Západočeská univerzita v Plzni

Fakulta právnická

Katedra veřejné správy

DIPLOMOVÁ PRÁCE

GDPR VE VEŘEJNÉ SPRÁVĚ

Mgr. Barbora Čechurová

Plzeň 2019

Západočeská univerzita v Plzni

Fakulta právnická

Katedra veřejné správy

DIPLOMOVÁ PRÁCE

GDPR VE VEŘEJNÉ SPRÁVĚ

Vedoucí diplomové práce: JUDr. Tomáš Louda, CSc.

Zpracovala: Mgr. Barbora Čechurová

V Plzni, 2019

„Prohlašuji, že jsem tuto diplomovou práci zpracovala samostatně, a že jsem vyznačila prameny, z nichž jsem pro svou práci čerpala způsobem ve vědecké práci obvyklým.“

Plzeň, březen 2019 ……

Mgr. Barbora Čechurová

Touto prací bych zároveň ráda poděkovala mému vedoucímu diplomové práce JUDr. Tomáši Loudovi, CSc. za velmi cenné rady a odbornou pomoc při jejím vypracovávání, dále mé rodině za neopomenutelnou pomoc a podporu nejen při závěrečných zkouškách a psaní této práce, ale i při celém vysokoškolském studiu.

Vloženo oficiální zadání diplomové práce

Obsah

1. Úvod

Diplomová práce s názvem *GDPR ve veřejné správě* se svým obsahem snaží cílit zejména na problematiku ochrany osobních údajů v době po nabytí účinnosti Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné Nařízení o ochraně osobních údajů), v práci dále označované jako „Nařízení GDPR", či jen „Nařízení".

Hlavním záměrem, který se autorka práce snažila pokrýt, je přínos přehledného, souvislého, stručného (jelikož by problematika Nařízení GDPR mohla být analyzována bez pochyb i na odbornější vědecké úrovni), avšak přesto kompaktního pohledu na oblast ochrany osobních údajů, a to nejen v soukromé sféře.

Jelikož je toto téma vskutku široké, obsáhlé a jeho problematika nesmírně vyčerpávající, bylo nutné stanovit konkrétní směr, kterým se práce dále ubírá. Tímto vyčleněným směrem je zejména ochrana osobních údajů ve světle Nařízení GDPR v kontextu veřejné správy, dále též analýza problematiky v rámci Evropské unie a komparace úpravy ochrany osobních údajů v jednom z členských států Unie (konkrétně Spolková republika Německo) s Českou republikou.

Úvodní kapitoly a podkapitoly diplomové práce jsou pro lepší přehlednost a celkovou postupnou strukturu věnovány obecným pojmům jako *Veřejná správa* či *eGovernment*, také obecnému tématu *Ochrany osobních údajů*, jakožto jednoho ze základních lidských práv a to jak obecně, tak v kontextu veřejné správy a v poslední řadě též v rámci vnitrostátní i evropské judikatury – z pohledu ochrany moci soudní. Opomenuta není ani obecná situace v rámci právních předpisů v této oblasti – kapitola nesoucí název *Právní pohled – bezpečnost, soukromí*.

Kapitoly následující jsou již zaměřeny na hlavní téma diplomové práce, tedy na *GDPR ve veřejné správě* a to jednak ze stránky čistě teoretické, jednak také ze stránky praktické, ve které je zachyceno pojetí GDPR v rámci samosprávných celků, vypracovávání Metodik státních orgánů či přínosy nebo naopak negativa, která v souvislosti s tímto právním předpisem vyvstávají. Závěrečné části práce jsou věnovány stavu ochrany osobních údajů v Evropské unii a příkladnému a stručnému *Srovnání úpravy institutu ve Spolkové republice Německo a v České republice*.

Základními metodami, se kterými je následně pracováno, jsou tyto níže uvedené:

a) metoda abstrakce – zejména v úvodních popisných částech práce
b) metoda odborné analýzy – v celkovém průběhu zpracování práce
c) metoda komparace – v závěrečné části práce

V několika pasážích se jevilo vhodným doplnit pro demonstraci grafické znázornění či vzorový formulář. Veškeré grafy, obrazové materiály či formuláře jsou získány z vlastního dotazníkového šetření autorky či z oficiálních zdrojů, které jsou vždy uvedené.

V práci jsou použity prameny více typů, prvním z nich jsou odborné knižní publikace různých autorů z oblasti veřejné správy, ochrany osobních údajů, kybernetické bezpečnosti, a dalších. Dále jsou hojně využívány platné právní předpisy (jednak evropské právo, vnitrostátní a cizozemské zákony a též podzákonné právní předpisy) a judikatura soudů národních i Evropského soudu pro lidská práva. Posledním, nikoli však minoritním, zdrojem jsou odborné webové stránky (zejména Ministerstva vnitra, dále portál veřejné správy a další, včetně cizojazyčných).

2. Veřejná správa

2.1 Úvod do veřejné správy

Pojem veřejná správa je možné vnímat v několikerém kontextu, tedy z více úhlů pohledů či podle zaměření z několika odlišných hledisek. Jednak zejména proto, že neexistuje její jedna jednotná, legální a teorií ustálená definice a jednak také z jejího esenciálního jádra samotného (= tedy objemná masa činností, postupů, teoretických principů a zásad, atp., pojících se i mimo jiné s tzv. neurčitými právními pojmy jako typicky například veřejný zájem a dalšími).

Přes tato teoretická úskalí je fenomén veřejné správy bezesporu klíčovým pojmem (nejen) správního práva, a to jak v jejím materiálním – činnostním (funkčním) slova smyslu, tak samozřejmě i ve smyslu formálním – institucionálním (organizačním). Veřejná správa je mimo jiné toliko předmětem samotného oboru správního práva. Její činnost lze charakterizovat dle různých kritérií jako závislou, odbornou, specializovanou, neutrální ve smyslu politickém a také jako činnost stálou, trvalou [1].

Základní pojmové znaky veřejné správy je možné spatřovat zejména v těchto následujících [2]:

a) podzákonnost
b) nepřetržitost
c) veřejný zájem
d) nařizovací a výkonná funkce
e) pravomoc a působnost
f) a případné další.

Jak lze zpozorovat, tak i samotní odborníci z právnické, veřejnosprávní či jiné praxe se v názoru na eventuální sjednocení definice veřejné správy neshodují a ve svých výkladech nezaujímají jednotné stanovisko k této problematice [3]. Nejběžněji a veřejnosti (laické i odborné) také nejpochopitelněji se veřejná správa popisuje jako tzv. *Správa věcí veřejných*

[1] HENDRYCH, Dušan. *Správní právo: obecná část*. 9. vydání. V Praze: C.H. Beck, 2016. Academia iuris (C.H. Beck). ISBN 978-80-7400-624-1. Str. 5
[2] ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 3.
[3] Například definice veřejné správy J. Pražáka: „činnost nesoucí se za trvalým účelem řídit ty které záležitosti“. Definice J. Hoetzela: „činnost orgánů označených jako správní úřady“. Výrok Forsthoffův výrok: „veřejná správa může být jen popsána, nikoli však definována“.

ve veřejném zájmu (v této univerzálně přijímané definici lze spatřovat rovněž problematiku právě tzv. neurčitých právních pojmů).

Jelikož je téma diplomové práce zaměřeno na ochranu osobních údajů (v souvislosti s přijetím Nařízení GDPR) v prostoru veřejné správy, je vhodné zde zmínit, alespoň okrajově, i prostředí tzv. eGovernmentu = elektronické prostředí veřejné správy, nikoli jen veřejnou správu obecně, ve smyslu čistě klasicky institucionálním.

2.2 Moderní veřejná správa

Moderní veřejná správa by měla být prostředkem k udržování příznivého přístupu orgánů veřejné moci [4] (ať již státní správy či samosprávy) vůči svým klientům (zejména občanům). Vhodné je zmínit též samotný pojem modernizace veřejné správy, což znamená jistý přechod od společnosti industriální k postindustriální (informační). V publikaci *Modernizace veřejné správy* [5] se objevuje též tzv. „manažerializace" veřejné správy. Tímto termínem lze rozumět moderní postupy a metody řízení ve veřejné správě (management veřejné správy). Z klasické právní (veřejnosprávní) teorie ale stále plyne tendence rozlišovat veřejnou správu a management, tedy řízení, kdy proces vedení činností a personálních zdrojů patří spíše do soukromého sektoru. Praxe se však kloní k postupnému prolínání veřejného a soukromého sektoru, právě v těchto oblastech (moderní metody ve veřejné správě).

2.3 eGovernment [6]

Termínem eGovernment (= electronic government, doslovně přeloženo jako elektronické vládnutí) se rozumí soustavný proces elektronizace celé veřejné správy – tedy státní správy i samosprávy. Nelze mluvit o veřejné správě v kompletním celku v elektronické podobě jako takové, jelikož se jedná o neustále se vyvíjející a rozšiřující se úseky (stejně tak, jako veřejná správa samotná). Lze jej popsat například jako [7]: „*Sérii procesů, vedoucích k výkonu státní správy a samosprávy a uplatňování občanských práv a povinností fyzických a právnických osob, realizovaných elektronickými prostředky*". Organizace pro hospodářskou spolupráci a rozvoj (OECD) vyslovila svou následující definici eGovernmentu, kdy podle ní

[4] LOUDA, Tomáš, Jiří GROSPIČ a Lenka VOSTRÁ, ed. *Modernizace veřejné správy v Evropě a České republice: sborník příspěvků z workshopu s mezinárodní účastí: Praha 22.-23. 11. 2005*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006. ISBN 80-7380-001-2. Str. 51

[5] LOUDA, Tomáš, Jiří GROSPIČ a Lenka VOSTRÁ, ed. *Modernizace veřejné správy v Evropě a České republice: sborník příspěvků z workshopu s mezinárodní účastí: Praha 22.-23. 11. 2005*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006. ISBN 80-7380-001-2. Str. 51

[6] ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 3

[7] VANÍČEK, Zdeněk a Stanislav A. MARCHAL. *Právní aspekty eGovernmentu v ČR*. Praha: Linde, 2011. ISBN 978-80-7201-855-0. Str. 11

jde o [8]: „*Využití informačních a komunikačních technologií, především internetu, jako prostředku k dosažení dobré (lepší) správy“,* či o: „*Různé úkoly, které se zabývají elektronizací výkonu činnosti veřejné správy nebo v širším pojetí spíše orgánů veřejné moci vůbec“.*

Hlavní pointou myšlenky elektronizace veřejné správy je heslo (nebo lépe řečeno - teorie), že úřady nemají obíhat občané, ale právě dokumenty v elektronické podobě klienty - občany. Dle této teze je nesmyslné, až absurdní a komplikované, aby občané kvůli jedné záležitosti museli několikrát navštívit několikero úřadů, případně prokázat více skutečností, které by si daná instituce mohla jednoduše zjistit a zajistit elektronickou cestou sama [9].

