti došlo k rozšíření, úpravě a zpřesnění práv a povinností jednotlivých pracovníků na úřadech. Bylo nutno zpracovat a vydat soubor technických a organizačních opatření pro zpracování osobních údajů, které mají za cíl zajistit, že zpracování osobních údajů bude obcí, tedy správcem, prováděno v souladu s GDPR. Vydáním norem (směrnic) došlo k úpravě evidence a rozdělení klíčů od kanceláří, vchodů do budovy a také jiných objektů ve vlastnictví obce. O klíčích se vede samostatná evidence. Duplikáty klíčů jsou uloženy v uzamykatelné skříni. Další norma, která v souvislosti s nařízením vznikla, řeší ochranu osobních údajů při nakládání se spisovým materiálem. Norma nařizuje způsob, jakým se materiály ukládají do složek a šanonů. Ty se musí uložit do uzamykatelných skříněk, aby nedošlo ke zneužití nepovolanými osobami. K této normě je zpracována příloha, kde je určeno, který zaměstnanec pracuje s údaji souvisejícími s jeho prací a má k nim přístup. Je zde také určena podoba zpracování (listinná či počítačová), doba uložení a skartační a archivační znak.

Během činnosti obce může vzniknout podezření, že hrozí nebezpečí úniku osobních údajů či jiné porušení zabezpečení osobních údajů. Pokud taková situace nastane, je klasifikována jako bezpečnostní incident. Pokud je incident klasifikován dle zákona o ochraně osobních údajů, obec je povinna nahlásit situaci dozorovému úřadu.

„Dozorová činnost je základním posláním Úřadu pro ochranu osobních údajů. V souladu s čl. 51 odst. 1 nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů) ve spojení s § 50 zákona č. 110/2019 Sb., o zpracování osobních údajů, je Úřad ústředním správním úřadem pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem, jinými právními předpisy, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropské unie.“⁴⁸ Existují případy, kdy únik osobních údajů může představovat riziko pro práva a povinnosti fyzických osob, jejichž údaje byly zasaženy. Nemusí se jednat pouze o osobní údaje, ale také o informace či události s nimi spojené. V podobné situaci je nutné informovat i osoby, na které se toto riziko bezprostředně vztahuje.

⁴⁸ Dozorová a rozhodovací činnost. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-07-08]. Dostupné z: <https://www.uouu.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277>

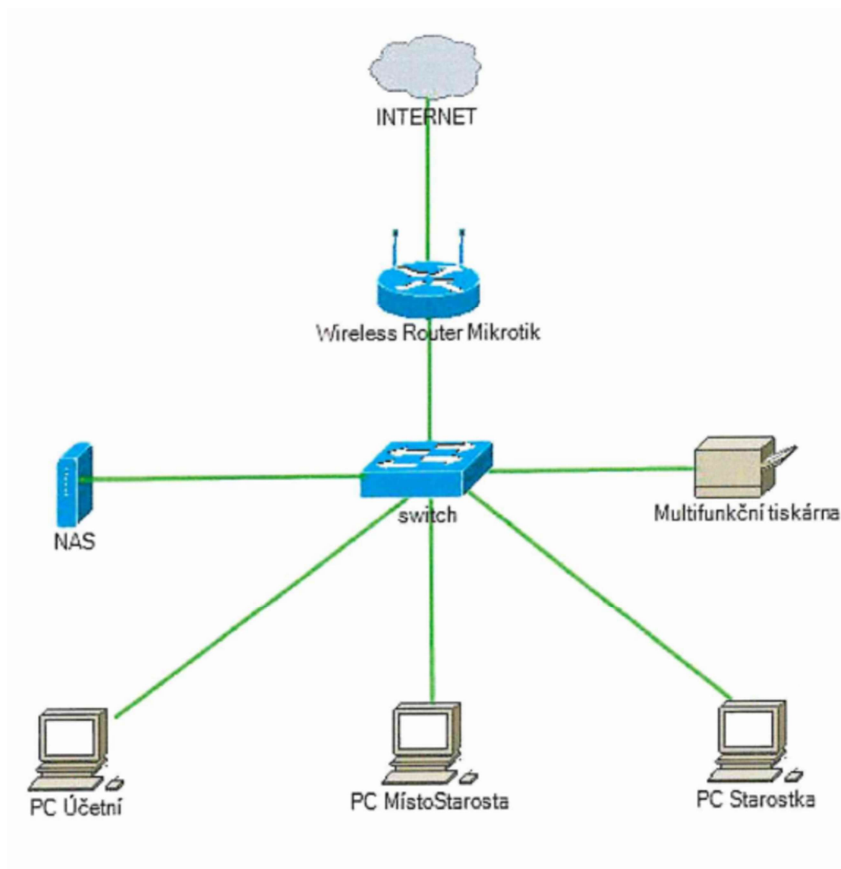
II. PRAKTICKÁ ČÁST

4 KRITICKÉ POSOUZENÍ AKTUALNÍHO STAVU INFORMAČNÍHO SYSTÉMU

Nedílnou součástí všech činností a povinností spojených s výkonem zastupitelů a pracovníků obce jsou informační systémy. Ke zhodnocení současného stavu a využití informačního systému společně s ochranou osobních údajů byla vybrána menší obec (dále v textu jako „obec“).

Ve zmíněné obci je evidováno 870 obyvatel. Dle statistik 80 % obcí v ČR má počet obyvatel do 1 000. Většina obcí má stejná nebo podobná zařízení.

Všichni administrativní pracovníci v obci ke své práci využívají počítač vybavený potřebným softwarem. Všechny počítače jsou napojeny na jednu tiskárnu, která obsahuje scanner a kopírku. Počítače jsou proti neoprávněnému využití opatřeny přístupovými hesly.



Obrázek č. 3 Síťové připojení v obci

Počítačová síť v obci je tvořena následujícími zařízeními:

- switch (přepínač),
- router,
- síťové úložiště (NAS),
- multifunkční tiskové zařízení,
- počítače.

Switch (přepínač) slouží k fyzickému propojení všech zařízení (ke každému zařízení vedené zvláštní kabel).

Router slouží k přidělování síťových adres, jednotlivým zařízením a zároveň jim umožňuje připojení k internetu, zajišťuje také provoz WiFi v rámci budovy úřadu obce a slouží i jako firewall, tzn., že chrání síť před útoky z internetu.

Síťové úložiště (NAS) slouží k zálohování dat z počítačů a zároveň poskytuje sdílené složky pro počítače, přes které se můžou data mezi uživateli vyměňovat.

Multifunkční tiskové zařízení slouží jako tiskárna pro všechny počítače a zároveň umožňuje skenování dokumentu buď na síťové úložiště, nebo na email.

Softwarové vybavení úřadu

Mezi softwarové vybavení jsou zařazovány všechny programy zpracovávající informace, které jsou používány při práci na počítači. V případě některých programů je možné použít výraz aplikace. Operačním systémem na obecním úřadě je Windows 10. Každý uživatel má své přístupové heslo. „Úkolem operačního systému je zajištění komunikace s okolím, tedy vytvoření rozhraní, jehož prostřednictvím uživatel ovládá počítač. Abychom mohli na počítači spouštět a pracovat s programy, musí operační systém zajišťovat jejich řízení i zpracování (správa procesů a operační paměti). Zajišťuje také správu souborů ukládaných na pevný disk, správu uživatelů, umožňuje připojení počítače do sítě a mnoho dalšího.“⁴⁹

ESET Ebdpoint antivirus zajišťuje PC monitoring a ochranu před viry a hrozbami. „Antivir je označení pro antivirový program, který má účinně zabraňovat a důsledně eliminovat výskyt škodlivého malwaru a dalších různých typů velmi nebezpečně zhoubných počítačových virů

⁴⁹ Operační systémy. *Jak na internet* [online]. 2020 [cit. 2020-04-24]. Dostupné z: <https://www.jaknainternet.cz/page/1757/operacni-systemy/>

a trojských koní. Mezi typickou činností antiviru patří i analýza došlých e-mailových zpráv a v případě hrozby rázně zasáhne a uchrání tak uživatele před krokem nákazy jeho dat v souborovém systému v počítači.⁵⁰

Firewall a ochrana sítě jsou od značky Windows. „Firewall v počítačové síti blokuje nebo povoluje navazované komunikace na základě předdefinovaných nebo dynamických pravidel a politik. Chrání zařízení, jež jsou zapojena za ním, před různými typy útoků, včetně těch, které umožní útočníkovi převzít kontrolu na zařízení. V překladu jde o ohnivzdornou stěnu, což je v IT světě analogie pro software nebo hardwarové zařízení, které filtruje příchozí i odchozí komunikaci do vnitřní sítě. Zjednodušeně si funkci můžeme představit jako strážce vstupu do pevnosti, které podle příkazů rozhodují o tom, koho pustí dovnitř a ven.“⁵¹

„Počítačový program je sada instrukcí, které provádí specifický kód, když je počítačem používán. Počítač vyžaduje, aby programy fungovaly, a obvykle provádí pokyny programu v centrální procesní jednotce. Počítačový program je obvykle napsán počítačovým programátorem v programovacím jazyce. Z programu ve své lidsky čitelné formě zdrojového kódu může kompilátor vytvořit strojový kód – formu tvořenou instrukcemi, které počítač může přímo spouštět. Alternativně může být počítačový program prováděn za pomoci tzv. interpretu. Část počítačového programu, který provádí dobře definovaný úkol, je známý jako algoritmus. Sbírkou počítačových programů, knihoven a souvisejících údajů je označována jako software. Počítačové programy mohou být rozděleny jako funkce do kategorií, jako je aplikační software nebo systémový software.“⁵²

Programy využívané na obecním úřadě jsou následující:

- KEO-W (program pro vedení účetnictví),
- KEO 4 (evidence pošty),
- KEOX (evidenční moduly a spisová služba),
- ALISUIS (odesílání dokumentů pro veřejnou správu).

Pro kancelářské běžné užívání jsou to zejména:

- MS Word,

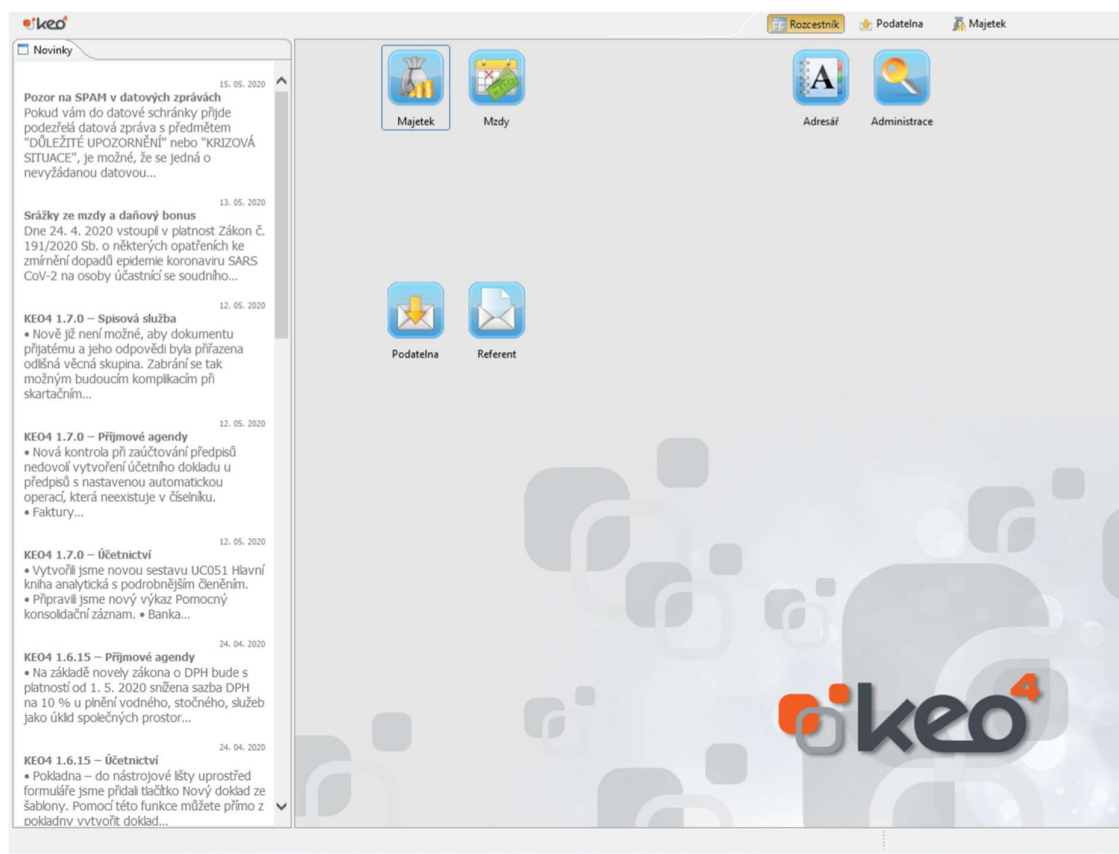
⁵⁰ Ochrana počítače proti virům. *Microsoft: Support service* [online]. Microsoft, 2020 [cit. 2020-08-04]. Dostupné z: <https://support.microsoft.com/cs-cz/help/17228/windows-protect-my-pc-from-viruses>

⁵¹ Firewall. *Esset* [online]. 2020 [cit. 2020-05-08]. Dostupné z: <https://www.eset.com/cz/firewall/>

⁵² Program. *IT Slovník* [online]. 2020 [cit. 2020-05-09]. Dostupné z: <https://it-slovník.cz/pojem/program>

- MS Excel,
- MS PowerPoint,
- MS Outlook (e-mailová komunikace),
- Acrobat reader (PDF),
- CODEXIS (Legislativní program).