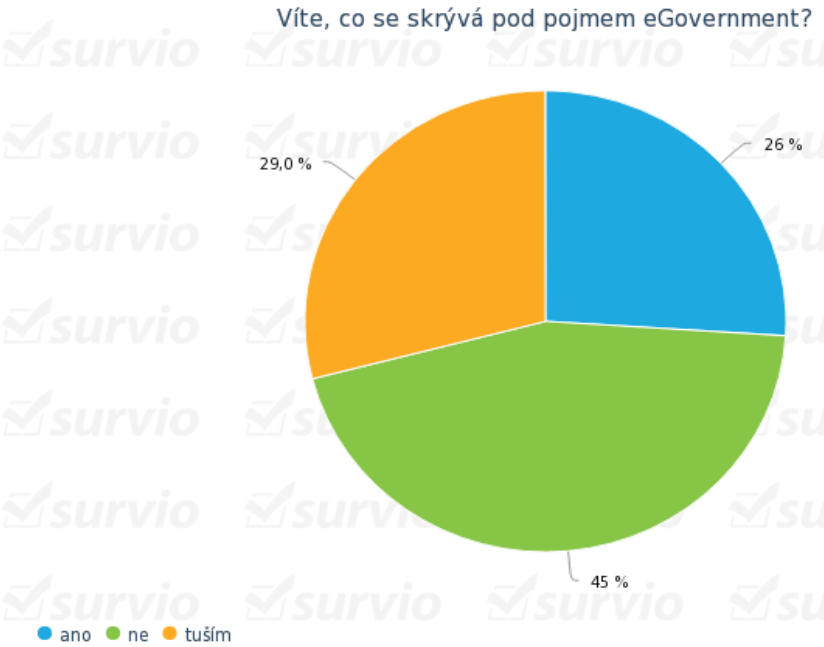
Ministerstvo vnitra České republiky definuje, respektive popisuje eGovernment jako [10]: *„Myšlenkou tzv. eGovernmentu je správa věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější.“.*

Postupný proces modernizace veřejné správy, ve smyslu její neustálé elektronizace, je činností, která v současné době stále ještě není všem klientům zcela blízká, jak také dokazuje doložený graf (pro celkové shrnutí a doplnění tohoto tématu) z vlastního dotazníkového šetření autorky [11], téměř polovina respondentů (ve složení mužů i žen, ve věkovém rozmezí cca 18-40 let; středoškolsky až vysokoškolsky vzdělaní) neví, co pojem eGovernment znamená.

Graf je znázorněn na následující straně.

[8] VAVROCHOVÁ, Simona. *Vzdělávání v eGovernmentu*. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. ISBN 978-80-86847-74-0. Str. 4
[9] ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 3
[10] *Http://www.mvcr.cz/clanek/co-je-egovernment.aspx,* © 2015 Ministerstvo vnitra České republiky, [online]. [cit. 2019-02-01]
[11] Data jsou z roku 2018, kdy diplomantka odevzdávala diplomovou práci na téma eGovernment.

Graf číslo 1: Pojem eGovernment



Zdroj: vlastní výzkum pomocí online vytváření grafů na www.survio.com

2.3.1 Principy/zásady eGovernmentu

Právní zásady jsou obecným vodítkem, výkladovou pomůckou, jak se orientovat v jakémkoli právním odvětví a jak jej interpretovat a aplikovat nejen de iure, ale i de facto. Proto i správní právo, veřejná správa a také eGovernment mají své specifické právní zásady/principy, podle kterých je poté samotná materie těchto oblastí dále interpretována, potažmo aplikována v praxi. Jde o následující principy a zásady (nejedná se o taxativní výčet, pouze o ty hlavní, jež definují eGovernment ve svém teoretickém slova smyslu):

- dobrá správa
- zákonnost
- spolehlivost
- předvídatelnost
- transparentnost
- otevřenost
- hospodárnost
- odpovědnost

3. Ochrana osobních údajů ve veřejné správě

3.1 Osobní údaje

Pod termínem osobní údaj se většině společnosti vybaví zejména:

- jméno a příjmení fyzické osoby,
- datum narození či rodné číslo,
- trvalé bydliště,
- případně další, specifické nebo citlivé osobní údaje, jako jsou například náboženství, sexuální orientace, vzorky otisků prstů nebo i vzorky DNA.

Jsou to pojmy, které se více či méně dotýkají daného subjektu a konkretizují tak jeho osobnost. Některé z těchto údajů jsou za určitých okolností proměnné (typicky trvalé bydliště, ale i jméno a příjmení), jiné však nikoli (typicky vzorky DNA). Co se považuje za osobní údaj z právního hlediska je objasněno v kapitole věnující se Nařízení GDPR.

Obecně je předpokládáno a tvrzeno, že osobní údaje souvisí se soukromím jednotlivce, a nemělo by se do nich tedy svévolně zasahovat – musí zde existovat relevantní, legální důvod, pro jakýkoli, byť sebemenší zásah. Soukromí není na národní ani nadnárodní úrovni nikterak výslovně a legálně definováno, je to v podstatě další neurčitý právní pojem, který je pouze výkladově dovozován v ad hoc případech. Ochrana soukromí a s tím související instituty, jako i ochrana osobních údajů, jsou zakotveny od národních, státních úrovní (v ČR Ústava, Listina základních práv a svobod [12], jednotlivé zákony, a další) až po úrovně mezinárodní (Evropská úmluva o lidských právech, unijní předpisy a další).

S rostoucím technologickým pokrokem (= modernizací) se ochrana osobních údajů a dat dostává čím dál tím více do popředí nejen soukromých, ale i veřejných zájmů. Jedná se o celosvětově diskutované téma, které, dalo by se říci, neustále nabírá na intenzitě. Velmi často je otázka ochrany osobních údajů spojována (a to zejména v důsledku medializace) s určitými negativními kontexty. Je tomu tak pravděpodobně proto, že samotná média (ať již se jedná o televizní či rozhlasová vysílání, periodický tisk, sociální sítě, či jiná masmédia) společnost informují v drtivé většině o nejrůznějších případech porušování této ochrany a nebezpečí s nimi spojenými.

[12] Konkrétně článek 10, odstavec 3 Listiny základních práv a svobod, který praví: „ *Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě*.“.

Problematika ochrany těchto údajů je velice citlivým tématem, se kterým se musí denně vypořádávat soukromý i veřejný sektor. Ne vždy jsou jasné hranice, kdy už se jedná o porušování této ochrany a kdy dal dotyčný subjekt svým jednáním souhlas [13]. I zde však jednání mohlo být činěno za jiným prvotním účelem, ale osobní údaje přesto zneužity nebyly.

3.1.1 Ochrana osobních údajů v soukromém a veřejném sektoru

Výše uvedená fakta se dotýkají zejména soukromého sektoru, soukromé sféry, kde taková jednání činíme dobrovolně, z vlastní soukromé a svobodné vůle. Jinak je tomu však u veřejné správy, obecně tedy u vztahů [14], kde jedním prvkem je zejména orgán veřejné moci (typicky u státní správy či územní samosprávy konkrétní úřad) a postavení subjektů je vzájemně nerovné - subordinační. V těchto vztazích je poskytování osobních údajů vázáno zejména na určitou právní skutečnost, či určité právní jednání, kdy orgán veřejné správy musí prokázat, že účel, pro který osobní údaje žádá, je legitimní. Výjimkou však není ani poskytování osobních údajů v důsledku protiprávního jednání dotčeného subjektu, případně objektivně nastalého protiprávního stavu bez cizího, subjektivního, zavinění [15]. Dojde-li zde k porušení ochrany osobních údajů, viníkem je veřejná správa v zastoupení konkrétního státního orgánu či jiného, samosprávného orgánu.

3.2 Veřejná správa a ochrana osobních údajů

Demokraticky smýšlející a fungující státy musí bezvýjimečně respektovat soukromí každého subjektu, každé fyzické, potažmo i právnické osoby. Do sféry soukromí je možné řadit například samotné smýšlení člověka, týkající se jeho záležitostí rodinných, pracovních, jeho soukromé aktivity, rodinný a pracovní prostor, ale samozřejmě také osobní informace a osobní údaje. Do práva na soukromí subjektu v nejobecnějším slova smyslu, i v tom užším, zaměřeném právě na ochranu osobních údajů, je možné legálně zasahovat pouze státní, veřejnou mocí, v legálně stanovených důvodech, pokud samotný subjekt nedává svým jednáním souhlas sám [16].

Ochrana osobních údajů velice úzce koreluje s veřejnou správou právě (ale nejen) v jejím elektronickém prostředí, tedy v již zmiňovaném eGovernmentu, jelikož právě zde se

[13] Například „bezmyšlenkovitého“ poskytování osobních údajů1 fyzické osoby v rámci internetového kyberprostoru – nakupování na e-shopech, přihlašování na sociální sítě atp.
[14] Z teorie známé jako tzv. administrativněprávní vztahy.
[15] Například tzv. situace vis maior, kdy se může jednat o určité živelné katastrofy (požáry, povodně, události nastalé v důsledku silných bouří či nepříznivých povětrnostních podmínek atp.).
[16] KLÍMA, Karel. *Veřejná správa a lidská práva*. Praha: Metropolitan University Prague Press, 2015. ISBN 978-80-87956-27-4. Str. 16

odehrávají procesy různého typu, ve kterých dochází k operacím s osobními údaji (online zápisy do registrů, veřejných rejstříků, atd.). Proto je nutné celou oblast veřejné správy legálně zajistit tak, aby manipulace s těmito údaji všech dotčených subjektů byla co možná nejbezpečnější.

Ochranu osobních údajů v rámci veřejné správy je možné chápat ve dvojím, speciálním, pojetí [17]:

1. jako obecná hranice mezi právem na soukromí každého a na jeho ochranu a shromažďováním a jejich uchováváním
2. jako výčet kompetencí a rozsah, kterými může veřejná správa ve vztahu k osobním údajům disponovat – jaké údaje tedy vůbec smí od subjektu požadovat a v jaké míře

V neposlední řadě se jedná též o zamezení jakéhokoli zneužívání osobních dat – v případě veřejné správy samotné o jakékoli nelegitimní činnosti, které by do této sféry zasahovaly a v případě třetích, nezúčastněných, stran o jakékoli nelegální zásahy obecně (zejména hackerské útoky).

Během poslední desítky let se těmto otázkám počala věnovat značná pozornost. Zaměření pozornosti odborníků padlo zejména na oblast legislativy. Největší pozornost se vztáhla na okruh informací, které jsou oběma sektory (soukromým i veřejným) zpracovávány a na délku doby uchování těchto informací. Druhým tématem v pořadí bylo předávání a tok osobních údajů [18]. Tyto okruhy jsou úzce spjaty s prostorem a s neustálým rozvojem informačních a komunikačních technologií, dnešní moderní doba je proto někdy nazývána též dobou informační nebo dobou vyspělé techniky [19].

3.3 Okruh údajů uchovávaných veřejnou správou

Veškeré informace a osobní údaje, se kterými veřejná správa jakkoli manipuluje, nebo je pro své účely uchovává, musí být jednak získány legálním způsobem, a jednak musí být založen platný právní důvod, pro který jsou shromažďovány, případně po delší časový úsek

[17] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2. Str. 10

[18] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2. Str. 10

[19] Zde může vyvstat též otázka, zdali se dnešní vyspělá část světa a jeho lidstvo nedostává do postupného stavu technokratické společnosti, kdy se nejrůznější procesy a činnosti, které dříve zastávali běžní pracovníci, automatizují, přechází se na elektronickou komunikaci, elektronickou správu informací a dat. S tím souvisí právě problematika ochrany soukromí a osobních údajů, jelikož veškeré procesy pomocí těchto technologií trvají mnohonásobně kratší časové úseky a možnost zneužití dat s tímto faktem bohužel stále úměrně roste.

ukládány (obecně je předpokládáno na tzv. nezbytně nutnou dobu, pokud samozřejmě není doba pro možnost uchovávání zakotvena v právních předpisech konkrétně). Dalším aspektem, který musí veřejná správa plně respektovat, je účelnost získávaných osobních údajů a dalších informací – tedy údaj, který získá k určitému, konkrétnímu důvodu, smí být využit reálně jen k tomuto důvodu a nikoli například k prověřování dané osoby. Oporu v zákoně lze prozatím nalézt především v zákoně č. 101/2000 Sb., o ochraně osobních údajů (v brzké době vejde v účinnost tzv. adaptační zákon – viz dále). Pokud by veřejná správa, resp. její zaměstnanci shromažďovali takovéto údaje od subjektů nelegální cestou nebo bez řádného odůvodnění, jednalo by se o velmi citelný zásah do práva na soukromí každého jednotlivce, které je chráněno jak na ústavní, tak na mezinárodní úrovni [20].

Petra Melotíková ve své knize *Ochrana osobních údajů ve veřejné správě* uvádí následující, tzv. Gandyho dělení okruhu informací (tedy jaké druhy informací), které veřejná správa získává, jsou jimi [21]:

a) osobní údaje fyzických osob
b) informace ze sféry sociálního zabezpečení
c) informace právního charakteru
d) tzv. jednorázově využitelné informace
e) informace o právnických osobách

3.3.1 ad a) Osobní údaje fyzických osob

Tyto informace se týkají jen a pouze fyzických osob, nikoli osob právnických. Údaje může veřejná správa získávat různými způsoby – například podáními fyzických osob vůči orgánu veřejné správy nebo mohou být součástí povinně vedených veřejných rejstříků.

3.3.2 ad b) Informace ze sféry sociálního zabezpečení

V dnešní době tvoří tato kategorie informací podstatnou část objemu, jež veřejná správa zpracovává a uchovává. Smysl práva sociálního zabezpečení pramení z tzv. teorie welfare state = teorie sociálního státu, který jak svými aktivními, tak pasivními nástroji [22] řeší nastalé sociální události nejrůznějších skupin obyvatelstva. Aby stát mohl na tomto principu

[20] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2. Str. 28
[21] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2. Str. 28
[22] viz. Teorie aktivních (předcházení negativním sociálním událostem) a pasivních nástrojů (řešení a zmírňování dopadů nastalých sociálních událostí) politiky zaměstnanosti

kvalitně fungovat, je nutné znát od dotyčných subjektů potřebné údaje. Jedná se o vesměs rozšířený okruh informací, který je veřejná správa oprávněna požadovat. Nikoli jen základní osobní údaje (jméno a příjmení fyzické osoby, trvalé bydliště, datum narození atp.), ale i údaje specifické nebo citlivé (informace o zdravotním stavu, předchozí zaměstnání, finanční situace a příjem finančních prostředků a další).

3.3.3 ad c) Informace právního charakteru

Tyto údaje by se daly řadit mezi specifické, zvláštní a to proto, že nepodávají informace o konkrétní fyzické osobě, ale spíše o jejích poměrech k určitým statkům. Vztahují se k soukromí osoby, ale je nutné, aby je stát měl ve svém držení pro eventuální další, navazující účely a pro účely veřejné správy jako takové. Může se jednat o informace vedené v katastru nemovitých věcí, záznamy v rejstříku trestů, atp.

3.3.4 ad d) tzv. Jednorázově využitelné informace

Jednorázově, případně dočasně využitelné informace, jsou takové, které již ze svého názvu má veřejná správa v držení jen na omezenou dobu, pro konkrétní krátkodobý účel. Typickým příkladem je výpis z bankovního účtu

3.3.5 ad e) Informace o právnických osobách

Údaje o právnických osobách tvoří asi nejvíce specifickou a samostatnou skupinu. Jedním z důvodů je zejména to, že právnická osoba je uměle právem utvořený organizovaný útvar, který nepožívá ochrany v rámci zákona o ochraně osobních údajů ani Nařízení GDPR (tyto právní předpisy se vztahují pouze k fyzickým osobám).

Zmíněná je zde tato skupina zejména pro úplnost výše zmíněné Gandyho teorie sdílení informací a také z důvodu, že každá právnická osoba je jen fikcí osoby, kdy za ni vždy vystupují právě osoby fyzické. Přes veškerou tuto fiktivní konstrukci, kdy právnické osoby nemohou existovat bez minimálního de iure základu fyzických osob, se jim dostává stále většího zájmu z hlediska konkrétních možných práv a povinností. Příkladem je vznik trestní odpovědnosti právnických osob (přijetí a účinnost zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim), kdy se již trestní odpovědnost neváže výlučně na osoby fyzické, nýbrž je zde dána tzv. přičitatelnost jednání.

3.4 Ochrana osobních údajů orgány moci soudní

Všechna tato fakta a úskalí rozhodně nejsou diskutována odborníky jen teoreticky, naopak, v určitých situacích se zde musí angažovat i jiná odborná praxe – tímto autorka práce míří na otázku bezpečnosti a poskytování ochrany právům – tedy justici, ochranu poskytovanou nezávislými a nestrannými soudy. V České republice se do těchto témat zapojují jednak obecné soudy a jednak i soudní orgán ochrany ústavnosti – Ústavní soud. Na nadnárodní úrovni pak Evropský soud pro lidská práva a Soudní dvůr Evropské unie [23]. Soudy rozhodují v rozličných případech, kdy se často ochrana osobních údajů dostává do kolize i s jinými, základními lidskými právy a svobodami.

3.4.1 Judikatura vnitrostátní

Jedním z nejznámějších, téměř kazuistických, případů byl spor z roku 2008, kdy se do kolize dostala právě dvě základní lidská práva – právo na ochranu soukromí (resp. konkrétně nedotknutelnost obydlí) a právo na ochranu osobních údajů, identity. Spor p. Ryneš vs. dva občané ČR, kteří se do domu pana Ryneše (dále jen stěžovatel) opakovaně vloupávali. Proto stěžovatel postupoval tak, že nainstaloval na svůj dům bezpečnostní kamery, z důvodu ochrany svého základního práva. Pokud se stručně shrne celý případ, šlo o skutečnost, že kamerový systém natáčel i veřejné prostranství před domem stěžovatele, tudíž mohly být shromažďovány a zpracovávány osobní údaje případem nedotčených osob. Byla zde i značná nejednotnost v názorech orgánů veřejné moci a to konkrétně Úřadu pro ochranu osobních údajů a Nejvyššího správního soudu. Ke stěžovateli se nakonec přiklonil právě Nejvyšší správní soud, který zrušil pokutu udělenou Úřadem pro ochranu osobních údajů a rozhodnutí Městského soudu v Praze [24].

Z další judikatury vnitrostátní i evropské lze zmínit několik případů, ve kterých soudy rozhodovaly. Z české judikatury je možné okrajově uvést například [25]:

- **Usnesení Ústavního soudu České republiky, IV. ÚS 4041/16 ze dne 12. 1. 2017** - ústavní stížnost společnosti FTV Prima, spol. s r. o., proti rozsudku proti rozsudku Nejvyššího správního soudu ze dne 20. 9. 2016, č. j. 5 As 198/2015-60, a rozsudku Městského soudu v Praze ze dne 26. 8. 2015, č. j. 3 A

[23] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2. Str. 11
[24] KLÍMA, Karel. *Veřejná správa a lidská práva*. Praha: Metropolitan University Prague Press, 2015. ISBN 978-80-87956-27-4. Str. 143-151
[25] https://www.uoou.cz/ustavni-soud/ds-2854/archiv=0 [online]. [cit. 2019-02-01]

1/2012-82. Jednalo se o záležitost neoprávněného zveřejnění rodného čísla, kdy Úřad pro ochranu osobních údajů uložil pokutu 4000 Kč.

- **Nález Ústavního soudu České republiky, Pl. ÚS 1/12 ze dne 27. 11. 2012, 437/2012 Sb. N 195/67 SbNU 333** - Sloučení parlamentní rozpravy k více návrhům zákonů; Povinnost uchazečů o zaměstnání vykonávat veřejnou službu; Návrh na zrušení zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Ve věci zákona o zdravotních službách se opět mimo jiné jednalo o nakládání s rodnými čísly pacientů.
- **Usnesení Ústavního soudu České republiky, I. ÚS 28/02 ze dne 16. 3. 2004** - Ústavní stížnost Českého statistického úřadu proti usnesení Městského soudu v Praze ze dne 8. 11. 2001, sp. zn. 38 Ca 454/2001. V tomto případě byla jádrem věci Úřadem pro ochranu osobních údajů uložená likvidace některých osobních údajů, které zpracovával a uchovával Český statistický úřad.
- **Usnesení Ústavního soudu České republiky III. ÚS 381/01 ze dne 17. 10. 2001** - ústavní stížnost Městského úřadu Dobřany proti nezákonnému zásahu státu v zastoupení Úřadu na ochranu osobních údajů v Praze. Zde se jednalo o pochybnosti o důvodnosti zpracování citlivých údajů [26].

3.4.2 Judikatura evropská

Z judikatury Evropského soudu pro lidská práva lze zmínit následující [27]:

- **Rozsudek Evropského soudu pro lidská práva – případ S. a Marper versus Spojené království, ze dne 4. 12. 2008.** Tento případ je typicky ukázkovým, kdy soud rozhodoval v případě ochrany osobních údajů ve věci uchovávání otisků prstů a dalších specifických a jedinečných osobních údajů státními orgány (buněčné vzorky, vzorky DNA), a to po pravomocném skončení trestního stíhání stěžovatelky (po jejím osvobození od trestního stíhání).
- **Rozsudek Evropského soudu pro lidská práva - případ Satakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku, ze dne 27. 6. 2017.** V tomto rozsudku rozhodoval soud ve věci zveřejňování osobních údajů spojených s informacemi o zdanitelném příjmu a majetku fyzických osob. Šlo

[26] údaje národnostní, rasové, údaje o trestné činnosti, zdravotním stavu a členství v politických stranách apod.
[27]https://www.uoou.cz/vismo/zobraz_dok.asp?n=evropsky-soud-pro-lidska-prava&archiv=0&id_ktg=2853&tzv=1&pocet=25&stranka=1 [online]. [cit. 2019-02-01]

mimo jiné o kolizi práva svobody projevu s právem na ochranu osobních údajů.