Bezpečné používání programů, tak aby nedocházelo k unikání informací, je zajištěno heslem pro každého uživatele.



Obrázek č. 4 Pohled na hlavní stranu programu KEO⁵³

4.1 Účetnictví obcí

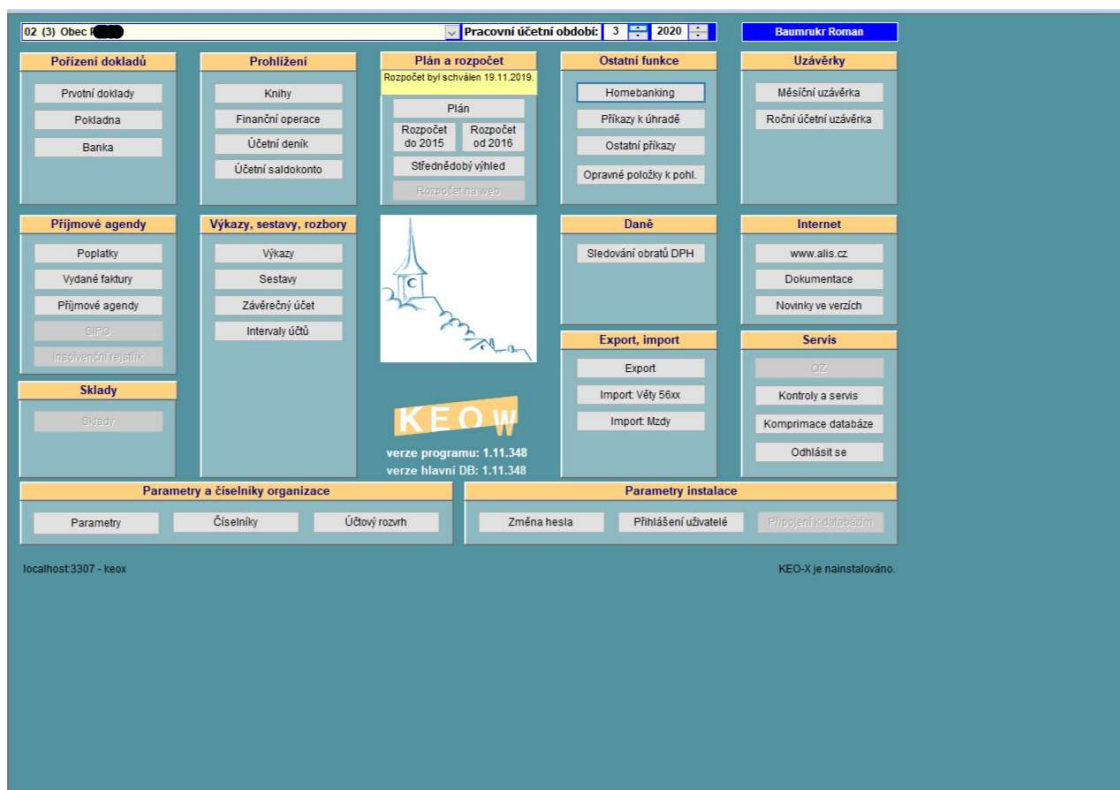
Nejpoužívanějším modulem je modul pro vedení účetnictví, což je nejrozsáhlejší agenda. „Program KEO-W Účetnictví se skládá z modulů Účetnictví (ve kterém je zahrnuto i výkaznictví, saldokonto a rozpočet), DPH, Homebanking, Fakturace, Poplatky / Příjmové

⁵³ ALIS spol. s.r.o. *KEO (-X, -W, 4)* [software]. 2004–2018 [cit. 2020-07-22]. Dostupné z: <http://www.alis.cz/cs>

agendy a Tisk složenek. Tyto moduly jsou navzájem propojené. Uživatel si může pořídit pouze ty moduly, které potřebuje. Data lze importovat do Microsoft Word a Microsoft Excel.“⁵⁴

Do knihy došlých faktur se zapisují všechny faktury, které se přijmou od dodavatelů. Zakládání faktur je o to jednodušší, že firmu, která fakturu vystavila, lze nalézt pomocí internetového připojení v registru ekonomických subjektů. Stačí jen zadat IČ a potvrdit výběr firmy. Poté může být faktura pomocí předvoleného zadání zaúčtována. V knize došlých faktur se automaticky generuje platební příkaz. Po schválení plateb určenými pracovníky lze příkaz odeslat do banky a po zadání jména a hesla lze platbu odeslat z účtu obce.

To funguje i opačným směrem, tedy po zaplacení transakcí v bance lze stáhnout výpis z účtu a spárovat se zadanými platbami. Tím se získá okamžitý přehled o tom, co je zapláceno a co na zaplacení čeká.



Obrázek č. 5 Přehled modulů v části účetnictví⁵⁵

⁵⁴ KANOVOVÁ, Lucie. *Analýza využití účetních programů v účetnictví obcí*. České Budějovice, 2013. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Ekonomická fakulta. Vedoucí práce Ing. Hana Hlaváčková.

⁵⁵ ALIS spol. s.r.o. *KEO (-X, -W, 4)* [software]. 2004–2018 [cit. 2020-07-22]. Dostupné z: <http://www.alis.cz/cs>

V tomto modulu lze přijímat a vydávat finance v hotovosti na obecním úřadě přes pokladnu. S účetnictvím jsou propojeny všechny ostatní moduly, protože jsou úzce provázány a všechny využívají zadané údaje.

„K programu KEO-W Účetnictví existuje uživatelská příručka. Tyto manuály se s každou aktualizací programu přepisují, aktualizují. Jsou dostupné nejen z internetových stránek firmy ALIS, ale i přímo z programu. V manuálu lze hledat pomocí klávesové kombinace Ctrl+F. K modulům Poplatky a Účetnictví jsou namluvena vizuální školení.“⁵⁶

Modul evidence obyvatel je jedenkrát měsíčně aktualizován tak, aby údaje souhlasily s centrálním registrem obyvatel. Co se týká obsahu osobních údajů, je evidence obyvatel nejrozsáhlejší. K této databázi jsou speciálně vytvořené přístupy, kterými se přihlašuje.

V systému zůstává po každém přístupu stopa a podle přístupových kódů lze identifikovat, kdo, který den a v jakém čase se do systému přihlásil a jaký k tomu měl důvod. Přihlašování a poskytování informací má své úrovně a pracovníci úřadů mají určené, které informace mohou získat. Při přihlášení „zakliknou“ důvod svého připojení a tyto údaje zde zůstanou uloženy.

V evidenci obyvatel jsou všechny citlivé údaje o každém z nás. Je možné získat jméno, příjmení, rodné číslo, adresu trvalého pobytu, rodinný stav, zda lidé mají omezení k právním úkonům, vazby na rodinné příslušníky a údaje o nich. Evidence obyvatel i matrika jsou evidence veřejně nepřístupné.

Pokud si požádá fyzická osoba o informace, lze je z hlediska zákona o ochraně osobních údajů poskytnout osobě starší 15 let, a to jen údaje o jeho osobě. K osobě blízké, kterou je otec, matka, prarodiče, sourozenec, dítě, vnuk, manžel nebo partner, se poskytují pouze údaje o úmrtí nebo soudním prohlášení za mrtvého nebo nezvěstného.

Obecní úřad, o jehož systém se tato práce opírá, je pouze ohlašovnou, tzn., že na úřadě v obci se nový občan přihlásí k trvalému pobytu. Tato obec nemá matriční úřad, a proto se zde nevydávají rodné listy a občanské průkazy. Oddávat na úřadě je možné pouze za účasti úředníka z obce, která má matriční úřad.

V evidenci obyvatel je identifikátorem rodné číslo. Podle tohoto čísla lze fyzickou osobu dohledat v mnoha registrech a evidencích. Z tohoto důvodu má zvláštní ochranu podle zákona o evidenci obyvatel a rodných čísel. Nepatří však do zvláštní kategorie (tzv. citlivých) údajů,

⁵⁶ KANOVOVÁ, Lucie. *Analýza využití účetních programů v účetnictví obcí*. České Budějovice, 2013. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Ekonomická fakulta. Vedoucí práce Ing. Hana Hlaváčková.

kteří mají přísnější režim podle článku 9 GDPR. Obec může rodná čísla občanů využívat, jestliže je rodné číslo zákonem stanovený identifikátor, např. občana v evidenci obyvatel, vlastníka v katastru nemovitostí, daňového subjektu podle daňového řádu apod. Případně i tam, kde to vyplývá ze zákonem stanovené působnosti správního úřadu.

Rodné číslo lze použít jako součást adresních údajů v případě úřední zásilky, kdy jde o přesnou identifikaci adresáta. Je-li rodné číslo zákonem stanoveným identifikátorem, je i jeho použití pro přesnou identifikaci adresáta úřední nebo soudní zásilky zákonné. Na poštovní zásilce přitom nejde o zveřejnění rodného čísla či data narození. S údaji na obálce se kromě odesílatele a adresáta seznamuje pouze doručovatel, který je vázán poštovním tajemstvím. Ten podle zákona o poštovních službách nesmí umožnit, aby se s údaji neoprávněně seznámila jiná osoba.

Pokud zákon nestanoví uvádění rodného čísla ve smlouvách, např. pracovních, kupních, nájemních, nemusí jeho nositel své rodné číslo ve smlouvě uvádět. Zaměstnavatel je oprávněn pro pracovně-právní účely získat rodné číslo z dostupných databází a podle zákona je může využívat. Stejná situace nastává při prodeji a koupi nemovitosti, kdy rodné číslo účastníků vkladového řízení – fyzických osob musí obsahovat návrh na zahájení vkladového řízení, který podáváme na katastrálním úřadě na zákonem stanoveném formuláři.

Podle zákona o evidenci obyvatel a rodných číslech je obec uživatelem těchto údajů, pokud je to nezbytné pro výkon její působnosti. I když je rodné číslo uvedeno jako zákonem stanovený identifikátor ve veřejných rejstřících, neznamená to, že každý může takto zveřejněné rodné číslo libovolně využívat. Neoprávněné nakládání s rodným číslem jiné fyzické osoby je přestupkem podle zákona o evidenci obyvatel a rodných číslech. Pokud se ho dopustí fyzická osoba, je projednáván jako přestupek, který projednávají v přenesené působnosti obecní úřady s rozšířenou působností podle místa pobytu obyvatele, který se jich dopustil. „Úpravu používání rodného čísla obsahuje zákon č. 133/2000 Sb. Podle § 13 odst. 9 je rodné číslo oprávněna užívat nebo rozhodovat o jeho využívání v mezích stanovených zákonem výlučně fyzická osoba, které bylo rodné číslo přiděleno (nebo její zákonný zástupce); jinak lze rodné číslo využívat jen v případech stanovených v § 13c tohoto zákona. Příklady oprávněného zpracování rodných čísel: ustanovení § 6 odst. 7 zákona č. 277/2009 Sb. a ustanovení § 37 odst. 2 věta první zákona č. 21/1992 Sb.“⁵⁷

⁵⁷ K rodným číslům. ÚOOÚ [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-04-26]. Dostupné z: <https://www.uoou.cz/k-rodny-m-cislum/ds-5091/archiv=0&p1=3938>

Pokud se prokáže neoprávněné využívání rodných čísel právnickou osobou, je to přestupek, který projednává Úřad pro ochranu osobních údajů.

4.2 Mzdy a personalistika

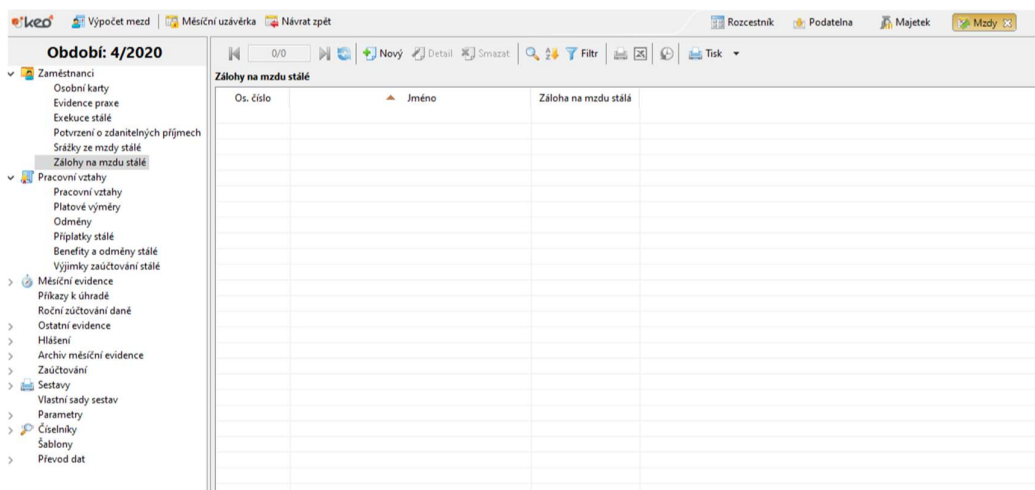
V tomto modulu jsou uloženy všechny údaje o zaměstnancích obecního úřadu a zastupitelích. Vytváří se zde pracovní smlouvy, smlouvy o pracovní činnosti a dohody o provedení práce. V personalistice se ukládají všechny údaje o dosavadním profesním životě zaměstnanců.