- **Rozsudek Evropského soudu pro lidská práva - případ Godelli proti Itálii, ze dne 13. 3. 2013.** Tento případ se týkal kolize práva na informace a právo na ochranu osobních údajů.
- **Rozsudek Evropského soudu pro lidská práva – případ KH a dalších proti Slovensku, ze dne 6. 11. 2009.** V tomto případu šlo o kolizi práva na informace (ze zdravotní dokumentace) a práva na ochranu osobních údajů (zejména jejich uchovávání/archivace) Stěžovatelé uvedli, že po dobu tří let nemohli získat fotokopie svých zdravotních záznamů (v jednom případe dotčená žalovaná nemocnice dokonce měla ztratit uchovávané záznamy pacienta).
- **Rozsudek Evropského soudu pro lidská práva – případ KU proti Finsku, ze dne 2. 3. 2009.** Zde došlo k porušení ochrany soukromí dokonce ještě mladistvého (12letého) jednotlivce a zneužití jeho osobních údajů díky falešnému inzerátu podanému 3. osobou, kdy tato osoba veřejně uvedla bez vědomí poškozeného jeho osobní údaje.

4. Právní pohled – bezpečnost, soukromí

4.1 Legislativa v oblasti ochrany osobních údajů

Veškeré procesy, jež se odehrávají ve veřejné správě, ať již se jedná o ty interní (tedy mezi jejími orgány navzájem), či naopak o procesy externí (mezi těmito orgány a soukromoprávními subjekty (občany a dalšími subjekty)), musí být de iure i de facto realizovány a zajišťovány prostřednictvím kvalitních postupů, metod a zároveň pevných pravidel (zásada zákonnosti); a v rámci eGovernmentu bezesporu i prostřednictvím kvalitních technologií [28].

4.2 Zákonné limity

Stejně tak, jako v reálném prostředí a životě, tak i v kybernetickém prostředí dochází k porušování práv na ochranu soukromí, k narušení ochrany osobních údajů atp. Tomu se snaží nejen česká, ale i evropská legislativa čelit právními předpisy, které by měly napomáhat k dodržování těchto práv a eventuálními sankcemi k minimalizaci protizákonného jednání. Mezi jedny z hlavních evropských dokumentů, upravujících bezpečnost a soukromí občana v kybernetickém prostoru jsou [29]: Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (z roku 1981), Smlouva o fungování Evropské unie (článek 16), Listina základních práv Evropské unie (článek 8) a další. Tyto předpisy korespondují s principy otevřenosti a transparentnosti, kdy se informace mohou zveřejňovat a poskytovat na jejich základě a v mezích zákonných limitů.

V prostředí elektronické komunikace se stejně jako v běžném životě promítá jedno ze základních lidských práv, a to konkrétně právo na soukromí a ochranu osobnosti. Toto právo je zakotveno v Listině základních práv a svobod, v článku 7 (dále i dotčené články 10, 12 a 13). Z hlediska elektronické komunikace a celkově virtuálního prostředí je nutno řešit otázku soukromí v kontextu kontroly informací o subjektu samém. Ústavní soud toto definoval následovně [30]: „*Právo na soukromí rovněž garantuje právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení*.“

[28] ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 32

[29] NOVOTNÝ, Vladimír. *Elektronizace veřejné správy – Soubor vědeckých statí*. Praha, Metropolitní univerzita Praha, 2011. CD-ROM Str. 15

[30] DONÁT, Josef a Jan TOMÍŠEK. *Právo v síti: průvodce právem na internetu*. V Praze: C. H. Beck, 2016. ISBN 978-807400-610-4. Str. 68

Právě prostor informačních a komunikačních technologií je velmi citlivým „územím“ – hrozí zde snadnější zneužití (nejen) osobních dat, kyber-útoky hackerů, problémy při prokazování totožnosti atp., proto je třeba dbát zvýšené pozornosti při tvorbě, aplikaci a interpretaci právních předpisů a dalších nenormativních metodik, které tento prostor okleští jasnými hranicemi a při eventuálním porušení primární povinnosti vznikne pachateli sankční povinnost ve formě určité, konkrétní újmy - trestu. K tomu je třeba kvalitní a dostatečné úpravy nejen tuzemského práva a právních předpisů, ale i práva evropského, případně mezinárodního [31].

4.3 Právní předpisy na ochranu osobních údajů

Níže je možno spatřovat demonstrativní výčet nejdůležitějších a nejzákladnějších zákonů, upravující a dotýkající se problematiky ochrany osobních údajů (případně dalších rovin bezprostředně souvisejících) ve veřejné správě. Tento výčet neobsahuje zmínku o Nařízení GDPR, jelikož tomu je věnována značná část diplomové práce jako samostatnému a hlavnímu celku. Mezi klíčové vnitrostátní právní předpisy patří [32]:

- **Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů** - v tomto zákoně, konkrétně hned v jeho 3. paragrafu je uvedeno, že ochrana se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby a zároveň, že tato ochrana platí na jakékoli zpracování údajů, včetně elektronické formy.
- **Zákon č. 106/1999 Sb., o svobodném přístupu k informacím** – tento zákon upravuje podmínky pro poskytování informací ze strany státních orgánů, územních samosprávných celků a jejich orgánů a také veřejných institucí.
- **Zákon č. 480/2004 Sb., o některých službách informační společnosti** – zde jsou upravena práva a povinnosti subjektů, které vznikají při realizování právních vztahů za pomoci elektronických prostředků. Jde o elektronickou komunikaci prováděnou prostřednictvím elektronické pošty, automatické volací a komunikační systémy, sítě elektronických komunikací, atp.
- **Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)**, ve znění pozdějších

[31] ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 32
[32] https://www.uoou.cz/pravni-predpisy/ds-1257 [online]. [cit. 2019-02-01]
https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267 [online]. [cit. 2019-02-01]

předpisů – tento právní předpis upravuje ochranu autorských děl hmotných i nehmotných – softwarů a jiných elektronicky dostupných děl a projektů.

- **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů**, který upravuje práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.
- **zákon č. 89/2012 Sb., občanský zákoník** - jméno a bydliště člověka (§ 77 až § 80), osobnost člověka (§ 81 až 117)
- **zákon č. 365/2000 Sb., o informačních systémech veřejné správy** a o změně některých dalších zákonů
- **zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů**
- **zákon č. 111/2009 Sb., o základních registrech**
- **zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)**
- **zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)**
- **zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů**

a značné množství dalších, včetně nařízení vlády, vyhlášek ministerstev a případných jiných, metodických pokynů. Toto jsou klíčové právní předpisy z hlediska české legislativy, které se vztahují k ochraně osobních údajů. Jejich úplný výčet by byl až vyčerpávající a v rozsahu diplomové práce nemožný, jelikož oblasti veřejné správy a osobních údajů se všemi oblastmi a činnostmi související je značně široká.

Česká republika, jako téměř jedna z posledních zemí Evropské unie, neměla do nedávna stále ještě definitivně vyřešenou otázku novelizace či přijetí nového zákona na ochranu osobních údajů v reakci na přijetí Nařízení GDPR. Adaptačním zákonem bude v brzké době derogován do nynější doby účinný zákon č. 101/2000 Sb. – o ochraně osobních údajů.

5. Obecné Nařízení GDPR

Velmi často diskutované (a to jak laickou, tak i odbornou veřejností), leckdy i po roční účinnosti neporozuměné nebo i dokonce opomíjené – jedná se o 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).

Veřejnosti je známé spíše pod zkratkou GDPR (v originálním překladu jím rozumíme: General Data Protection Regulation), které vešlo v účinnost 25. května 2018 (po dvouleté legisvakanční lhůtě, kdy v platnost vešlo již v roce 2016). Toto Nařízení se dotýká mimo veřejnosprávní sféry také sféry soukromoprávní.

5.1 Historický exkurs vývoje ochrany osobních údajů

Stejně tak, jako ostatní instituty z oblasti veřejného i soukromého práva, tak i ochrana osobních údajů prochází postupem doby určitým vývojem a jakousi „modernizací“. Tento fenomén je spjat s několika vývojovými tendencemi a to zejména s přeshraničním cestováním osobních údajů v rámci europrostoru a mezinárodním prostoru i přes hranice Evropské unie, dále s modernizací v oblasti informačních a komunikačních technologií a mimo to neméně i se zpřísňováním ochrany soukromí jednotlivce, které je v demokratické společnosti nediskutabilní a jednoznačné.

Prvním moderním právním předpisem, resp. normativní právní smlouvou, na mezinárodní úrovni, jež upravovala ochranu osobních údajů, byla Všeobecná deklarace lidských práv, která byla přijata Valným shromážděním OSN v roce 1948 a to ve Spojených státech amerických, konkrétně v San Franciscu. Zde článek 12 zakotvuje zákaz svévolného zasahování do soukromé sféry jednotlivců a také zákaz zásahu do jakékoli jejich korespondence. Na relativně stejném principu na evropské úrovni vystupuje článek 8 Evropské úmluvy o ochraně lidských práv a základních svobod z roku 1950, který garantuje ochranu soukromí, rodinného života [33]. Tyto dokumenty jsou v rámci ochrany osobních údajů klíčové, a to i přes absenci konkrétní úpravy této problematiky [34]. Jsou toliko základními předpisy.

[33] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 13

[34] v tomto kontextu lze (v rámci základních pravidel teorie práva) chápat ochranu osobních údajů jako speciální oblast teorie obecné ochrany soukromí jednotlivce.

V průběhu zmíněné modernizace, zejména v oblasti informačních a komunikačních technologií, dochází k většímu přesunu masy osobních údajů. Proto bylo nutné reagovat na tuto situaci a poptávka po zvýšené právní regulaci ochrany osobních údajů tak vzrostla. Jednotlivé státy začaly tuto poptávku uskutečňovat a ochraně osobních údajů věnovat větší zájem. Zmínit je možné jednu ze směrnic OECD, přijatou roku 1980, jež se věnovala rovněž ochraně soukromí z obecného hlediska a zároveň také mezistátnímu pohybu osobních údajů a jejich ochraně - Směrnice o ochraně soukromí a přeshraničních tocích osobních údajů [35].

Zlomovým okamžikem se stal 28. leden 1981 [36], kdy byla přijata Úmluva o ochraně osob se zřetelem na automatizované zpracování dat (č. 115/2001 Sb. m. s.). Touto Úmluvou se prvně v historii oficiálně a legálně vyčlenilo a osamostatnilo právo na ochranu osobních údajů z práva na ochranu soukromí jednotlivce, jehož rozvoj neustále pokračuje a rozšiřuje se. Došlo zde například k definování základních pojmů – osobní údaj, správce zpracování osobních údajů, automatizované zpracování, atp. Zakotvily se zde rovněž základní zásady pro nakládání a práci s údaji [37].

Dalším předpisem na nadnárodní úrovni, který upravuje danou oblast opět o krok napřed, je Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Tato Směrnice, ačkoli je „produktem" orgánů Evropské unie, zasahuje nejen v jejím prostoru, ale i v zemích mimo Unii [38]. V této Směrnici je zakotven tzv. harmonizační účinek pro jednotlivé členské státy, což v praxi znamená, že právě tyto státy musí do svých právních řádů včlenit, resp. sladit, obsah ustanovení této Směrnice (a jelikož se jedná o formu směrnice, je na každém státu, jakou metodu včlenění zvolí, zda inkorporaci, transformaci či adaptaci).

S postupnou modernizací, zejména již výše zmíněných informačních a komunikačních technologií, bylo nutné posunout ochranu osobních údajů (a to jak na úrovni mezinárodní (evropské), tak i na úrovni vnitrostátní) na další, vyšší úroveň. Rozvoj počítačových softwarů, rychlosti internetového připojení, postupný růst rozvoje inteligentních elektronických zařízení a jejich aplikací, popularizace a narůstající počet uživatelů sociálních sítí, atp. – to vše bylo, je

[35] http://www.oecd.org/sti/ieconomy/15589535.pdf [online]. [cit. 2019-02-01]
[36] Právě v tento den, tedy 28. 1., se právě v souvislosti s výše zmíněnou Úmluvou, koná tzv. Mezinárodní den ochrany osobních údajů.
[37] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 14
[38] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 15

a bude nadále faktorem vysoce ovlivňujícím úpravu ochrany osobních údajů. Všechny tyto faktory navíc působí právě nejen ve vnitrostátním prostoru států, ale i mimo ně, tedy přeshraničně.

5.2 Přijetí Nařízení GDPR

Nejnovějším posunem na poli legislativy ochrany osobních údajů v rámci Evropské unie a jejích členských států bylo přijetí Nařízení Evropského parlamentu a Rady Evropské unie č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné Nařízení o ochraně osobních údajů = Nařízení GDPR [39]).

Nařízení GDPR je v členských státech Evropské unie přímo a bezprostředně použitelné díky své formě, která je závazná svým přímým účinkem. Státy jsou povinny toto Nařízení přijmout a sladit s ním svou vnitrostátní legislativu.

5.2.1 Evropský sbor pro ochranu osobních údajů

Pracovní skupina WP29 byla založena na základě Směrnice 95/46/ES, konkrétně ustanovení jejího článku 29. Každý členský stát byl zastoupen jedním zástupcem dozorového úřadu, dále zde figuroval jeden zástupce Evropského inspektora ochrany údajů a Evropské Komise. Tato skupina významně figurovala na poli problematiky ochrany osobních údajů zejména před přijetím Nařízení GDPR.[40]

25. května 2018, s účinností Nařízení GDPR, ji nahradil právě Evropský Sbor pro ochranu osobních údajů (dále jen „Sbor“), nezávislý subjekt (právnická osoba sui generis) veřejného (evropského) práva, s vlastní právní subjektivitou a s přesně definovanými kompetencemi a úkoly. Sbor je složen podobně jako bývalá Pracovní skupina WP29, s rozdílem oslabeného postavení Evropské Komise, která v tomto případě má již jen poradní hlas a nepožívá hlasovacího práva [41].

Článek 70 Nařízení GDPR poskytuje Sboru konstruktivní informace pro jeho činnost, stanovuje úkoly, kterými jsou zejména oprávnění vydávání pokynů a doporučení, včetně praxí osvědčených postupů, jak dosáhnout optimálního cíle - poskytování a zajišťování nástrojů

[39] v originále General Data Protection Regulation
[40] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 29
[41] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 30

k efektivní ochraně osobních údajů. Sbor působí v postavení svým způsobem poradního subjektu, je jakousi prodlouženou rukou samotného Nařízení GDPR [42]. V rámci své činnosti Sbor od prosince roku 2016 [43] vydal již několik doplňujících metodik, vztahující se zejména k otázkám automatizace v případě zpracovávání osobních údajů, dále k otázkám transparentnosti zpracovávání, či k problematice porušování principů zabezpečení ochrany osobních údajů, případně k otázkám souhlasu ke zpracování těchto údajů samotnými subjekty.

V České republice jsou dokumenty vydané Sborem přehledně dostupné v českém překladu na webu Úřadu pro ochranu osobních údajů, kde se aktuálně nachází 13 Pokynů vydaných k provedení Nařízení GDPR či k výkladu, případně doplnění určitých pojmů [44].

5.3 Nařízení jako právní akt EU

Forma nařízení, jakožto sekundárního právního aktu Evropské Unie, je zvolena zejména pro svou přímou závaznost, použitelnost a aplikační přednost v jednotlivých členských státech, ty jej tím pádem nemusí nijak zvlášť implementovat do svého právního řádu. Není zde potřeba žádného prováděcího vnitrostátního právního předpisu, navíc jsou za jeho dodržování plně odpovědné. Veškerá obecná nařízení, která jsou Evropskou unií vydána, lze dohledat v tzv. Úředním Věstníku Evropské unie. Cílem volby tohoto typu právního předpisu je, dalo by se říci, jakási pomyslná unifikace veškerých dílčích celků kompletní upravované oblasti, a to v celé Evropské unii jednotně – ve všech členských státech. Přes tuto unifikaci může nařízení v určitých otázkách ponechat státům jistou libovůli a ty tak mohou s úpravou v mezích daných nařízením manipulovat.

5.4. Nařízení GDPR – základní informace

Cílem Nařízení GDPR je poskytnout všem občanům Evropské unie vyšší ochranu jejich osobním údajům, než doposud. Jakousi nepsanou tezí poté je, že ochrana osobních údajů a dat cestuje přes hranice spolu s osobními údaji. Tento cíl má být realizován prostřednictvím dvou základních pravidel a to [45]:

[42] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 30
[43] tedy od okamžiku platnosti, nikoli účinnosti, Nařízení GDPR
[44]https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=28603&n=schvalene-pokyny&p1=4720 [online]. [cit. 2019-02-01]
[45] https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938, [online]. [cit. 2019-1-23]

- obecně mít přehled a aktuální informace o stavu osobních údajů a mimo to mít možnost získávat informace o tom, jaké údaje o daném subjektu jsou zpracovávány a z jakého důvodu
- možnost domáhat se dodržování pravidel, včetně nápravy stavu – v případě porušení či nesplnění primární povinnosti přichází sekundární povinnost v podobě (typicky přiměřené finanční) sankce [46].

Nařízení GDPR, jak je již výše zmíněno, je tedy závazné pro oba sektory – pro veřejný i soukromý. Hlavními otázkami, kterými se veřejná správa (včetně eGovernmentu) může zabývat a zabývá, a na které se autorka diplomové práce bude snažit v praktické části později také odpovědět, jsou následující:

1. **Jakým přínosem je Nařízení GDPR pro veřejnou správu v České republice?**
2. **Je (bylo) v České republice možné již od samého počátku účinnosti Nařízení GDPR jeho plné dodržování a aplikování?**
3. **Jsou sankce za porušení Nařízení GDPR přiměřené?**
4. **Jak se od května 2018 vypořádaly samosprávy s účinností Nařízení GDPR a jak funguje Nařízení GDPR po půlročním fungování**?

Zde může vyvstat a v praxi také často vyvstává otázka, co vlastně oním osobním údajem je a může či naopak nemůže být? Takovým údajem se podle zákona č. 101/2001 Sb. rozumí [47]: „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.*“.

V Nařízení GDPR jsou osobní údaje definovány jako takové informace, které se vztahující k identifikované či identifikovatelné osobě. Mezi tzv. obecné osobní údaje lze zařadit typicky jednak jméno, pohlaví, věk a datum narození (případně rodné číslo), osobní stav, ale mimo tyto také například i IP adresu a fotodokumentaci fyzické osoby. Vzhledem k tomu, že se vztahuje i na podnikající fyzické osoby (= fyzické osoby podnikatele), je možné zařadit mezi osobní údaje i tzv. organizační údaje. Jedná se zejména o e-mailové spojení, telefonní číslo či různé další identifikační údaje, vydané státem [48].

[46] neoprávněné nakládání s osobními údaji je i podle české právního řádu trestným činem – zákon č. 40/2009 Sb. (trestní zákoník), §180
[47] §4, písmeno a) zákona č. 101/2001 Sb. – zákon o ochraně osobních údajů
[48] https://www.gdpr.cz/gdpr/osobni-udaje/ [online]. [cit. 2019-02-08]

Publikace *Praktický průvodce GDPR* JUDr. Jiřího Žůrka hned ve svých úvodních větách Předmluvy konstatuje osobní údaje jako jakýsi faktor, či fenomén, jež pomyslně zhmotňuje bytí osob ve společnosti a navzájem je od sebe rozlišuje a mimo to také – což je hlavním účelem, zejména pak z právního a správního hlediska – zmiňuje, že osobní údaje identifikují. Právě identifikace je jedním z klíčových pojmů celé oblasti osobních údajů a jejich ochrany, je nástrojem pro odhalení právní osobnosti člověka (důkaz jeho existence po stránce veřejnoprávní i soukromoprávní) a zároveň procesem, ve kterém se odehrávají důležité zásahy do těchto údajů – manipulace s osobními údaji (ať již ze soukromých účelů, či účelů veřejných, ve veřejné správě).

Jednotlivé atributy osobních údajů zakládají jedinečnost každé fyzické osoby, stejně tak, jako má každá taková osoba svůj nezaměnitelný biologický a genetický kód, tak v tomto případě se jí připisuje i jedinečný kód jako subjektu práva [49]. Právo na ochranu osobních údajů se úzce kryje s ochranou soukromí každého jedince, které je mimo jiné základně garantováno článkem 10, odstavci 3. Listiny základních práv a svobod, kde se praví následující [50]: „*Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě* „.

Nařízení GDPR přineslo pro členské země Evropské unie nejen společnou právní úpravu obecných pojmů, zásad, zpracování, ukládání a dalších institutů, ale také společné sankce (resp. druhy sankcí a hranice jejich výše) při porušení povinností plynoucích z tohoto Nařízení.