Při nástupu do práce zaměstnanci vyplňují dotazník, kde jsou dotázáni mimo jiné i na vzdělání a dosavadní praxi, předchozí zaměstnavatele a zdravotní pojišťovnu, u které jsou registrováni. Zaměstnanci jsou odměňováni podle nařízení vlády č. 341/2017 Sb., nařízení vlády o platových poměrech zaměstnanců ve veřejných službách a správě. Zaměstnanci jsou zařazeni do platové třídy podle druhu vykonávané činnosti. S tím může pomoci katalog prací, platový stupeň se určuje podle počtu let započitatelné praxe. Pokud je dosavadní praxe ve stejném oboru, započítá se celá, pokud je v jiném oboru, lze započíst podle druhu oboru až dvě třetiny odpracované doby.

Agenda mezd je spojená i s hlášením pro zdravotní pojišťovny, sociální správu a finanční úřad. S těmito institucemi je nutné smluvní ujednání o elektronickém přeposílání dat. Nastavením elektronické komunikace dochází ke snadnějšímu odesílání pravidelných měsíčních hlášení. Mzdy zaměstnanců i odměny zastupitelů jsou spojeny s nutnými odvody, které platí zaměstnanci a zastupitelé v podobě daní a zdravotního pojištění a zaměstnanci ještě sociální pojištění. Také zaměstnavatel odvádí těmto institucím nemalou finanční částku.

Zastupitelé jsou pro výkon své funkce uvolněni, tzn., že funkci vykonávají jako své hlavní zaměstnání nebo jsou pro výkon funkce neuvolněni a vykonávají ji ve svém volném čase. Za výkon funkcí jsou odměňováni dle přílohy k nařízení vlády č. 318/2017 Sb.

Díky propojení systému KEO a internetového bankovníctví lze platby po schválení a zadání příslušných hesel odeslat rovnou příjemcům.



Obrázek č. 6 Program KEO – část mzdová

4.3 Poplatky

Dalším modulem, kde se využívá osobních údajů, je poplatková agenda. Jsou zde ukládány všechny poplatky, které obec vybírá podle obecně závazných vyhlášek. Zastupitelstvo schvaluje vyhlášky k vybírání poplatků za svoz tuhého domovního odpadu, poplatek ze psů aj. Dále lze v tomto modulu pořizovat poplatky z uzavřených smluv, např. pronájem obecních bytů, pronájem nebytových prostor a uzavírání pachtovních smluv, na pronájem pozemků. Zde jsou využívány údaje z ROB. Avšak podle Úřadu pro ochranu osobních údajů se považuje zveřejnění nebo zpřístupnění osobních údajů dlužníků za nátlakové jednání, kterým je porušován článek 10 Listiny základních práv a svobod.

Zveřejnění osobních údajů v souvislosti s neuhrazením pohledávek je nepřipustné zasahování do soukromí.

4.4 Spisová služba

Je nejrozsáhlejší agendou. Obce zajišťují odbornou správu dokumentů, které vznikají z vlastní činnosti, popřípadě z činnosti předchůdců. Spisová služba zahrnuje příjem dokumentů, evidenci, rozdělování, oběh, vyřizování, vyhotovování, podepisování, odesílání, ukládání a vyřazování ve skartačním řízení, včetně kontroly těchto činností. Výkon spisové služby nelze omezit pouze na evidenci doručených dokumentů nebo pouze odeslaných.

Dokumenty, které vznikají činností obce, jsou všechny, které u obce vznikly, ale také dokumenty, které byly obci doručeny nebo jinak předány. Spisová služba není zřízena pouze

pro zbytečné zatěžování státní správy a samosprávy, ale naopak by měla být nástrojem, jehož smyslem je průhledná, průkazná a účelná činnost státní správy a samosprávy viditelná pro občana. Spisová služba zajišťuje průkaznost existence dokumentu v čase, a to se děje zaevidováním dokumentů v číselné posloupné řadě konkrétního roku a vazbou mezi podáním a vyřízením dokumentu.

Oblast spisové služby upravuje zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů ve znění pozdějších předpisů a jeho prováděcí vyhláška č. 259/2012 Sb. Pro snadnější orientaci a pochopení vypracovalo Ministerstvo vnitra ČR Metodické doporučení k činnosti územních samosprávných celků s názvem Povinnosti obcí stanovené zákonem č. 499/2004 Sb. Je to zákon o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, v oblasti výkonu spisové služby a archivnictví.

Pokud je spisová služba vedena v elektronické podobě, musí elektronický systém, v němž je provozována, splňovat požadavky Národního standardu pro elektronické systémy spisové služby, dané již výše zmíněnou vyhláškou. Obec zmiňovaná v diplomové práci využívá pro tuto činnost opět produkt firmy KEO.

Pro spisovou službu je to modul KEO X. Tento modul nám velice usnadňuje práci. Co se týká listin doručených fyzicky, tzn. klasickou poštou nebo osobně, naskenují se do programu a uloží dle času a data doručení. Dokumenty doručené datovou schránkou je možné stáhnout zadáním příkazu a vše se označí datem, časem a pořadovým číslem. Práce v tomto modulu není složitá.

V praxi na úřadě obce pracovník, mezi jehož pracovní činnosti patří příjem pošty, poštu přijme a zaregistruje. Dále označí dle skartačního řádu, jak dlouho se bude dokument evidovat (např. běžné písemnosti se archivují 5 let, dotační 10 let, mzdové trvale), jakého odvětví se pošta týká (např. nakládání s majetkem, stavební agenda aj.). Dále lze u jednotlivých listin zadat, kdo vyřídí odpověď a kdo může na jednotlivé listiny nahlížet. Do tohoto modulu má každý pracovník také své přístupové jméno a heslo. Je zde možné jednoduše zajistit odpověď, a to přímo v tomto programu, kde vybereme nabízenou šablonu, pomocí které může být odpověď vepsána. V šabloně je již předepsaný adresát, číslo jednací a věc, která je předmětem vyřízení, nebo je odpověď napsána v jiném programu, např. ve Wordu, a vložena do systému.

Pokud se odpověď odesílá datovou schránkou, připojí se elektronický podpis a odešle se na příslušnou adresu datové schránky. Odpověď o přijetí zprávy do datové schránky je doručena téměř okamžitě. Doručování datovou schránkou je bezpečné, rychlé a spolehlivé. Umožňuje okamžité doručení všech písemností, což je velká výhoda oproti klasickému

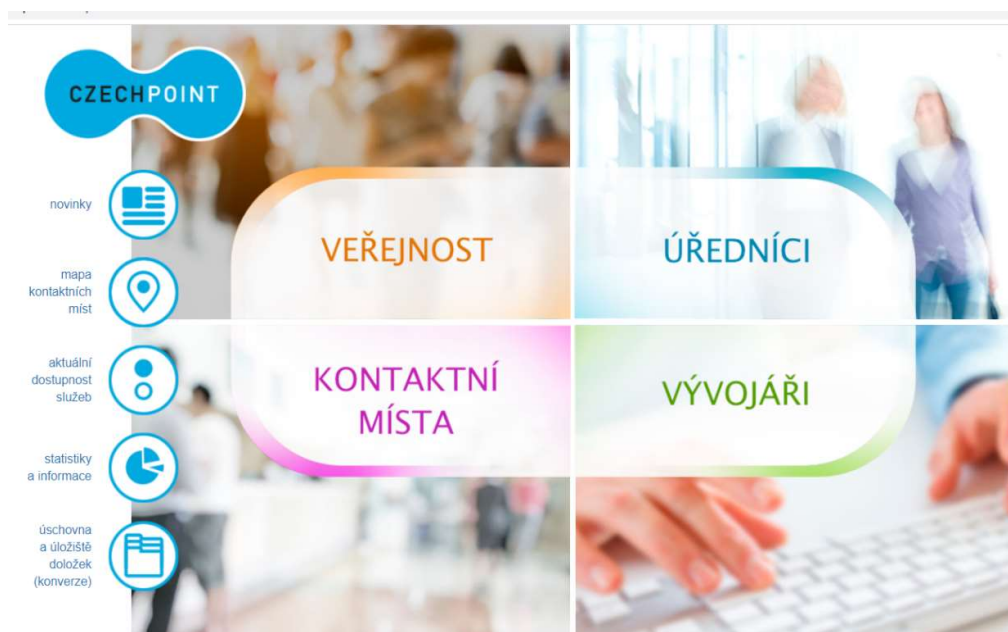
doručování poštou. Datové zprávy se uchovávají po dobu devadesáti dnů ode dne doručení přihlášením. Zpráva se považuje za doručenou okamžikem, kdy se oprávněný uživatel datové schránky s oprávněním číst zprávu do schránky přihlásí, bez ohledu na to, zda byla datová zpráva uživatelem přečtena nebo ne. Pokud se uživatel do datové schránky nepřihlásí, je zpráva považována za doručenou desátým dnem po jejím dodání do schránky, tzv. doručení fikcí. To znamená, že z právního hlediska se na datovou zprávu doručenou fikcí pohlíží jako na doručenou, i když se vůbec neotevře. Datové schránky fungují od roku 2009.

„**Datová schránka** – „datovka“ je definována jako elektronické úložiště, které je určeno k doručování dokumentů orgány veřejné moci, k provádění úkonů vůči orgánům veřejné moci a současně k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob. Jejich zřizovatelem a správcem je Ministerstvo vnitra.“⁵⁸

S funkcí spisové služby jsou spojeny dva velice důležité úkony, a to konverze dokumentů a zaručený elektronický podpis. Konverze dokumentů je vlastně úplné převedení elektronického dokumentu do listinné podoby a také z listinné podoby do elektronické. Dokument, který se konvertuje, má stejné právní účinky jako dokument, jehož předvedením výstup vznikl. Konverze zajišťuje shodu obsahů těchto dokumentů a připojí se doložka o provedení konverze. Konverze se provádí prostřednictvím internetové aplikace CZECH POINT.

Názvem **CZECH POINT** jsou označena místa na poštách a úřadech, která slouží jako asistované místo výkonu veřejné správy a umožňuje komunikaci se státem prostřednictvím jednoho místa tak, aby obíhala data, ne občan. Cílem projektu míst CZECH POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím právě tohoto místa, kde je možné získat a také ověřit data a dokumenty, získat informace o průběhu správních řízení aj.

⁵⁸ ŠVANDERLÍKOVÁ, Klára. Fikce doručení do datové schránky. *Právní prostor* [online]. 6. 2. 2018 [cit. 2020-04-26]. Dostupné z: <https://www.pravniprostor.cz/clanky/procesni-pravo/h-fikce-doruceni-do-datove-schranky>



Obrázek č. 7 Internetový portál Czech POINT⁵⁹

Pro elektronickou komunikaci je důležitý zaručený elektronický podpis. K vytvoření zaručeného elektronického podpisu je vlastně potřeba vydat kvalifikovaný certifikát, který se uloží na USB token, což je kvalifikovaný prostředek uznávaný v celé EU. O kvalifikovaný certifikát požádá zástupce právnické osoby prostřednictvím služeb České pošty pro své zaměstnance a pro sebe. Po vytvoření certifikátu a uložení na USB token je možné elektronicky podávat daňové přiznání, odesílat datové zprávy, komunikovat s českou správou sociálního zabezpečení, využívat elektronické formuláře e-podatelný aj.

K výkonu spisové služby má obec vytvořen **spisový řád**, kde jsou uvedena pravidla pro vedení spisové služby a obsahuje také skartační řád a spisový a skartační plán. Ve spisovém řádu má obec uvedeny podrobnosti týkající se nakládání s dokumenty a fyzické osoby, oprávněné k podepisování dokumentů a používání úředních razítek. Spisový a skartační plán jako součást spisového řádu je tvořený uspořádanými věcnými skupinami. U jednotlivých typů dokumentů rozříděných do věcných skupin jsou vyznačeny spisové znaky, skartační znaky a skartační lhůty. Skartačním znakem „A“ se označí písemnosti, které mají být trvale uloženy, jako jsou mzdové listy zaměstnanců, nebo se zařazují s návrhem na vybrání archiválií, těmi jsou např. zápisy z jednání zastupitelstva, rady, obecně závazné vyhlášky, výsledky voleb. Skartačním

⁵⁹ Czech POINT reg. č. CZ.1.06/1.1.00/03.05921. *Czech POINT* [online]. Praha: Ministerstvo vnitra České republiky, 2020 [cit. 2020-06-12]. Dostupné z: <https://www.czechpoint.cz/public/>

znakem „S“ se označují dokumenty bez trvalé hodnoty, které se vyřazují a skartují obvykle po pěti letech, např. faktury, dohody o provedení práce. Skartační lhůty vyplývají z právních předpisů.

V obci zmiňované v této diplomové práci probíhá skartační řízení následovně. Zástupce okresního archivu přijede na obecní úřad a vytipuje podle skartačního plánu dokumenty, které budou skartovány (označeny znakem „S“). A ty, které budou převezeny do okresního archivu, označí znakem „A“ jako „archiválie“, tzn. zápisy ze zastupitelstva, usnesení zastupitelstva, závěrečná vyúčtování, roční účetní závěrky, volební výsledky, výsledky referend, kroniky atd.). Odbornou archivní prohlídku dokumentů, spisů a úředních razítek navržených do skartačního řízení může pracovník zcela přehodnotit a k archivaci vybrat i jiné spisy. Všechny takové dokumenty se shromáždí na jednom místě. Dokumenty, které jsou vybrány k archivaci v okresním archivu, si zástupce převezme, udělá záznam o tom, které dokumenty byly odvezeny a budou zlikvidovány. Dokumenty, které mají být zlikvidovány, jsou převezeny do sběrných surovin, kde jsou za účasti pracovníka úřadu uloženy do beden. V bednách čekají na likvidaci. Bedny s materiály k likvidaci pracovník sběrných surovin dopraví na váhu. Pracovníkovi úřadu je vydáno potvrzení o váze dokumentů určených k likvidaci. Doklady jsou poté zlikvidovány ve spalovně.

Povinnosti spojené s řádným vyřazováním dokumentů ve skartačním nebo mimo skartační řízení (povinnost „uchovat dokumenty a umožnit výběr“), která je adresována původcům, tzn. nejenom obcím, ale i dalším subjektům podle § 3 odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě, není nikterak v rozporu s Nařízením Evropského parlamentu a Rady EU GDPR. Archivy jsou oprávněny ukládat trvale archiválie, včetně archiválií obsahujících osobní údaje žijících osob, což vyplývá i z čl. 17 a čl. 89 GDPR.

Dokumenty a spisy s osobními údaji, vybrané v procesu skartačního řízení nebo při výběru mimo skartační řízení za archiválie, lze bez jakéhokoli rizika uložit ve veřejném archivu. Tímto krokem přechází správa a odpovědnost na archiv. Další činností obce jsou jednání zastupitelstva a z jeho činnosti vyplývají další povinnosti.

4.5 Zveřejňování dokumentů z jednání orgánů obce

Dle platného zákona o obcích č. 128/2000 Sb., jednání zastupitelstva musí být minimálně jedenkrát za tři měsíce a je veřejně přístupné. Zákon nestanovuje povinnost zveřejňovat zápisy nebo usnesení z jednání zastupitelstva. Obce mohou zápisy a usnesení zveřejňovat dobrovolně.

Obec zveřejňuje usnesení z jednání zastupitelstva na webových stránkách obce. Pro zveřejňování je charakteristické, že se s uvedenou informací může seznámit v podstatě kdokoliv. Proto je důležité v tomto případě provést anonymizaci, tj. znečitelnění osobních údajů fyzických osob, které se ve zveřejňovaných dokumentech vyskytují. V tomto případě je třeba zvážit, a to vždy vzhledem k okolnostem, zda je důležité seznámit veřejnost s identitou dotčené osoby. Je třeba mít na paměti, že účelem zveřejnění osobních údajů je zpřístupnit informaci o činnosti obce, nikoli informovat o soukromí, osobním životě a poměrech fyzických osob. Jiný případ bude, když si občan přeje do dokumentů nahlížet nebo si požádá o informace podle **zákona o svobodném přístupu k informacím**. Zákon o obcích opravňuje občana obce nahlížet do uvedených dokumentů a pořizovat si z nich výpisy, aniž by stanovil jakákoliv obsahová omezení. Není možné údaje anonymizovat. Občan má právo na neomezený přístup k uvedeným dokumentům včetně osobních údajů.

The infographic is divided into two columns: 'Datová schránka' (Data Mailbox) and 'JIP' (Internal Information System). Each column contains a series of steps with icons and text instructions.

Datová schránka:

- Step 1:** K přihlášení použijte přihlašovací údaje vašeho zaměstnavatele. Pozn. přihlášením do této aplikace nevstupujete přímo do datové schránky. (Icon: Padlock)
- Step 2:** Nahrajte soubor (třeba i v obrázkovém formátu) a po úpravě jej aplikace sama převede do strojově čitelného formátu. (Icon: Document)
- Step 3:** Proveďte začernění osobních údajů a případně i obchodního tajemství. (Icon: Eraser)
- Step 4:** Soubor se uloží ve formátu pdf s textovou vrstvou. (Icon: PDF)
- Step 5:** K dokumentu můžete doplnit metadata. (Icon: Dashed circle)
- Step 6:** Výsledný soubor a vyplněná metadata aplikace přepoše do Registru smluv – přímo z tohoto prostředí. (Icon: Envelope)

JIP:

- Step 1:** K přihlášení použijte přihlašovací údaje do JIP – musíte mít v JIP zřízený účet (pokud nemáte, obraťte se na administrátora vaší organizace). Pozn.: proces zřízení účtu v JIP je popsán v dokumentaci Czech POINT. (Icon: Padlock)
- Step 2:** Nahrajte soubor (třeba i v obrázkovém formátu) a po úpravě jej aplikace sama převede do strojově čitelného formátu. (Icon: Document)
- Step 3:** K přihlášení použijte přihlašovací údaje do JIP – musíte mít v JIP zřízený účet (pokud nemáte, obraťte se na administrátora vaší organizace). Pozn.: proces zřízení účtu v JIP je popsán v dokumentaci Czech POINT. (Icon: Eraser)
- Step 4:** Soubor se uloží ve formátu pdf s textovou vrstvou. (Icon: PDF)
- Step 5:** Výsledný soubor použijte jako přílohu při zveřejňování nebo opravě smluv prostřednictvím publikačních formulářů Registru smluv dostupných z Portálu veřejné správy – nebo využijte spisovou službu. (Icon: Star)

Obrázek č. 8 Návod k anonymizaci dokumentů⁶⁰

⁶⁰ Nástroj k anonymizaci dokumentů. *Portál veřejné správy* [online]. Praha: Ministerstvo vnitra České republiky, 2018 [cit. 2020-06-12]. Dostupné z: <https://anonymizace.gov.cz/crossroad/>

[REDACTED]

[REDACTED]

Zlín 18. 12. 2019

Žádost o poskytnutí informací ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Žadatel: [REDACTED]

zastoupená [REDACTED]

Ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, Vás žádám o poskytnutí následujících informací:

- 1) znaleckého posudku č. 7500-070/19 ze dne 2. 6. 2019 znalce Ing. Pavla Titla,
- 2) znaleckého posudku č. 7524-094/19 ze dne 17. 7. 2019 znalce Ing. Pavla Titla.

Oba výše uvedené znalecké posudky byly podkladem pro určení ceny pozemků směřovaných na základě směnné smlouvy mezi obcí Podolí a [REDACTED] uzavřené dne 13. 9. 2019.

Informaci žádám poskytnout v písemné formě a zaslat elektronicky na výše uvedenou e-mailovou adresu.

Za poskytnutí informace předem děkuji.

S pozdravem

[REDACTED]

Obrázek č. 9 Příklad anonymizovaného dokumentu⁶¹

V zápisech nebo v usneseních z obecních jednání ustupuje ochrana soukromí zastupitelů veřejnému zájmu. Osobní údaje členů zastupitelstva nebo jiných osob, které zastávají funkci veřejnou, mohou být zveřejněny. Týká se to i osob z řad občanů obce, kteří se aktivně zajímají o dění v obci a vystoupí na zasedání zastupitelstva ve veřejném zájmu, jde-li o dodavatele veřejné zakázky a zaměstnance obce.

Dále není potřeba anonymizovat osobní údaje, které jsou zveřejněny např. v katastru nemovitostí, obchodním rejstříku, registru smluv, atd. „V uvedených případech anonymizace osobních údajů postrádá smysl. Obec také musí při zveřejňování osobních údajů ve výše uvedených případech obzvláště zvažovat rozsah osobních údajů s ohledem na princip

⁶¹ Informace poskytnuté dle zákona č. 106/1999 Sb. *Obec Podolí* [online]. Podolí u Uherského Hradiště, 2020 [cit. 2020-06-12]. Dostupné z: <http://www.obecpodoli.cz/dokumenty/poskytnute-informace/000168.pdf>

proporcionality. Princip proporcionality je vlastně posouzení přiměřenosti jeho použití v praxi, zvažuje se zejména při střetu práva na ochranu soukromí s právem na svobodný přístup k informacím.⁶² Zmínku o principu proporcionality můžeme nalézt v Listině základních práv EU, která ve svém čl. 52 odst. 1 říká, že: „každé omezení v uplatňování práv a svobod uznaných touto Listinou musí být stanoveno zákonem a musí být přitom chráněna jejich podstata. V souladu se zásadou proporcionality lze omezení uplatnit jen tehdy, jsou-li nezbytná a odpovídají-li účelům, sledujícím obecný zájem uznaný Unií nebo potřebě chránit práva a svobody druhých.“⁶³

V práci obce se nejčastěji do střetu dostává **právo na ochranu soukromí**⁶⁴, které zahrnuje i právo na ochranu osobních údajů a právo na svobodný přístup k informacím. V tomto případě je nutné provést test proporcionality. V rámci tohoto testu se řeší kolize práva na ochranu osobních údajů s právem na informace. Při testu proporcionality je třeba, aby povinný subjekt posoudil a provedl:

- Nultý krok testu – je potřeba uvážit, zda omezení práva sleduje legitimní cíl. Nelze omezit právo na informace ani ochranu soukromí z jiného důvodu než připouští zákon (např. odmítnutí poskytnutí informace z důvodu, že to možná ukazuje GDPR, ač třeba nejde o osobní údaje, nebo naopak zveřejnit citlivé údaje jen pro účely něčí skandalizace, i když je zřejmé, že nesmí být zveřejněny).
- První krok testu – vhodnost – je daný prostředek způsobilý dosáhnout požadovaného cíle? V tomto případě, zda poskytnutí požadovaných osobních údajů odpovídá účelu práva na informace a zda je vůbec způsobilé jej naplnit. Účelem práva na informace je veřejná kontrola postupů obce.
- Druhý krok testu – potřebnost – jde tohoto cíle dosáhnout jiným způsobem? Pokud se splní předešlé kroky, posuzuje se, zda výše uvedeného cíle, tzn. účelu žádosti, nelze dosáhnout jiným způsobem. Například poskytnout požadované písemnosti a začernit osobní údaje nebo osobní údaje ochránit tzv. **pseudonymizací**. „Pseudonymizace osobních údajů je proces skrytí identity, jehož účelem je mít možnost sbírat další údaje

⁶² KAUFNER, Jiří, ed. Správa osobních údajů v praxi obcí a měst. *SMO ČR* [online]. Praha: Svaz měst a obcí České republiky, 2020 [cit. 2020-06-12]. ISBN 978-80-88375-07-4. Dostupné také z: <https://www.smocr.cz/Shared/Clanky/8403/e-sprava-osobnich-udaju-v-praxi-obci-a-mest.PDF>

⁶³ Listina základních lidských práv Evropské unie. *EUR-Lex* [online]. Štrasburk, 2012 [cit. 2020-04-26]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:12012P/TXT>

⁶⁴ Chraňme si zákon na ochranu soukromí. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-08-04]. Dostupné z: <https://www.uouu.cz/chranme-si-zakon-na-ochranu-soukromi/ds-2469>

týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. Údaje kódované pomocí klíče jsou klasickým příkladem pseudonymizace. Informace se týkají jednotlivců, kteří jsou označeni kódem, přičemž klíč spojující kódy s běžnými identifikátory těchto jednotlivců (jméno, datum narození, adresa apod.) se uchovává odděleně. Pseudonymizované osobní údaje nicméně nejsou anonymizovanými údaji, proto se na ně stále vztahuje GDPR.⁶⁵

V následujícím příkladu je v tabulce č. 6 uveden příklad pseudonymizace osobních informací uvedených v tabulce č. 5, ve zkratce jsou konkrétní data nahrazena jiným identifikátorem (ID). Veřejně dostupný bude tak pouze nic nevyzrazující identifikátor.

Tabulka č. 5 Ilustrační osobní informace

Jméno a příjmení	Datum narození	Email
Jana Rýpalová	1. 4. 2000	jana@centrum.cz
Pavel Nebeský	2. 8. 1980	nebesa@gmail.com

Tabulka č. 6 Pseudonymizace osobních informací

Jméno a příjmení	Datum narození	Email	ID
Jana Rýpalová	1. 4. 2000	jana@centrum.cz	1
Pavel Nebeský	2. 8. 1980	nebesa@gmail.com	2

Definice podle Úřadu pro ochranu osobních údajů: „Pseudonymizace je definována v Obecném nařízení jako zpracování osobních údajů takovou formou, že nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací. Tyto dodatečné informace musí být z principu oddělené od zbytku informací o fyzické osobě a musí být technicky a organizačně zabezpečené. Využití pseudonymizace snižuje „riziko zpracování“. Je tedy velice vhodným nástrojem pro široké skupiny správců osobních údajů, kteří tímto sníží míru své odpovědnosti. Přímou v Obecném nařízení je pseudonymizace zmíněna jako vhodné technické

⁶⁵ Pseudonymizace osobních údajů. *GDPR* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-04-26]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/>

a organizační opatření pro zabezpečení osobních údajů.“⁶⁶ Tohoto způsobu lze využít, např. jde-li o žádost sdělení výše platů úředních osob. Žadatel dostane informace bez konkrétních jmen.