5.5 Jednotlivé základní pojmy definované Nařízením GDPR

Nařízení GDPR ve svém 4. článku obsahuje základní výčet a definice základních, klíčových pojmů, které jsou dále využívány jak samotným Nařízením, tak dalšími předpisy a dokumenty, které interpretaci a aplikaci právě těchto pojmů využívají. Jsou jimi [51]:

a) osobní údaj – jím se rozumí veškeré informace o identifikované (ta osoba, která se přímo identifikuje) nebo identifikovatelné (tuto lze přímo či nepřímo identifikovat odkázáním na určitý konkrétní údaj = identifikátor, kterým může být jméno fyzické osoby, její identifikační číslo, či jiný specifický údaj vztahující se k její sociální,

[49] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 8
[50] článek 10 (3) zákona č. 2/1993 Sb. – Listina základních práv a svobod
[51] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 32-35

ekonomické, psychologické, genetické či kulturní identitě) fyzické osobě. Osobní údaje a jejich ochrana se v tomto kontextu vztahují na žijící fyzické osoby, nikoli na osoby již zesnulé.

b) správce osobních údajů – správcem osobních údajů může být jak fyzická, tak i právnická osoba. Mezi tzv. právnické osoby sui generis se řadí stát a jeho orgány, tudíž orgány veřejné moci. Mezi další správce se mohou řadit agentury a další, jež vykonávají činnosti nesoucí se za účelem dalšího nakládání (= tedy zpracování) s nimi. Tyto subjekty samy či společně s jinými určují prostředky (metody) zpracování a hlavní účel zpracování.

c) zpracovatel osobních údajů – jím se rozumí fyzická či právnická osoba (včetně státu a jeho orgánů či již zmíněných agentur), která zpracovává osobní údaje pro správce.

d) zpracování, omezení zpracování – zpracováním se rozumí nejrůznější operace, tedy nakládání s osobními údaji. Děje se takto buď tzv. „ručně“, čili bez pomoci automatizovaných systémů anebo naopak tzv. automatizovaně (zejména pomocí elektronizace, případně za pomoci informačních a komunikačních technologií). Zpracování může probíhat rozličnými způsoby a to například jako shromažďování, ukládání, pozměňování, přizpůsobování, strukturování, šíření či zpřístupnění, seřazování a kombinování, vyhledávání, vymazávání nebo jiné fyzické zničení a další operace.

e) příjemce osobních údajů – jím je opět fyzická či právnická osoba (včetně veřejnoprávních sui generis či agentur), které jsou údaje poskytovány.

f) tzv. „třetí strany“ – třetími stranami v rámci zpracovávání osobních údajů se rozumí fyzické nebo právnické osoby (opět všechny viz. výše), které samy nejsou dotčeným subjektem údajů, zpracovatelem, správcem ani jinými osobami, zpracovatelům či správcům podléhající a jsou oprávněné nakládat s osobními údaji.

g) profilování – profilováním se rozumí automatizované zpracovávání osobních údajů, které vede k hodnocení daných osobních aspektů fyzické osoby. Dle publikace JUDr. Žůrka doslova jako [52]: „*jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se*

[52] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 32

k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování…“. V tomto bodě lze velmi zřetelně spozorovat prolínání různých sfér, které se v rámci obecné úpravy osobních údajů fyzických osob střetávají. Nejde tedy jen o jejich čisté shromažďování či evidování.

h) pseudonymizace – tento víceúrovňový krok v rámci zpracování osobních údajů v praxi znamená, že konkrétnímu subjektu jsou přiřazeny další, dodatečné informace, bez kterých není možné dále operovat. Osobní údaje se tedy musejí zpracovat tak, že bez použití dodatečných informací je není možné subjektu přiřadit a dále s nimi pracovat.

i) evidence – evidencí se v dokumentu rozumí logicky seřazený, strukturovaný soubor osobních údajů a dalších informací, jež je přístupný podle zvláštních pravidel. Může se vyskytovat jednak na národní či na mezinárodní úrovni.

j) souhlas ke zpracování – souhlas subjektu osobních údajů je chápán jako svobodný, informovaný, konkrétní a dobrovolný projev vůle, učiněný zejména prohlášením o svolení ke zpracování osobních údajů daného subjektu.

k) porušování zabezpečení ke zpracování osobních údajů – jedná se o taková jednání, která svou povahou odporují pravidlům určeným k zabezpečení osobních údajů subjektů a tímto primárním jednáním je poté způsoben nežádoucí sekundární efekt ve formě protiprávního (případně i náhodného) zničení, změně, zneužití či až k úplné nebo částečné ztrátě osobních údajů v dané konkrétní evidenci.

l) tzv. „genetické údaje“, „biometrické údaje“ a údaje o zdravotním stavu – genetickými údaji fyzické osoby jsou takové, které se (jak je znatelné již z názvu) pojí s její genetickou výbavou a zděděnými, případně i získanými genetickými znaky (kódy) a poskytují jedinečné informace o každém jedinci. Je možné je získávat zejména biologickými odběry vzorků (vzorky DNA z vlasů, slin atp.). Biometrickými údaji se rozumí osobní údaje, které jsou již automatizovaně zpracované právě z konkrétních fyzických či fyziologických údajů konkrétního subjektu (typicky se jedná například o daktyloskopické údaje). Pokud se jedná o zdravotní údaje fyzické osoby, jde o konkrétní informaci týkající se fyzického, případně i psychického stavu člověka. Může jít o záznamy o prodělaných chorobách, úrazech, podstoupných vyšetřeních či operačních zákrocích, ale například i predispozice k dědičným chorobám.

m) dozorový úřad, dotčený dozorový úřad – dozorovým úřadem se rozumí nezávislý orgán veřejné moci, který je zřízen každým jednotlivým členským státem. Dotčený dozorový úřad je takový úřad, kterého se zpracovávání osobních údajů přímo dotýká takovým způsobem, že správce nebo zpracovatel je usazen na území jiného členského státu a to v rámci tohoto úřadu; případně subjekty, s jejichž osobními údaji bude nakládáno, mají bydliště (pobyt) na území dozorového úřadu a budou dotčeny zpracováním dotčeného dozorového úřadu. Poslední možností je, že u dotčeného dozorového úřadu byla podána stížnost týkající se porušení ustanovení Nařízení GDPR.

n) přeshraniční zpracování – jedná se o takový druh zpracování, které probíhá přeshraničně, přes několik orgánů různých členských států.

o) mezinárodní organizace – zde figuruje zasahující nadnárodní prvek, který přesahuje hranice nejen jednoho, či více států, ale celé Evropské unie. Právní úprava zde podléhá legislativě mezinárodního práva veřejného.

a samozřejmě některé další pojmy, které však nejsou pro zaměření této diplomové práce toliko relevantními.

5.6 Základní zásady zpracování osobních údajů

Jako každá jiná právem upravovaná oblast, tak samozřejmě i ochrana osobních údajů a jejich zpracování musejí mít určitý pevný základ, který bude poskytovat základní aplikační vodítka a určovat hranice, jaké operace s osobními údaji jsou možné, kým a jakým způsobem. K tomuto slouží základní pávní zásady, jiným slovem principy či ideje, kterými jsou následující [53]:

a) zákonnost – tato základní zásada je jednou z nejdůležitějších vůbec. Je alfou a omegou celé právní úpravy nejen Nařízení GDPR, ale kompletně celé oblasti ochrany osobních údajů. Důležitým aspektem je zde tzv. právní důvod. Právním důvodem se v obecné teorii rozumí určitá skutečnost, která legitimně opravňuje subjekt (v tomto případě obecný subjekt práva) k dlouhodobému výkonu dané činnosti, případně k provedení jen určitého, jednorázového úkolu. V případě správce osobních údajů se promítá zásada zákonnosti v nutnost existence minimálně jednoho právního důvodu, aby mohl tyto údaje zpracovávat. Pokud právní důvod

[53] Obecné nařízení GDPR, článek 6

od počátku absentuje, či zcela zanikne, správce musí veškeré údaje, s kterými nakládal, zlikvidovat. Nařízení GDPR údává jako právní důvody tyto [54]:

„*Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu*:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“

b) korektnost – zásada korektnosti ukládá správci údajů povinnost vůči subjektu osobních údajů postupovat profesionálně, v souladu s obecnou zásadou dobré správy, a to zejména v případě poskytování informací, z jakého důvodu a jakým způsobem bude s osobními údaji nakládáno, a nikterak nezatajovat účel zpracování osobních údajů. Stručně vzato, tato zásada (v návaznosti na zásadu předchozí – zákonnost) zakotvuje a upevňuje princip postupovat pouze ex lege, nikoli praeter legem, či dokonce contra legem, popřípadě in fraudem legis.

c) transparentnost – princip transparentnosti (průhlednosti) spočívá v možnosti subjektu osobních údajů ke snadnému přístupu k informacím, které jsou mu poskytovány správcem údajů. Transparentnost však úzce hraničí s rizikem, kdy se

[54] Obecné nařízení GDPR, článek 6

průhlednost a dostupnost dostává do sféry narušení nebo porušení hranice ochrany osobních údajů a ty poté mohou být snadněji zneužitelnými.

d) minimalizace údajů – zde plyne nutnost postupovat při zpracovávání osobních údajů bezpečně, přiměřeně, omezeně pouze k danému konkrétnímu účelu, z minimálně jednoho konkrétního důvodu a jen v nezbytném rozsahu.
e) omezení účelu – tzv. účelové omezení zakotvuje nutnost nakládání a zpracovávání osobních údajů pouze legálním způsobem (viz zmínka výše) a pouze pro konkrétní, předem vyjádřené a stanovené důvody.

f) přesnost – osobní údaje by měly být aktualizovány a zpracovávány ve své přesné, odpovídající podobě. Správce však není povinen přezkoumávat veškerou správnost údajů, v jeho kompetenci je možnost korekce zjevných gramatických chyb, překlepů, atp.

g) omezení uložení – zásada rámcově určuje dobu, po kterou by měly být osobní údaje ukládány. Tato doba je stanovena jako nezbytně nutná co do okamžiku naplnění účelu či odpadnutí důvodu pro zpracování.

h) integrita, důvěrnost – neboli také celistvost, hraje v tomto případě roli v otázce zejména technického zabezpečení systémů, kde se osobní údaje uchovávají. Je zde požadavek řádného zabezpečení a zároveň dostupnosti.

5.7 Důvody zpracování

Aby osobní údaje subjektu mohly být legálně zpracovávány a následně používány, musí existovat platná, legitimní právní skutečnost, která zakládá na základě toho více či méně konkrétní právní důvod pro zpracovávání a další činnosti. Těmito právními důvody jsou buďto souhlas samotného subjektu zpracovávaných údajů, plnění smlouvy či zákonem uložené povinnosti, ochrana životně důležitých zájmu subjektu údajů, plnění úkolu orgány veřejné moci/ve veřejném zájmu a správce je tímto pověřen anebo v případě oprávněných zájmů správce případně další, též oprávněné třetí strany [55].

[55] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 67

5.8 Působnost Nařízení GDPR

Stejně tak, jako u všech ostatních právních předpisů, tak i u tohoto je možné rozlišit celkem 4 okruhy působnosti a to osobní (personální), místní (teritoriální/prostorová), věcnou (meritorní) a časovou (temporální). Lze vymezit též výjimky, ve kterých se Nařízení neaplikuje [56].

5.8.1 Osobní působnost

Osobní působnost vymezuje subjekty = adresáty, na něž se Nařízení, resp. práva a povinnosti z něj plynoucí, vztahuje. Těmito subjekty jsou správci, zpracovatelé, samotné subjekty osobních údajů – tedy fyzické osoby, dozorové úřady a Evropský sbor pro ochranu osobních údajů. Mimo tyto lze zařadit mezi adresáty i samotné členské země Evropské unie, kterým Nařízení v některých situacích nechává možnost upravit dané oblasti vlastní právní úpravou odlišně či naopak nařizuje opatřit konkrétní, speciální zákonnou úpravu [57].

5.8.2 Místní působnost

Místní působnost vyjadřuje prostor, ve kterém se právní předpis uplatňuje. Materie Nařízení se tak vztahuje jednak na členské státy Evropské unie a jednak také na Evropský hospodářský prostor (tedy i na Norsko, Island a Lichtenštejnsko, které nejsou členskými zeměmi). Otázkou zůstává, jak bude situace řešena v případě Brexitu. Velká Británie se zavázala Nařízením řídit i nadále, změnilo by se však její postavení jako již nečlenského státu – na toto bohužel nejde stále odpovědět, jelikož otázka není plně dořešena.