- Třetí krok testu – přiměřenost v užším smyslu – porovnání závažnosti obou v kolizi stojících základních práv. Přiměřenost poskytnutí informací si lze uvést na příkladu, kdy občan požádá o sdělení údajů o zdravotním stavu starostky obce z jejího personálního spisu, v tomto případě přednost dostane ochrana soukromí. Naproti tomu si občan požádá o potvrzení nebo vyvrácení domněnky, zda účetní obce je v příbuzenském vztahu se starostou, což je relevantní z hlediska veřejné kontroly, účelu žádosti o informace nelze dosáhnout jinak, a i když jde o soukromí starosty a účetní, převažuje zde veřejný zájem na kontrole činnosti obce (např. zda starosta či zastupitelé nezaměstnávají své příbuzné, byť mají potřebnou kvalifikaci).

Vždy je nutné zvážit, jakou informaci a osobní údaje tazatel požaduje a posoudit individuálně okolnosti každého případu. Posuzováním dojde obec k závěru, které právo bude upřednostněno a které naopak upozaděno. V případech, kdy povinnost poskytnout, či neposkytnout vyplývá přímo ze zákona, není potřeba složitých úvah. Test se použije především v případech, kde zákon jasné vodítko nedává.

4.6 Zveřejňování informací na úřední desce obce

Při zveřejňování informací na úřední desce kamenné i elektronické rozlišujeme, zda je zveřejňování povinné, či nepovinné. Obec povinně zveřejňuje informace o konání zasedání zastupitelstva, vydané obecně závazné vyhlášky, rozpočty, veřejnoprávní smlouvy, dle správního řádu lze prostřednictvím úřední desky doručit písemnosti. V případě, že obec doručuje písemnost veřejnou vyhláškou z vlastního rozhodnutí a ta obsahuje citlivé údaje ze soukromí občana, je vhodné zveřejnit pouze oznámení o možnosti převzít písemnost se základními identifikačními údaji občana a nezveřejňovat celou písemnost. Tu si vyzvedne ve stanoveném čase v kanceláři obecního úřadu. Kde je však dána zákonná povinnost obce osobní údaje zveřejnit, mohou být zveřejněny v plném rozsahu.

Obec musí také vydávat dokumenty, které jí v rámci své činnosti zasílají jiné orgány veřejné správy, protože jim to ukládá zvláštní právní předpis. V těchto případech nese odpovědnost za dodržování nařízení GDPR a dalších předpisů v ochraně osobních údajů orgán, který danou

⁶⁶ Slovníček nejdůležitějších pojmů. ÚOOÚ [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-04-26]. Dostupné z: <https://www.uouu.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617/archiv=0&p1=3938>

písemnost k vyvěšení zaslal obecnímu úřadu. Ten už nemůže obsah písemnosti měnit. Pouze ji zveřejní na své úřední desce po dobu, kterou uvedl zasílající úřad. Po uplynutí doby vyvěšení písemnost z úřední desky sejme, označí na ní dobu, po kterou byla vyvěšena, a odešle orgánu veřejné moci, který ji k vyvěšení zaslal.

Dalším druhem uveřejňovaných informací jsou majetkoprávní transakce. Při zveřejňování usnesení zastupitelstva obce, např. směna obecního pozemku, darování a prodej, platí stejné principy ochrany osobních údajů, jako u jiných informací o činnosti obce. V tomto případě jsou zveřejnitelné základní osobní údaje v rozsahu jména a příjmení, roku narození, popř. obce, v níž má dotyčná osoba bydliště. Z hlediska sledovaného účelu není potřeba zveřejňování detailnějších osobních údajů. Zpřístupnění dalších osobních údajů by neobstálo v rámci testu proporcionality.

Aby zastupitelstvo obce mohlo disponovat s obecním majetkem, např. prodej, směna, pronájem, pacht, výpůjčka, výpros a darování, je potřeba tento úkon schválit. Tomu musí předcházet oznámení dispozice s tímto majetkem a zveřejnění na úřední desce obce po dobu minimálně 15 dní. K záměru se mohou v určené době vyjadřovat všichni občané, uplatnit vlastní návrhy, nabídky a připomínky. V oznámení záměru musí být zamýšlená dispozice a označená nemovitá věc, která se označí údaji podle zákona o katastru nemovitostí (parcelní číslo a označení katastrálního území). Uvedení bližších údajů o záměru a smluvních podmínkách není povinností obce.

Jiné je to u tzv. adresného záměru, v němž obec deklaruje vůli dispozice vůči předem vytipovanému zájemci. Pokud obec zveřejní adresný záměr, osobní údaje dotčené osoby může zveřejnit pouze s jejím souhlasem. Pokud dotčená osoba nedá souhlas se zveřejněním osobních údajů, uvede se jen obecný popis věci bez informací o konkrétní osobě, anebo je nutné osobní údaje u vytipovaného zájemce anonymizovat.

Obce při své činnosti uzavírají nejrůznější druhy smluv, jako jsou kupní, nájemní, pachtovní, smlouvy o dílo aj., dále vystavují objednávky a proplácejí faktury. Všechny tyto dokumenty obsahují osobní údaje, které podléhají ochraně osobních údajů dle nařízení GDPR. Smlouvy musí povinné subjekty zveřejňovat podle zákona č. 340/2015 Sb., o registru smluv. Výjimku ze zveřejňování smluv v registru mají dle § 3 písmene k) obce, které nevykonávají rozšířenou působnost. Obce s rozšířenou působností jsou ty, které mají matriční úřad.

Opačná situace nastává při plnění zákona č. 134/2016 Sb., o veřejných zakázkách. Dle tohoto zákona si obec vytvoří účet u některého poskytovatele této služby, např. Profil zadavatele,

Vhodné zveřejnění, E-zakázky.cz, E-ZAKMZE aj. Na některém z těchto portálů má obec povinnost zveřejnit smlouvu uzavřenou s vyšší hodnotou než 500 000 Kč bez DPH, uvedou se také dodatky a všechny přílohy. Cílem zveřejňování je kontrola hospodaření státní správy s veřejnými penězi. Obce mohou nakupovat zboží, služby, objednávat stavební práce, v těchto situacích vystupují jako zadavatel veřejné zakázky. Na ni musí orgány státní správy vybrat dodavatele na základě veřejného zadávacího řízení, pokud předpokládaná finanční hodnota dosáhne na dodávky nebo služby 2 000 000 Kč bez DPH nebo 6 000 000 Kč bez DPH na stavební práce. Předpokládaná hodnota zakázky zahrnuje všechna plnění, tvoří jeden funkční celek.

Zadavatel nesmí zakázku rozdělit, tím by mohlo dojít ke snížení předpokládané hodnoty a vyhnul by se přísnější zákonné regulaci pro zadávací řízení. Obec musí zakázku zveřejnit na některém z internetových portálů a komunikovat pouze elektronicky. Všechny firmy, které se chtějí o zakázku ucházet, musí splnit podmínky určené zadavatelem. Ty jsou zveřejněny na portále společně s rozpočtem, kde jsou předvyplněny údaje o stavbě, množství materiálu, popsány práce, které budou probíhat. Dodavatel doplní ceny do tzv. slepého rozpočtu. V zadávacích podmínkách jsou kromě rozpočtů také záruční podmínky. Bývá požadována odborná způsobilost firmy k zadávaným odborným pracím, která se dokládá patřičným osvědčením. Může být také požadováno dokladování realizace staveb za určitou hodnotu, např. zkušenost s výstavbou silničních staveb nad částku 6 000 000 Kč, výsadbou zeleně nad 900 000 Kč aj. Zadavatel také zveřejní návrhy smlouvy o dílo, kterou zadavatel a dodavatel po skončení výběrového řízení podepíše. Před podpisem zasedne výběrová komise, která zkontroluje, zda dodavatelská firma předložila všechny požadované materiály, nacenila všechny položky rozpočtu atd. Doporučí zastupitelstvu ke schválení vybranou firmu. Podle zákona o zadávání veřejných zakázek je možné rozhodnout při výběru dodavatele dle různých kritérií, jako je kvalita odvedené práce, reference firmy nebo cena. Praxe je však úplně jiná. Ve všech případech rozhoduje pouze nejnižší cena.

Výběr dodavatele s dobrými referencemi, případně zkušenostmi z předchozích zakázek nebo doporučení od jiných realizátorů staveb by mohlo být považováno za neoprávněné zvýhodnění a zakládalo by na spekulaci o zvýhodňování za účelem osobního prospěchu. Pokud zakázka nedosáhne zadávacích limitů, jedná se o tzv. zakázku malého rozsahu. Pro tyto zakázky neplatí tak přísná pravidla. Při zadávání lze přímo oslovit libovolný počet firem, které se poptávanými pracemi zabývají. Všechny však musí dostat stejné zadávací podmínky a také se předkládá

smlouva, kde je vše, co zadavatel od dodavatele prací poptává. Ve smlouvě je především uvedeno datum zahájení a ukončení prací, podmínky, za jakých budou probíhat, např. v případě prací spojených s budovou školy je možné určit, že se uskuteční v odpoledních hodinách po skončení vyučování. Dále jsou ve smlouvě sjednány podmínky platby za odvedenou práci, zda práce budou fakturovány průběžně nebo po skončení díla, zajištění bezpečnosti na staveništi. Dodavatel prací musí mít uzavřeny pojistné smlouvy, které předkládá atd. V době elektronizace veřejné správy vznikl projekt Národního elektronického nástroje (NEN). Byl součástí projektu NIPEZ, který provozuje Ministerstvo pro místní rozvoj. NEN byl financován ze zdrojů EU jako projekt Národní infrastruktura pro elektronické zadávání veřejných zakázek. Certifikaci na shodu se zákonem získal v roce 2017. Je určen zejména pro zadavatele, kteří nechtějí investovat do vlastního řešení elektronického nástroje a zároveň chtějí využít nástroj garantovaný státem. Centrální orgány státní správy mají povinnost NEN využívat jako elektronické tržiště od roku 2018. Ostatní zadavatelé, města a obce jej mohou využívat dobrovolně. I když se jedná o zakázky malého rozsahu, musí zadavatel dodržet **základní zásady zákona o zadávání veřejných zakázek (ZZVZ)**.

- **Zásada transparentnosti** – zadavatel musí předem jasně stanovit kritéria výběru a postupovat tak, aby nevznikla pochybnost o objektivním výběru vítězné nabídky.
- **Zásada rovného zacházení** – zadavatel stanoví stejné podmínky všem potenciálním dodavatelům, tedy možnost přístupu k veřejné zakázce a možnost úspěchu ve výběrovém řízení je dána všem bez rozdílu.
- **Zásada zákazu diskriminace** – zadavatel nesmí neoprávněně zvýhodnit nebo znevýhodnit některého ze zájemců oproti ostatním, všichni mají stejnou příležitost zakázku získat.
- **Zásada přiměřenosti** – zadavatel nastaví parametry zadávacího řízení tak, aby byly přiměřené charakteru či předmětu veřejné zakázky (přiměřené požadavky na kvalifikaci, přiměřené zadávací podmínky, lhůty, smluvní podmínky).

4.7 Registr smluv

V registru smluv jsou evidovány především smlouvy o dílo, které se zveřejňují na základě zákona o registru smluv 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv. Některé obce v rámci zajištění vyšší míry transparentnosti a informování svých občanů o činnosti obce zveřejňují smlouvy, objednávky a

faktury dobrovolně. I v tomto případě v rámci ochrany osobních údajů je nutné osobní údaje anonymizovat. Obec, kterou zmiňujeme v této práci, má právě v rámci zvýšení transparentnosti a informování na webových stránkách odkaz na tzv. transparentní bankovní účet. Široká veřejnost, která si může prohlédnout webové stránky obce, se může v rámci internetového bankovníctví podívat na běžný účet obce vedený u Komerční banky a nahlížet na její příjmy a výdaje realizované na tomto účtu. I v tomto případě dochází k anonymizování osobních údajů, především při převodu finančních částek na účty zaměstnanců.

The screenshot shows a web browser window with two tabs: 'Povinné informace' and 'Komerční banka'. The main page is for 'PODOLÍ u Uherského Hradiště'. A red arrow points to a browser window titled 'Komerční banka' which displays a table of transactions. Below the table, a link 'Transparentní účet' is circled in red. To the right, there is a section for 'Povinné informace' with a list of details.

Datum zahájení	Připsáno/odepsáno (v měně úřtu)	Variabilní / Konstantní / Specifický symbol	Název a číslo protičtu 7práva pro příjemce
27. 4. 2020	- 1 613,00 CZK	1406017541 / — / —	E.ON ENERGIE, A.S. (19- CDCHOZI ÚHRADA
23. 4. 2020	2 500,00 CZK	193 / — / —	PRÍCHOZI ÚHRADA
22. 4. 2020	7 720,27 CZK	291242 / 4146 / —	FU pro ZLín (1650- PRÍCHOZI ÚHRADA
22. 4. 2020	- 100,30 CZK	291242 / 3552 / 7256235100	CDCHOZI ÚHRADA příspěvek na pens.přijímců

Poplatky
Územní plánování a strategický rozvoj
Informace poskytnuté dle zákona č. 106/1999Sb.
Transparentní účet

Povinné informace
Povinné zveřejňované informace podle vyhlášky č. 442/2009, která stanoví strukturu informací zveřejňovaných o povinném subjektu dle § 2 odst. 1 a z zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

- Název**
Obec Podolí
- Děvod a způsob založení**
Obec PODOLÍ (dříve jen obec) vznikla jako územní samosprávná jednotka v souladu s § 1 zákona č. 106/1999 Sb. v platném znění. Podle svobodného platného právního předpisu – zákona č. 110/2008 Sb., v obcích, ve znění pozdějších předpisů, se obec zřídkadlným územním samosprávným společenstvím obdává tvoří územní celek, který je vymezen hranicí území obce.
Více zde.
- Organizační struktura**
zde
- Kontaktní spojení**
 - Kontaktní poštovní adresa:
Obec Podolí
Podolí 190
686 04 Kunovice
 - Adresa úřadovny pro osobní návštěvu:
Obec Podolí
Podolí 190
686 04 Kunovice
 - Úřední hodiny:
pracovní dle OÚ:
pondělí, úterý, středa: 7:15 hod. – 12:00 hod., 12:30 hod. – 15:45 hod.
středa: 7:15 hod. – 12:00 hod., 12:30 hod. – 16:30 hod.
pátek: 7:00 hod. – 12:00 hod., 12:30 hod. – 14:30 hod.
 - Úřední dny: pondělí a středa
 - Telefonní číslo: 572 574 150
 - Adresa e-podatelny kontakt zde
 - Adresa internetové stránky: www.obecpodoli.cz

Obrázek č. 10 Transparentní účet⁶⁷

4.8 Jednání zastupitelstva a zveřejňování na internetu

Pokud pořizuje obec, zastupitel nebo jiná přítomná osoba záznam z veřejného jednání zastupitelstva, platí, že pokud jde v diskusi na tomto jednání o otázky a odpovědi na otázky týkající se veřejného zájmu, lze takový záznam bez souhlasu vystupujících osob zveřejnit bez ohledu na to, zda jde o vystoupení zastupitele nebo občana z řad veřejnosti. Ke zveřejnění

⁶⁷ Povinné informace/Transparentní účet. *Obec Podolí* [online]. Podolí u Uherského Hradiště [cit. 2020-04-26]. Dostupné z: <http://www.obecpodoli.cz/clanek/zobraz/povinne-informace>

by mělo docházet na internetových stránkách obce, nikoli na sociálních sítích, kde je vyšší riziko následného zpracování osobních údajů jinými subjekty.

Jiná situace vzniká u projednávaných bodů programu zastupitelstva nebo vystoupení, týkajících se soukromých záležitostí občanů. Tyto pasáže nelze zveřejnit, zejména pokud se týkají jejich zdravotního stavu nebo sociální nouze. Zveřejnění těchto informací na internetu by mohlo být v rozporu s § 86 občanského zákoníku i jako porušení GDPR. V případech, kdy se projednává např. uzavírání smluv mezi obcí a fyzickou osobou a následné zveřejnění na internetu, je třeba zvážit, kdy převažuje veřejný zájem a kdy by mělo být respektováno právo občana na ochranu osobních údajů. Ať je záznam pořízen z rozhodnutí zastupitelstva, individuálně zastupitelem nebo jinou osobou, měli by být přítomní v souladu se zásadou transparentnosti o pořizování záznamu předem informováni.

Samostatnou, rozsáhlou a z hlediska ochrany osobních údajů velice diskutovanou je kapitola o zveřejňování fotografií, audiovizuálních záznamech, blahopřání jubilantům, vítání občánků, kronice obce a vydávání obecních zpravodajů. Zákon o obcích stanoví, že obec může ocenit významné životní události svých občanů. Osobní údaje za účelem blahopřání jubilantům či zaslání pozvánky na vítání občánků lze získat z evidence obyvatel. Údaje, které takto získá, může obec nebo obecní úřad využívat jen tehdy, jsou-li nezbytné pro výkon jejich působnosti.

4.9 Bezpečnost na internetu

Antivirový program ESET, který je nainstalován na obecním úřadě, je dle mezinárodních měřítek velmi spolehlivou ochranou počítačového softwaru, což je jednou z nejzranitelnějších oblastí každé moderní kanceláře. „ESET patří mezi antiviry, které se každoročně umisťují na předních příčkách v nezávislých testováních. Díky jednoduchému ovládání a nadprůměrné podpoře je software vhodný i pro nezkušené uživatele. Celé prostředí je v češtině a instalace je intuitivní, proto není třeba být příliš pokročilým uživatelem. Silnou stránkou tohoto antiviru je především nízký stupeň falešných varovných hlášení. K celkové ochraně přispívají i funkce jako AntiMalware (brání počítač před infikováním malwarem, tedy veškerým škodlivým počítačovým virům), AntiSpyware (zabraňuje instalaci sledovacího softwaru), AntiAdware (brání zobrazování nechtěné reklamy) nebo ochrana před spamem.“⁶⁸

⁶⁸ ESET Smart Security Recenze. *5nej.cz* [online]. 26. 8. 2017 [cit. 2020-05-14]. Dostupné z: <https://www.5nej.cz/eset-smart-security-recenze/>

Antivirová ochrana je dostatečná, přesto je nesmírně důležité neustále aktualizovat program antivirového zabezpečení. Pro zvýšení bezpečnosti je důležité sledovat nové trendy a v rámci možností zvyšovat verzi Antivirus na co nejvíce citlivou tak, aby bylo možné předejít případným hrozbám síťového útoku. V pravidelných intervalech by bylo vhodné na počítačích revidovat nastavení Mikrotika (univerzální platforma na výstavbu routerů nebo WiFi přístupových bodů), který je tzv. vstupní bránou z internetu. Důležité je prověřovat správné nastavení firewallu a aktualizace ostatních programů.

Každý zaměstnanec musí být poučen o pravidlech bezpečného chování na internetu. Připojování přenosných médií do počítačů ve státní správě by mělo být zakázané, s výjimkou evidovaných a šifrovaných médií.

Dalším důležitým faktorem je nastavení silného přihlašovacího hesla (minimálně 10 znaků, kombinace velkých a malých znaků, čísel a speciálních znaků). Příklad takového hesla: Ov3c*PXD01. Není dobré hesla často měnit, při častých změnách hesla mají uživatelé tendenci přidávat například pouze datum změny.

Informační data se stávají tím nejdůležitějším prvkem každé kanceláře. „Data prezentují znalosti, zkušenosti, informace, které umožňují efektivní řízení a stanovení strategií do budoucnosti. Rizik je celá řada – poruchy hardware, působení virů, či hackerů přes požár, až po lidský faktor. A právě lidská chyba, obyčejné selhání hraje nejvíce rizikový faktor.“⁶⁹ Proto je důležité nepodceňovat zálohování dat. Praktickým řešením může být samostatný, klidně i méně výkonný počítač. Takové zařízení by mělo mít dostatečnou paměťovou kapacitu a mělo by být umístěno mimo hlavní budovu obecního úřadu. Na tomto počítači se mohou uskutečňovat periodické zálohy ostatních PC na úřadě, aby v případě závady nebo útoku hackera mohlo dojít k obnově dat. „Hacking je záměrná změna běžného chování počítače a připojených systémů. Obvykle je prováděn pomocí skriptů nebo programů, které manipulují s přenášenými daty, s cílem získat přístup k informacím ze systému. Hackeři napadají počítače pomocí virů, červů, trojských koní, ransomware, rootkitů nebo neautorizovanými změnami v nastavení DNS serverů. Mohou také zahltit systém velkým množstvím požadavků na určitou službu nebo stránku.“⁷⁰ Odstavení zálohovacího zařízení mimo hlavní budovu je vhodné také z hlediska fyzického zničení, např. při povodních, požáru nebo jiné nepředvídatelné situaci.

⁶⁹ Bezpečná řešení: Zálohování dat. *Storage* [online]. 2012 [cit. 2020-05-12]. Dostupné z: <https://www.storage.cz/cs/odborna-sekce/detail/id/47-zalohovani-dat>

⁷⁰ Hacker. *Avast* [online]. [cit. 2020-05-04]. Dostupné z: <https://www.avast.com/cs-cz/c-hacker>

Z hlediska ochrany informačních systémů (IS) je možné zpracování „Provozního řádu“ IS obecního úřadu, který stanoví pravidla provozu formou vnitřní směrnice. Ta je závazná pro všechny osoby pracující na obecním úřadě s IS. Pracovníci musí být proškoleni nejenom v oblasti bezpečnosti práce, ale také v oblasti bezpečnosti a používání IS, jako je bezpečné chování na internetu, připojení přenosných médií aj.

„Provozní řád informačního systému by měl určovat základní pojmy, jako je:

- Používání programového vybavení, licence používaného software, umístění a zapojení PC, terminálů a tiskáren, zásady péče o PC a terminál, či zásady ochrany dat.
- Určení doby provozu sítě, případně podmínky zprovoznění sítě mimo obvyklé hodiny provozu. Popisuje služby, které mají uživatelé k dispozici pro používání informačních systémů. Určuje způsob archivace dat, rozsah archivace a její termíny.
- Vymezení způsobu používání elektronické pošty. Hlavní bodem bývá vymezení použití elektronické pošty pouze pro služební účely.
- Vymezení způsobu využívání internetu, může oznamovat způsob monitorování provozu internetu.
- Zveřejňování informací na internetu a intranetu. Způsob zveřejňování, co zveřejňovat, definuje jednotlivé povinnosti a kompetence při zveřejňování.”⁷¹

Ochranu osobních údajů lze posílit omezeným přístupem uživatelů pouze do programů, které jsou nezbytné pro vykonávání funkce danou osobou. Každý pracovník má svůj přístup do IS a také heslo, pomocí kterého lze jeho práci monitorovat. Taková činnost s sebou ale opět přináší situaci, která by mohla způsobit konflikt s právy zaměstnance. Proto je důležité si tuto situaci pojistit a plně informovat zaměstnance o rozsahu případného monitoringu. „Kontrola aktivit a korespondence zaměstnanců by mohla být ze strany zaměstnavatelů přípustná, pouze však ve velmi omezeném (resp. přiměřeném) rozsahu, který odpovídá sledovanému účelu a cíli kontroly. Současně však bude důležité podobným způsobům kontroly zaměstnanců na pracovišti nastavit jasná a zřetelná pravidla a zaměstnance o nich důkladně informovat (např. v rámci interních směrnic či pracovních smluv).“⁷²

⁷¹ Provozní řád informačního systému. *ISVS* [online]. 2015 [cit. 2020-05-04]. Dostupné z: <http://2011-2015.isvs.cz/provozni-rad-informacniho-systemu/>

⁷² Může zaměstnavatel kontrolovat e-maily a sledovat online aktivitu zaměstnanců? *Podnikatel* [online]. 22. 6. 2017 [cit. 2020-03-04]. Dostupné z: <https://www.podnikatel.cz/clanky/muze-zamestnavatel-kontrolovat-e-mailu-a-sledovat-online-aktivitu-zamestnancu/>

Pro eliminaci rizik bezpečnosti a ochrany objektů je zásadní, aby úřady věnovaly alespoň část finančních prostředků do montáže elektronických poplašných systémů proti neoprávněnému vstupu ve večerních a nočních hodinách. „Elektronická zabezpečovací signalizace (EZS), označovaná také jako elektronický zabezpečovací systém nebo nověji poplachový zabezpečovací a tísňový systém (PZTS), je jednoúčelový, poplachový systém určený pro detekci přítomnosti vstupu nebo pokusu o vstup narušitelem do hlídaného prostoru a následnou akustickou či optickou signalizaci. Jde tedy o zařízení, které slouží k ochraně osob a majetku. Nejčastěji se ale používá pro poplašné systémy – alarmy, které reagují na narušení právě vyvoláním poplachu. Výstražný systém se může spustit analogovou (např. přerušením drátu) i digitální (detektor pohybu – PIR) detekcí. Komunikace mezi detektory a ústřednou může být vedena kabelem, bezdrátově anebo kombinací předešlých způsobů, tj. jeden detektor může být připojen kabelem a druhý bezdrátově. Systémů elektronického zabezpečení je nepřeberné množství. Od těch, kde ústředna funguje i jako detektor a signalizace, až po složité systémy s jednotlivými komponenty rozmístěnými nezávisle na sobě. Provedení může být buď jako drátový elektronický zabezpečovací systém (levnější řešení, nemusí se měnit baterie ve snímačích), nebo jako bezdrátový elektronický zabezpečovací systém, jehož výhodou je naopak zejména rychlá montáž i demontáž a snadná rozšiřitelnost EZS. Zásadní nevýhodou je však nekompatibilita bezdrátových EZS mezi rozdílnými výrobci.“⁷³

Zabezpečení vstupních dveří bezpečnostním kováním a cylindrickou vložkou by se mělo stát samozřejmostí. Ideální stav by nastal v případě montáže kamerového systému v budově obecního úřadu a okolí. V takovém případě je však opět potřeba dodržet všechna nařízení, která vychází z GDPR. „Zpracování osobních údajů provozováním kamerového systému je zákonné, pouze pokud je prováděno v odpovídajícím rozsahu v rámci některého z přípustných právních titulů zpracování osobních údajů uvedených v článku 6 GDPR. V praxi se jedná obvykle o zpracování nezbytné pro splnění úkolu prováděného při výkonu veřejné služby. V těchto případech je třeba dbát ustanovení příslušného zákona nařizujícího, resp. upravujícího zvláštní podmínky kamerové sledování, zpracování nezbytné pro účely oprávněných zájmů příslušného správce.“⁷⁴

⁷³ *Elektronické zabezpečovací systémy* [online]. Brno: Brno: Ezasys – elektronické zabezpečovací systémy [cit. 2020-06-12]. Dostupné z: <http://www.ezasys.cz/>

⁷⁴ K provozování kamerových systémů. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů, 2018 [cit. 2020-04-04]. Dostupné z: <https://www.uouu.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535>

Při využívání zabezpečovacích mechanismů nesmí být opomenuto právo na ochranu soukromí, zákoník práce a jiné. Přes všechna omezení je důležité věnovat velkou pozornost bezpečnosti informací tak, abychom se vyhnuli případné ztrátě dat či nechtěnému úniku informací.