5.8.3 Časová působnost

U tohoto druhu působnosti se typicky rozlišují dva základní pojmy teorie práva a těmi jsou platnost a účinnost právního předpisu. Pro ucelení podkapitoly autorka práce oba pojmy stručně shrne. Nařízení GDPR je platným okamžikem jeho vydání a publikací v Úředním věstníku Evropské unie, konkrétně dnem 24. května 2016, účinným se Nařízení stalo o dva

[56] Zpracování při činnostech, které nespadají do působnosti práva EU; Zpracování při činnosti související s politikou kontrol na hranicích, azylu a přistěhovalectví; Zpracování fyzickou osobou pro osobní a domácí potřebu; Příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání TČ nebo výkonu trestů, vč. ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení (Zpracování upraveno v směrnici č. 2016/680) – viz dokument *Obecné Nařízení ochrany osobních údajů (GDPR) ve veřejné správě*, autor Mgr. Michal Nulíček, LL.M.; společnost ROWAN LEGAL; Plenární zasedání Rady vlády pro informační společnost, Praha, 9. 9. 2016, dostupné pdf online: http://www.mvcr.cz/soubor/3-zasedani-rvis-zapis-rvis-09-09-2016.aspx [online]. [cit. 2019-02-08]

[57] viz například článek 6, odstavec 3 Nařízení GDPR – členské státy musí vnitrostátním právním předpisem upravit zřízení a záležitosti dozorového úřadu - ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 36

roky později, tedy 24. května 2018. Tímto okamžikem se stalo přímo použitelným (přímo aplikovatelným pro adresáty) a tím pádem i přímo vynutitelným. Mezi daty běžela tzv. legisvakanční lhůta, která slouží adresátům právního předpisu k zajištění dostatečného času na seznámení s předpisem a k zajištění všech potřebných změn v souvislosti s jeho přijetím a pozdější účinností [58].

5.8.4 Věcná působnost

Věcný okruh působnosti se vztahuje na vymezení, čeho všeho se daný právní předpis týká, jaké oblasti upravuje a jaké naopak nechává mimo své pole působnosti (viz také pozitivní a negativní vymezení věcné působnosti). Příručka Jiřího Žůrka trefně shrnuje věcné působení Nařízení GDPR jako [59]: „*Obecné nařízení se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.*“ Z této citace je možné zpozorovat obojí možnost vymezení – jak pozitivní, tak rovněž i negativní. Zpracování osobních údajů částečně či plně automatizovaně (registry, cloudová úložiště, atp.) nebo neautomatizovaně (klasické neelektronické kartotéky např. u lékařů) zakládá neutrální plochu věcné působnosti.

5.9 Práva subjektu údajů

Práva subjektu údajů vyvažují nerovnosti, které mohou vyvstávat v rámci administrativněprávních vztahů veřejné správy (resp. veřejné moci) a činnosti jejích orgánů, vznikajících při aplikaci tohoto předpisu. Některé údaje jsou subjekty orgánům veřejné správy povinny poskytovat, proto zde musí být určitý systém brzd, který bude pro subjekty protiváhou a jistou garancí v ohledu na ochranu osobních údajů. Důležitá je znalost práv nejen ze strany samostatného subjektu, ale i ze strany zpracovatele – a to zejména pro možnost plného uplatnění těchto práv. Znalostí se předchází neinformovanosti na obou stranách a tak i možnému porušení jejich ochrany a uložení adekvátní sankce. Zajištění výkonu práv subjektů je jednou z podmínek pro soulad postupu zpracovávaných údajů [60].

[58] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 40
[59] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 36
[60] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 130

Práva subjektu podle výše uvedené charakteristiky jsou následující [61]:

- právo na informace
- právo na přístup k osobním údajům
- právo na opravu a doplnění
- právo na vymazání = „právo být zapomenut“
- právo na omezení zpracování
- oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování
- právo na přenositelnost údajů
- právo vznést námitku
- právo nebýt předmětem automatizovaného individuálního rozhodování
- omezení práv a zásad zpracování

5.10 Kodexy chování

Novinkou, kterou přineslo Nařízení GDPR, konkrétně jeho články 40 a 41, jsou tzv. Kodexy chování. Jednoznačnou a kvalitní definici těchto dokumentů není prozatím v odborné literatuře snadné (možné) dohledat, autorka práce se tak pokusí naložit s dostupnými informacemi [62] o Kodexech chování a pokusí se alespoň rámcově tyto dokumenty popsat a charakterizovat.

Kodexy chování lze charakterizovat jako základní dokumenty směřující k naplňování zásady dobré správy v oblasti dodržování jednotlivých ustanovení Nařízení GDPR a jejich následné aplikace na konkrétní případy. Jsou to účelová sepsání bodů, které musí zpracovatel či správce (jež se ke konkrétnímu Kodexu určitého typu dobrovolně přihlásil) naplnit, aby dostál všech legálních požadavků na operace s osobními údaji subjektů [63].

Přínosem pro správce a zpracovatele je, že pokud jsou Kodexem oficiálně vázáni, mohou se odvolávat, že své povinnosti plní v souvislosti s Nařízením. Jsou tedy důležitým nástrojem, který by měl garantovat profesionalitu správců a zpracovatelů údajů.

[61] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 130
[62] informace viz https://www.uoou.cz/kodexy-chovani/d-29493/p1=4753 [online]. [cit. 2019-02-08]
[63] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 168

Kodexy chování, či jejich případné změny, schvaluje místně příslušný dozorový úřad. Ten ke kodexu může vznést připomínky či návrhy, anebo jej rovnou schválit. Kodex je možné vytvořit i pro více členských států, v tomto případě jej schvaluje Evropský sbor pro ochranu osobních údajů. V současné době jsou již používány Kodexy v oblasti přímého marketingu (FEDMA) či poskytovatelů cloudových úložišť [64]. V nejbližší době by měl být dokončován též Kodex chování v oblasti ochrany soukromí pro aplikace pro mobilní zdraví [65].

Podobně jako Kodexy chování jsou zpracovávány další dokumenty a to jednak tzv. Osvědčení (vydávání osvědčení, pečetí a známek osvědčující ochranu osobních údajů pro účely prokázání souladu zpracování) a jednak tzv. Vnitřní koncepce (politiky) ochrany osobních údajů (závazný dokument pro zaměstnance) [66].

5.11 Sankce

Je logické, že pokud právní předpis obecně stanovuje jakékoli povinnosti, může požadovat v případě nesplnění těchto povinností vynucení ze strany orgánu veřejné moci – státního (případně nadstátního) orgánu, které přichází v podobě sekundární povinnosti sankční povahy. Toto obecné schéma vychází již z klasické právní teorie, kdy je právní norma strukturována jako trichotomický (někdy i tetrachomický) vzorec: Hypotéza – Dispozice (eventuálně mezistupeň – Porušení dispozice) – Sankce. Právě sankce mají působit ideálně preventivně, a pokud k porušení reálně dojde, pak i nápravně a pro poškozenou stranu satisfakčně.

Nařízení GDPR též obsahuje sekundární povinnosti sankční povahy, pokud dojde k porušení jiných, daných ustanovení. Maximální výše částky, kterou je možné uložit, dosahuje 20 000 000 Euro, či 4% celkového ročního obratu, jedná-li se o podnik [67].

Výše sankčních opatření – tedy uložených pokut, se však člení do dvou základních skupin a to [68]:

a) do výše 10 000 000 EUR (nebo až do 2% celkového ročního celosvětového obratu, jde-li o podnik) Tato porušení, za které se ukládají pokuty s nižší sazbou, jsou s menší mírou

[64] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 168
[65]https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised [online]. [cit. 2019-02-08]
[66] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 173
[67] Obecné Nařízení GDPR, článek 84
[68] https://www.uoou.cz/11-sankce-pokuty/d-27287 [online]. [cit. 2019-02-08]

závažnosti (například porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, při porušení podmínek týkajících se jmenování a podmínek pověřence, povinnosti týkající se činnosti při získávání osvědčení, a další)

b) do výše 20 000 000 EUR (nebo až do 4% celkového ročního celosvětového obratu, jde-li o podnik). Tato skupina s přísnějším sankčním postihem se vztahuje na takové případy, kdy porušení dané povinnosti způsobuje těžší následek zásahu do sféry osobních údajů (zejména porušení podmínky souhlasu se zpracováním osobních údajů, citlivých údajů, porušení zásad a zákonnosti zpracování, porušení podmínek při předávání osobních údajů do třetí země, atp.).

Při ukládání pokut mohou hrát roli též tzv. polehčující či přitěžující okolnosti (povaha a závažnost porušení, délka porušení, zdali bylo porušení vědomé anebo nedbalostní, míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků, kategorie osobních údajů dotčené daným porušením, a další).

5.12 GDPR a Česká republika

Stav legislativy na poli ochrany osobních údajů v České republice nebyl téměř až do přelomu devadesátých let a milénia samostatně řešen. Do roku 2000 (konkrétně do 1. června 2000) neexistoval jednotný zákon, který by tuto oblast upravoval. Až přijetím zákona č. 101/2000 Sb., o ochraně osobních údajů, který je i nadále stále ještě účinný, je možné považovat ochranu osobních údajů a jejich zpracovávání za kompletní. Tato právní úprava přijala a zakotvila Úřad pro ochranu osobních údajů jako dozorový orgán [69].

Před přijetím a účinností výše zmíněného zákona upravoval problematiku zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Tento zákon však upravoval jen a pouze osobní údaje zpracovávané v elektronicky vedených informačních systémech, nikoli tedy v klasických, dříve běžně psaných a spíše vedených „papírových" evidencích. Zákon dokonce byl přijat dříve, než samotná Listina základních práv a svobod, která ve svém 10 článku, odstavci 3 zakotvuje ochranu osobních údajů na ústavní úrovni. Zde tedy zákonná úroveň předběhla úroveň, z hierarchie právního řádu, výše postavenou a to právě úroveň ústavní [70].

[69] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 18
[70] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 18

5.12.1 Adaptační zákon

Nynější zákon o ochraně osobních údajů (zákon č.101/2000 Sb.) musel se vstupem České republiky do Evropské unie projít v roce 2004 novelizací, v souvislosti s nutností transpozice Směrnice 95/46/ES. Ke dni účinnosti (použitelnosti, jak uvádí ono samotné) Nařízení GDPR, měl být tento zákon zrušen a měl být zároveň přijat tzv. adaptační zákon (zákon o zpracování osobních údajů), jehož úkolem mělo být přizpůsobení těch částí právního řádu, kterých se přijetí Nařízení přímo dotýká. Situace kolem adaptačního zákona však nabyla na aktuálnosti až v březnu letošního roku, tedy 2019.