5 EVALUACE SOUČASNÉHO STAVU ZABEZPEČENÍ BUDOVY MALÉHO OBECNÍHO ÚŘADU

Podle analýzy SWOT zpracované v tabulce č. 1 je možné posoudit silné stránky zabezpečení budovy, kterými jsou zejména mechanické zabezpečení, rozmístění hasících přístrojů v prostorách budovy a v neposlední řadě pravidelné proškolení zaměstnanců pohybujících se v prostorách budovy. Naopak slabé stránky jsou v elektronickém zabezpečení. S ohledem na finanční zátěž není hlavní překážkou samotné pořízení zabezpečovací techniky, které ve své podstatě představuje téměř marginální položku, ale zásadní náklady představuje implementace a odborná údržba takového systému. Přestože by takový systém mohl být zásadní příležitostí pro zabezpečení budovy.

V rámci zpracování diplomové práce byl proveden kvalitativní výzkum formou dotazníku. Na základě šetření stavu zabezpečení malých úřadů do 1000 obyvatel (viz tabulka č. 4) je možné konstatovat, že mechanické vybavení většiny dotázaných je dostačující. Malý obecní úřad je vybaven vstupními dveřmi s bezpečnostním kováním a cylindrickou vložkou. Také nechybí hasící přístroje pro případ vzniku požáru, které jsou však podmínkou plnění základních bezpečnostních pravidel. Uzamykatelné skříně určené k ukládání veřejných listin a dokumentů s právní relevancí, jako jsou mimo jiné smlouvy, dohody, usnesení nebo notářské zápisy. Zásadním prvkem při technickém zabezpečení fyzických předmětů je trezor, který je využíván pro úschovu úředních razítek, cenin a finanční hotovosti.

V současnosti se již standardem stává i elektronický zabezpečovací systém (tzv. EZS). Tyto systémy obvykle bývají rovněž napojeny na GSM síť či zásahové složky státního nebo soukromého charakteru, tím je míněna např. státní policie, městská policie nebo bezpečnostní agentura v rámci soukromého sektoru. Na základě kvalitativního vyhodnocení dotazníků vyplývá, že elektronické vybavení je zcela minimální. Malé obecní úřady většinou postrádají dnes již v zásadě základní systémy podpůrné elektronické ochrany jako jsou mimo jiné kamery pro denní i noční požití nebo pohybová a kouřová čidla.

Na následující příkladové studii s použitím hodnot z tabulky č. 2 je možné vypočítat rizikový stupeň a možnou míru rizika v budově malého obecního úřadu. Riziko je posuzováno za pomoci analýzy PNH.

- Varianta č. 1

3 – P – Pravděpodobná

1 – N – Vandalismus

1 – H – Téměř žádný vliv na bezpečnostní situaci

$$R = 3 \times 1 \times 1$$

$$R = 3$$

V tomto případě se jedná o V. rizikový stupeň s bezvýznamným rizikem. Z toho vyplývá, že vandalismus není z hlediska bezpečnosti faktorem, který bezprostředně ohrožuje objekt budovy obecního úřadu.

- Varianta č. 2

5 – P – Dlouhodobá

5 – N – Selhání lidského faktoru

5 – H – Velmi významný podíl vlivu na míře nebezpečí

$$R = 5 \times 5 \times 5$$

$$R = 125$$

Z uvedeného můžeme usoudit, že dlouhodobé selhávání lidského faktoru je nepřijatelným rizikem pro bezpečnost úřadu s nejvyšším stupněm rizika.

Při počítání dalších rizik může být odhalena míra nebezpečí, ať mírná či vysoká, je však velmi důležité předcházet možným rizikům předtím, než způsobí nenávratné škody na majetku nebo případně při úniku informací, jako by tomu mohlo být v případě nekontrolovaného pohybu osob (viz varianta č. 3).

- Varianta č. 3

5 – P – Dlouhodobá

4 – N – Volný pohyb osob po budově

2 – H – Nízký podíl na míře bezpečnosti

$$R = 5 \times 4 \times 2$$

$$R = 40$$

Přestože podle názoru hodnotitele může být podíl na míře bezpečnosti nízký, bude existovat mírné riziko, pokud se sníží bezpečnostní opatření, může se zvýšit riziko ohrožující celkovou bezpečnost.

Přes všechny zjištěné informace zůstává faktem, že sama budova malého obecního úřadu není hlavním zájmem případných vandalů nebo zlodějů. V budově se zpravidla nenachází významné historické předměty, které by mohly představovat zájem za účelem zbohatnutí, stejně tak se na úřadě nenachází vysoká finanční hotovost, protože v dnešní době se většina operací provádí bankovním převodem. Jednání obecního zastupitelstva, jakož i smlouvy a jiné dokumenty, jsou na vyžádání (např. podle zmiňovaného zákona č.106) přístupné všem občanům. Shrnutím tak může být, že silnou stránkou budovy malého úřadu, je právě jeho malá přitažlivost ze strany kriminálních živlů. A největším rizikem nadále zůstává případný útok na informační systém.

ZÁVĚR

Předložená diplomová práce je zaměřena na ochranu osobních údajů a informačních systémů z hlediska implementace GDPR ve veřejné správě.

Vybrané téma je úzce spjato se základními lidskými právy člověka. Přijetím GDPR došlo ke sjednocení pravidel pro zpracování osobních údajů v každém státě EU. Přijetí nařízení předcházely velké diskuze a také obavy, jak velké změny nastanou a co nařízení přinese. Po srovnání zákonů platných na území ČR před přijetím GDPR došlo prakticky pouze k administrativním změnám, kdy bylo nutné jmenovat pověřence pro ochranu osobních údajů, jehož úkolem je především poskytování informací a poradenství správci a zpracovateli osobních údajů. Z pohledu zákona pověřenec nemusí mít však žádné předepsané vzdělání. Jeho jediným předpokladem je odborná znalost práva a praxe v oblasti ochrany osobních údajů.

Ve veřejné správě, konkrétně na obecních úřadech, na které se tato práce zaměřuje, jsou řešeny konkrétní případy zveřejňování a poskytování osobních údajů z evidence obyvatel, zveřejňování v obecním zpravodaji a na úřední desce. Nedílnou součástí je zajištění ochrany informačních systémů, které s těmito údaji pracují. Dané téma je zásadní nejen pro zaměstnance ve veřejné správě, kteří se otázkou ochrany osobních údajů setkávají v každodenní praxi, ale také laickou veřejnost. Zájem dokazuje velké množství článků v novinách i na internetu, které se zabývají praktickými otázkami ochrany osobních údajů.

Před přijetím GDPR se ve veřejné správě dodržovaly již dříve přijaté normy a přijetím výše uvedeného nařízení k zásadním změnám nedošlo. Vydáním nařízení a také vydáním zákona o zpracování osobních údajů v roce 2019 došlo k přesnému vymezení, jak osobní údaje zabezpečit při zpracování, zamezit jejich zneužívání a jak je uchovávat. Dodržováním nařízení tak dochází k zachování jednoho ze základních lidských práv na ochranu osobnosti.

V teoretické části jsou rozebírány legislativní normy spojené s ochranou osobních údajů, kybernetickou bezpečností a více pozornosti je věnováno nařízení Evropského parlamentu a Rady (EU), č. 2016/679 (zkráceně GDPR). V dalších kapitolách je popsána struktura informačních systémů a jednotlivé druhy komunikace.

Aktuálním tématem je analýza současných rizik spojených se zabezpečením budovy malého obecního úřadu. Větší pozornost je věnována informačnímu systému menšího obecního úřadu s konkrétními příklady korektního zveřejňování listin, obsahujících osobní údaje podle příslušného zákona.

Diplomová práce předkládá návrh pro řešení ochrany informačního systému menšího obecního úřadu, jaké osobní údaje je možné zveřejnit v konkrétních situacích a v neposlední řadě doporučuje konkrétní řešení ochrany budovy obecního úřadů. Přínos práce je v jejím praktickém zaměření na vypracování návrhu implementace ochranných opatření ve státní správě v souladu s GDPR.

SEZNAM POUŽITÉ LITERATURY

- ALKER, Hayward R. a Thomas SCHMALBERGER. „Chapter 2: The Double Design of the CEWS Project“. In ALKER, Hayward R., Ted Robert GURR a Kumar RUPESINGHE (eds.). *Journeys Through Conflict: Narratives and Lessons*. Rowman & Littlefield, 2001. ISBN 978-0-74251-028-9.
- BARTÍK, Václav. *Zákon o ochraně osobních údajů s komentářem*. Olomouc: ANAG, 2010. Právo (ANAG). ISBN 978-80-7263-613-6.
- DITRICHOVÁ, Petra a Marek JUKL. *Základní prameny mezinárodního humanitárního práva*. Praha: Ministerstvo obrany České republiky – VHÚ Praha, 2017. ISBN 978-80-7278-698-5.
- GERŽA, Michal. *Posouzení bezpečnosti a ochrany objektu Městského úřadu Kunovice*. Zlín, 2013. Bakalářské práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce doc. Ing. Miroslav Tomek, Ph.D.
- JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN. *Informační technologie ve veřejné správě*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. ISBN 978-80-7318-607-4.
- KANOVOVÁ, Lucie. *Analýza využití účetních programů v účetnictví obcí*. České Budějovice, 2013. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Ekonomická fakulta. Vedoucí práce Ing. Hana Hlaváčková.
- KLÍMA, Karel a kol. *Komentář k Ústavě a Listině*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-44-X.
- LINHART, Jan. *Základní lidská práva a svobody a jejich procesní ochrana*. Brno, 2008. Diplomová práce. Masarykova univerzita, Právnická fakulta, Katedra právní teorie.
- PATTYNOVÁ, Jana. *Obecné nařízení o ochraně osobních údajů (GDPR): Zákon o zpracování osobních údajů: komentář*. 2. aktualizované a doplněné vydání. Praha: Leges, 2019. Komentátor. ISBN 978-80-7502-396-4.
- REKTOŘÍK, Jaroslav a kol. *Ekonomika a řízení odvětví veřejného sektoru*. Praha: Ekopress, 2002. ISBN 80-86119-60-2.
- SKOUPÝ, Arnošt. *Texty k obecným dějinám kapitalismu I*. Olomouc: Vydavatelství Univerzity Palackého, 1989.
- SMEJKAL, Vladimír. *Informační systémy veřejné správy ČR*. Praha: Oeconomica, 2003. ISBN 80-245-0533-9.

- Správní právo: (soubor zákonů)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, [2016]. ISBN 978-80-7380-649-1.
- ŠPAČEK, David a Jiří ŠPALEK. *Informační systémy ve veřejném sektoru: distanční studijní opora*. Brno: Masarykova univerzita v Brně, Ekonomicko-správní fakulta, 2004. ISBN 80-210-3503-X.
- Trestní právo: (soubor zákonů)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, [2019]. ISBN 978-80-7380-753-5.
- TRUNEČEK, Jan. *Management v informační společnosti*. 2. vydání. Praha: Vysoká škola ekonomická, 1999. ISBN 80-7079-683-9.
- UHLÁŘ, Jan. *Technická ochrana objektů*. Praha: Vydavatelství PA ČR, 2004. ISBN 80-7251-172-6.
- Úplné znění Ústavního zákona České národní rady č. 1/1993 Sb., Ústava České republiky: Úplné znění Usnesení České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky; některé další související právní předpisy*. 14. vydání. Praha: Armex Publishing, 2019. Edice kapesních zákonů. ISBN 978-80-87451-66-3.
- Všeobecná deklarace lidských práv*. Ilustroval Yacine AÏT KACI. Praha: Informační centrum OSN, [2015]. ISBN 978-80-86348-42-1.
- Všeobecná deklarace lidských práv. Usnesení č. DE01/48 Valného shromáždění OSN. New York, 1948.
- WIENER, Norbert. *Kybernetika a společnost*. Praha: Nakladatelství Československé akademie věd, 1963.
- ZAHÁLKA, Jiří. *Analýza rizik v průmyslovém podniku*. Brno, 2012. Diplomová práce. Vysoké učení technické, Fakulta strojního inženýrství, Ústav výrobních strojů, systémů a robotiky. Vedoucí práce Ing. Luboš Kotek, Ph.D.
- ZOBAL, Jaroslav. *Informační systém města či obce*. Brno, 2006. Diplomová práce. Masarykova univerzita, Ekonomicko-správní fakulta. Vedoucí práce Mgr. Jiří Špalek, Ph.D.
- ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.

Internetové zdroje

- ALIS spol. s.r.o. *KEO (-X, -W, 4)* [software]. 2004–2018 [cit. 2020-07-22]. Dostupné z: <http://www.alis.cz/cs>
- Bezpečná řešení: Zálohování dat. *Storage* [online]. 2012 [cit. 2020-05-12]. Dostupné z: <https://www.storage.cz/cs/odborna-sekce/detail/id/47-zalohovani-dat>
- Compatibility list KEO4. *ALIS* [online]. Česká Lípa: ALIS spol. s r.o. [cit. 2020-07-22]. Dostupné z: <http://www.alis.cz/uploads/assets/compatibilitylistkeo4.pdf>
- Czech POINT reg. č. CZ.1.06/1.1.00/03.05921. *Czech POINT* [online]. Praha: Ministerstvo vnitra České republiky, 2020 [cit. 2020-06-12]. Dostupné z: <https://www.czechpoint.cz/public/>
- Datové schránky* [online]. Praha: Ministerstvo vnitra České republiky, 2019 [cit. 2020-04-16]. Dostupné z: <https://www.datoveschranky.info/>
- Deklarace práv člověka a občana. *Informační centrum vlády* [online]. Praha: Vláda České republiky, 24. 8. 2009 [cit. 2020-03-10]. Dostupné z: <https://icv.vlada.cz/cz/tema/deklarace-prav-cloveka-a-obcana-60939/>
- Dozorová a rozhodovací činnost. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-07-08]. Dostupné z: <https://www.uouu.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277>
- Elektronické zabezpečovací systémy* [online]. Brno: Brno: Ezasys – elektronické zabezpečovací systémy [cit. 2020-06-12]. Dostupné z: <http://www.ezasys.cz/>
- ESET Smart Security Recenze. *5nej.cz* [online]. 26. 8. 2017 [cit. 2020-05-14]. Dostupné z: <https://www.5nej.cz/eset-smart-security-recenze/>
- Firewall. *Esset* [online]. 2020 [cit. 2020-05-08]. Dostupné z: <https://www.eset.com/cz/firewall/>
- Hacker. *Avast* [online]. [cit. 2020-05-04]. Dostupné z: <https://www.avast.com/cs-cz/c-hacker>
- Chraňme si zákon na ochranu soukromí. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-08-04]. Dostupné z: <https://www.uouu.cz/chranme-si-zakon-na-ochranu-soukromi/ds-2469>
- Informace poskytnuté dle zákona č. 106/1999 Sb. *Obec Podolí* [online]. Podolí u Uherského Hradiště, 2020 [cit. 2020-06-12]. Dostupné z: <http://www.obecpodoli.cz/dokumenty/poskytnute-informace/000168.pdf>

- JONÁK, Zdeněk. Informace. *Databáze Národní knihovny ČR* [online]. Praha: Národní knihovna ČR, 2003 [cit. 2020-07-07]. Dostupné z: http://aleph.nkp.cz/F/?func=direct&doc_number=000000456&local_base=KTD
- K provozování kamerových systémů. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů, 2018 [cit. 2020-04-04]. Dostupné z: <https://www.uouu.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535>
- K rodným číslům. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-04-26]. Dostupné z: <https://www.uouu.cz/k-rodnym-cislum/ds-5091/archiv=0&p1=3938>
- KAUFNER, Jiří, ed. Správa osobních údajů v praxi obcí a měst. *SMO ČR* [online]. Praha: Svaz měst a obcí České republiky, 2020 [cit. 2020-06-12]. ISBN 978-80-88375-07-4. Dostupné také z: <https://www.smocr.cz/Shared/Clanky/8403/e-sprava-osobnich-udaju-v-praxi-obci-a-mest.PDF>
- KOUDELKA, Ctirad a Václav VRÁNA. Rizika a jejich analýza. *VŠB* [online]. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, 2006 [cit. 2020-04-26]. Dostupné také z: <https://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf>
- Listina základních lidských práv Evropské unie. *EUR-Lex* [online]. Štrasburk, 2012 [cit. 2020-04-26]. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:12012P/TXT>
- Manuál pro obce k zákonu o svobodném přístupu k informacím. *MV ČR* [online]. Praha: Ministerstvo vnitra České republiky, 2017 [cit. 2020-04-23]. Dostupné z: <https://www.mvcr.cz/odk2/soubor/manual-pro-obce-k-zakonu-o-svobodnem-pristupu-k-informacim.aspx>
- Může zaměstnavatel kontrolovat e-maily a sledovat online aktivitu zaměstnanců? *Podnikatel* [online]. 22. 6. 2017 [cit. 2020-03-04]. Dostupné z: <https://www.podnikatel.cz/clanky/muze-zamestnavatel-kontrolovat-e-maily-a-sledovat-online-aktivitu-zamestnancu/>
- Nástroj k anonymizaci dokumentů. *Portál veřejné správy* [online]. Praha: Ministerstvo vnitra České republiky, 2018 [cit. 2020-06-12]. Dostupné z: <https://anonymizace.gov.cz/crossroad/>
- NOVOTNÝ, Jan. Hledá se starosta. *Euro* [online]. 5. 10. 2018 [cit. 2020-05-18]. Dostupné z: <https://www.euro.cz/politika/hleda-se-starosta-spravu-nad-radou-obci-prevezme-ministerstvo-vnitra-1423046>

- Ochrana počítače proti virům. *Microsoft: Support service* [online]. Microsoft, 2020 [cit. 2020-08-04]. Dostupné z: <https://support.microsoft.com/cs-cz/help/17228/windows-protect-my-pc-from-viruses>
- Operační systémy. *Jak na internet* [online]. 2020 [cit. 2020-04-24]. Dostupné z: <https://www.jaknainternet.cz/page/1757/operacni-systemy/>
- PASEKOVÁ, Eva. Svobodný přístup k informacím? Soudy jsou zahlceny žádostmi i šikanózními dotazy. *Česká justice* [online]. Praha: Ministerstvo vnitra České republiky 2016 [cit. 2020-04-23]. Dostupné z: <https://www.ceska-justice.cz/2016/12/svobodny-pristup-k-informacim-soudy-jsou-zahlceny-zadostmi-sikanoznimi-dotazy/>
- Povinné informace/Transparentní účet. *Obec Podolí* [online]. Podolí u Uherského Hradiště [cit. 2020-04-26]. Dostupné z: <http://www.obecpodoli.cz/clanek/zobraz/povinne-informace>
- Program. *IT Slovník* [online]. 2020 [cit. 2020-05-09]. Dostupné z: <https://it-slovník.cz/pojem/program>
- Provozní řád informačního systému. *ISVS* [online]. 2015 [cit. 2020-05-04]. Dostupné z: <http://2011-2015.isvs.cz/provozni-rad-informacniho-systemu/>
- Pseudonymizace osobních údajů. *GDPR* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-04-26]. Dostupné z: <https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/>
- Shrnutí „Analýzy aktuální úrovně zapojení ČR do konceptu SMART city a SMART region v souvislosti snovými trendy, včetně návrhů opatření.“ *Vláda* [online]. Praha: Vláda České republiky, 2018 [cit. 2020-07-22]. Dostupné z: <https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/Shrnuti-Analyzy-aktualni-urovne-zapojeni-CR-do-konceptu-smart-city-a-smart-region-v.pdf>
- Slovníček nejdůležitějších pojmů. *ÚOOÚ* [online]. Praha: Úřad pro ochranu osobních údajů [cit. 2020-04-26]. Dostupné z: <https://www.uoou.cz/slovnicek-nejdulezitejsich-pojmu/ds-2617/archiv=0&p1=3938>
- Státní informační politika – cesta k informační společnosti. *Vláda* [online]. Praha: Vláda České republiky [cit. 2020-03-19]. Dostupné z: <https://www.vlada.cz/cz/clenove-vlady/historie-minulych-vlad/statni-informacni-politika---cesta-k-informacni-spolecnosti---dokument-2089/>
- ŠVANDERLÍKOVÁ, Klára. Fikce doručení do datové schránky. *Právní prostor* [online]. 6. 2. 2018 [cit. 2020-04-26]. Dostupné z: <https://www.pravniprostor.cz/clanky/procesni-pravo/h-fikce-doruceni-do-datove-schranky>

Teorie informace. *IS Mendelu* [online]. Brno: Mendelova univerzita [cit. 2020-06-07].

Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7017

ŤOPEK, Martin. Správce převzal řízení obce, jejíž zastupitele vyhnaly stohy žádostí. *IDnes* [online]. 28. 1. 2014 [cit. 2020-05-18]. Dostupné z:

https://www.idnes.cz/pardubice/zpravy/spravce-obec-sec-zastupitelstvo-zadosti.A140128_2027379_pardubice-zpravy_mt

VŠETEČKA, Daniel. RIS3 strategie. *MPO* [online]. Praha: Ministerstvo průmyslu a obchodu, 2019 [cit. 2020-07-22]. Dostupné z: <https://www.mpo.cz/cz/podnikani/ris3-strategie/>

Základní registry. *OSF MV ČR* [online]. Praha: Odbor strukturálních fondů Ministerstva vnitra České republiky [cit. 2020-04-23]. Dostupné z: <http://www.osf-mvcr.cz/zakladni-registry>

Legislativa

Sdělení č. 115/2001 Sb. m. s., Ministerstva zahraničních věcí o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-21]. Dostupné z: <https://www.zakonyprolidi.cz/ms/2001-115>

Usnesení č. 2/1993 Sb., předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-21]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1993-2>

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-18]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106>

Zákon č. 111/2009 Sb., o základních registrech. In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-04-23]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-111>

Zákon č. 128/2000 Sb., o obcích (obecní zřízení). In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-06-30]. <https://www.zakonyprolidi.cz/cs/2000-128>

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel). In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-05-04]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-133>

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi – Sbíрка zákonů* [online]. [cit. 2020-04-29]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-18]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-227>

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákon. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-04]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-365>

Zákon č. 40/2009 Sb., trestní zákoník. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-06-02]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40?>

Zákon č. 89/2009 Sb., občanský zákoník. In: *Zákony pro lidi – Sbírka zákonů* [online]. [cit. 2020-05-12]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-89>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AWID	Asociace pro práva žen v rozvoji
CRIN	Mezinárodní síť práv dítěte
DPH	Daň z přidané hodnoty
ESIF	Evropské strukturální a investiční fondy
EU	Evropská unie
EZS	Elektronický zabezpečovací systém
GDPR	Obecné nařízení o ochraně osobních údajů
GSM	Globální systém pro mobilní komunikaci
HURIDOCS	Informační a dokumentační systémy o lidských právech
IS	Informační systém
NAS	Datové úložiště na síti
OHCHR	Úřad Vysokého komisaře OSN pro lidská práva
ORG	Převodník identifikátorů
OSN	Organizace spojených národů
PC	Osobní počítač
ROB	Registr obyvatel
ROS	Registr osob
RUIAN	Registr územní identifikace, adres a nemovitostí
ZZVZ	Zákon č. 134/2016 Sb., o zadávání veřejných zakázek

SEZNAM OBRÁZKŮ

Obrázek č. 1 Základní funkce informačních a komunikačních technologií.....	21
Obrázek č. 2 Schéma fungování základních registrů.....	27
Obrázek č. 3 Síťové připojení v obci	37
Obrázek č. 4 Pohled na hlavní stranu programu KEO.....	40
Obrázek č. 5 Přehled modulů v části účetnictví	41
Obrázek č. 6 Program KEO – část mzdová.....	45
Obrázek č. 7 Internetový portál Czech POINT	48
Obrázek č. 8 Návod k anonymizaci dokumentů.....	50
Obrázek č. 9 Příklad anonymizovaného dokumentu	51
Obrázek č. 10 Transparentní účet	58

SEZNAM TABULEK

Tabulka č. 1 SWOT analýza zabezpečení	30
Tabulka č. 2 Analýza PNH	31
Tabulka č. 3 Rizikový stupeň a míra rizika	32
Tabulka č. 4 Dotazník pro obce	33
Tabulka č. 5 Ilustrační osobní informace	53
Tabulka č. 6 Pseudonymizace osobních informací.....	53