Adaptační zákon nemá být pouze nástrojem k provedení Nařízení do českého práva a právního řádu, ale i prostředkem úpravy těch oblastí, které nechává Nařízení GDPR benevolentněji v dikci členských států [71]. Mimo tato fakta má být adaptační zákon také prostředkem pro stanovení rámcové hranice mezi právem ochrany osobních údajů a právem na svobodu projevu a informace, či má zakotvit aspekty zpracování osobních údajů pro účely výkonu svobody vědeckého a akademické bádání a umělecké tvorby a projevu [72].

Peripetie okolo přijímání adaptačního zákona, více než 6 měsíců po účinnosti Nařízení GDPR, byly ukončeny v prosinci roku 2018, kdy jej Poslanecká sněmovna ve svém 3. čtení schválila [73]. Po schválení Poslaneckou Sněmovnou však nastalo další zpoždění a to ze strany Senátu, který návrh zákona vrátil Poslanecké sněmovně s pozměňovacími návrhy. Zákon je aktuálně ke 12. březnu 2019 již přijat a nyní se již čeká na vyhlášení ve Sbírce zákonů.

Jedním z důležitých aspektů tohoto zákona je vymezení přestupků a výše jejich pokut pro veřejnoprávní subjekty. Zde došlo k omezení horní hranice uložených sankcí na 10 milionů korun (Nařízení GDPR stanovuje pokutu až do maximální výše 20 milionů EUR). Změnový zákon zároveň postihne úpravu 19 zákonů, jejichž obsah bude nutné přizpůsobit [74].

---

[71] Například stanovené odlišné věkové hranice mladistvých (GDPR 16 let) při udělování souhlasu se službou informační společnosti. Členský stát by si tak mohl stanovit věkovou hranici odlišně. Viz ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 20

[72] https://www.uoou.cz/1-obecne-narizeni/d-27266/p1=4744 [online]. [cit. 2019-02-08]

[73] Dle předpokladů by se tak mělo stát cca v první čtvrtině roku 2019. Viz https://www.pravniprostor.cz/clanky/ostatni-pravo/adaptacni-zakon-ke-gdpr

[74] https://drive.google.com/file/d/1DSF-HPQyLAPD65Ke5pZ_rpwPpNDEBSmZ/view [online]. [cit. 2019-02-08]

5.13 Dozorový úřad

Nezbytně nutné je do této části diplomové práce zařadit i nezávislý orgán veřejné moci, který je zřízen každým členským státem a to podle článku 4, bodu 21 a článku 51 ad. Nařízení GDPR. Jedná se o orgán (úřad), který vykonává určitý druh dohledu nad zpracováním osobních údajů fyzických osob, tedy subjektu údajů, a chrání tak jejich práva s tím spojená. Prostorová působnost je spojená s územím daného státu, kde konkrétní úřad působí – v České republice se jedná o Úřad pro ochranu osobních údajů, jehož úkoly jsou podle samotného Úřadu následující [75]:

„Úřad pro ochranu osobních údajů (ÚOOÚ) je nezávislým orgánem, který:

- *Provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů.*
- *Vede registr povolených zpracování osobních údajů.*
- *Přijímá podněty a stížnosti občanů na porušení zákona.*
- *Poskytuje konzultace v oblasti ochrany osobních údajů.*

Činnost Úřadu je vymezena zákonem č. 101/2000 Sb., o ochraně osobních údajů o změně některých zákonů, a některými dalšími zákony (detailně v rubrice Působnost Úřadu).

*Smyslem zákona o ochraně osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života **a** neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů. V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno.*“

Co se týče jednotlivých úkolů, jedná se hlavně o monitoring. Pravomoci Úřadu jsou však mnohem širší. Celkově by se daly shrnout do 4 základních bloků a to – **vyšetřovací** pravomoci, **nápravné**, **povolovací** a pravomoci **poradní**. Každý tento jednotlivý blok se vyznačuje svými specifickými pravomocemi. Vyšetřovací, jež jsou těmi základními, jsou například provádění auditů ochrany osobních údajů, ohlašování porušování Nařízení správcům, získávání osobních údajů pro konkrétní legální účely přístup k osobním údajům. Mezi pravomoci nápravné patří upozorňování na porušování Nařízení, udělování napomenutí, ukládání dočasných nebo trvalých omezení a opatření, a další. Povolovací pravomoci znamenají například samotné povolování zpracování údajů, vydávání osvědčení, povolování

[75] https://www.uoou.cz/urad/ds-1059/p1=1059 [online]. [cit. 2019-02-08]

a schvalování dalších činností vůči subjektům či třetím stranám, poskytování poradenství a další [76].

5.14 Dotazníkové šetření veřejného mínění

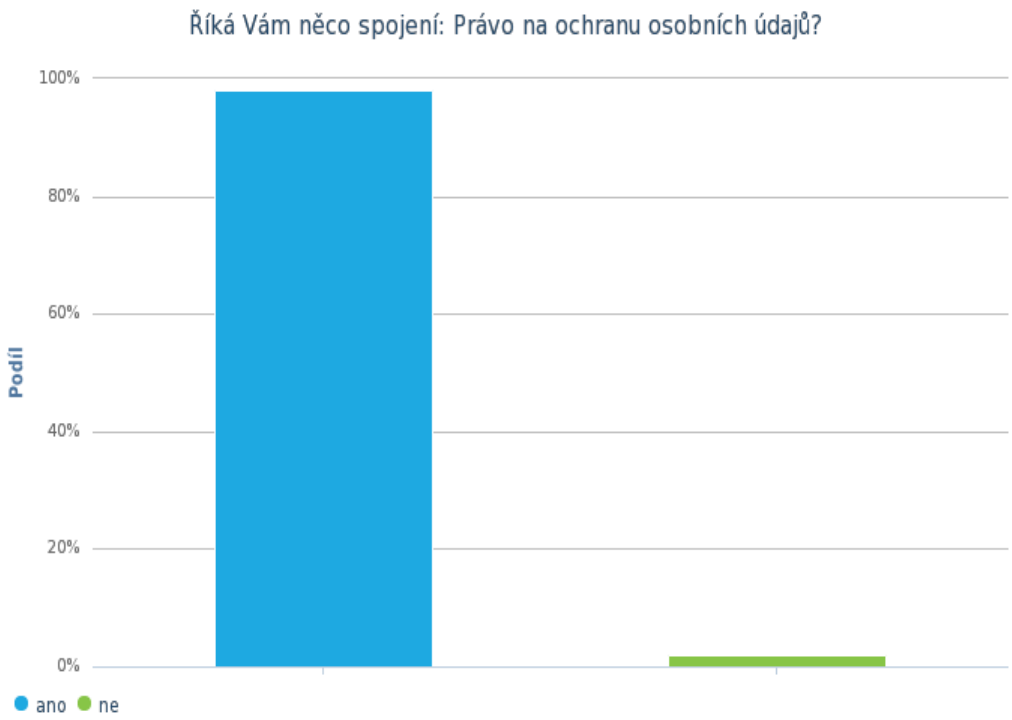
Pro ilustrační doplnění je v této podkapitole graficky zhodnocena a nastíněna aktuální situace, mapující vnímání a povědomí české veřejnosti v problematice ochrany osobních údajů. Z vlastního dotazníkového šetření autorky, které bylo zaměřeno na základní otázky ohledně osobních údajů a Nařízení GDPR (konkrétně položení otázek znalostí institutů Práva na ochrany osobních údajů a Nařízení GDPR), plyne obecná znalost obou těchto pojmů, alespoň svou základní materií („ o co se jedná, když se pojmy vysloví“).

Z celkem stovky respondentů, kdy se jednalo zhruba z poloviny o ženy a z poloviny muže, ve věkovém rozmezí cca mezi 20-55 lety, středoškolsky až vysokoškolsky vzdělané osoby (převážně v oborech zdravotnictví, školství, veřejné správy a práva, ekonomie a technických oborů, aplikované vědy, elektrotechnické vzdělání., strojírenství) odpovědělo na první otázku, týkající se znalosti pojmu práva na ochranu osobních údajů, celkem 98% kladně. Na otázku druhou, týkající se pojmu Nařízení GDPR (znalost a účel Nařízení) odpovědělo kladně 96% dotázaných.

Oba grafy jsou doloženy na následující straně.

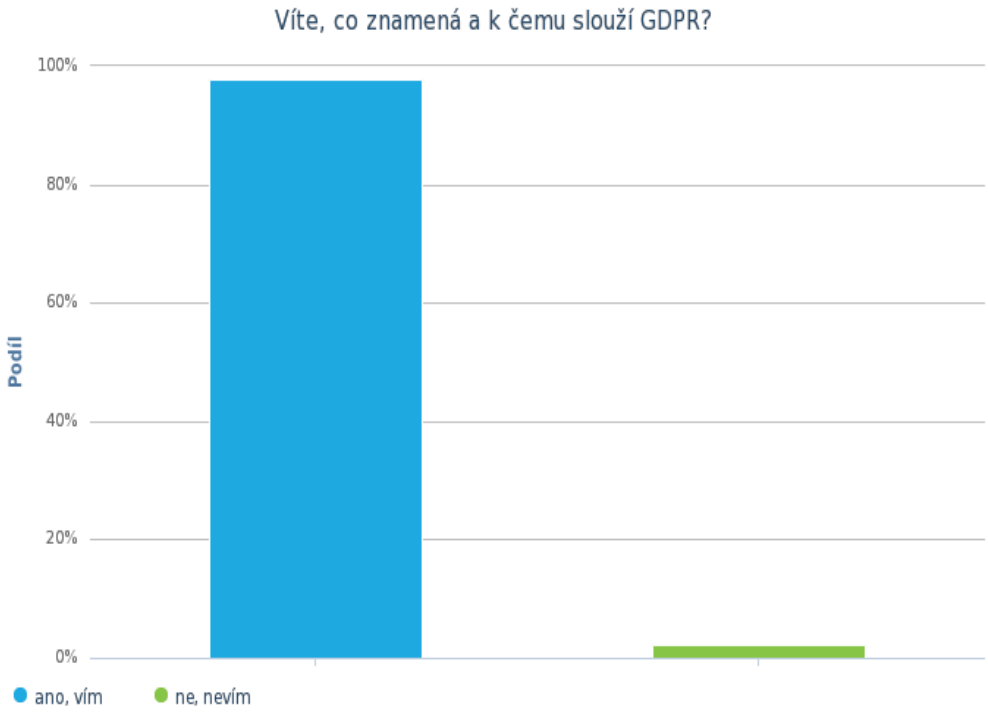
[76] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 175

Graf číslo 2: Co znamená pojem Právo na ochranu osobních údajů



Zdroj: vlastní výzkum pomocí online vytváření grafů na www.survio.com

Graf číslo 3: Co znamená pojem GDPR



Zdroj: vlastní výzkum pomocí online vytváření grafů na www.survio.com

6. GDPR VE VEŘEJNÉ SPRÁVĚ I. – teoretická část

V moderních společnostech a systémech, kde se prakticky téměř veškeré jejich fungování více či míně automatizuje a přechází se na IT technologie a řízení (management), je nezbytné, aby veškerá data (ať už se jedná o data nesoucí informace o osobách – osobní údaje, či jiná data v obecném slova smyslu) procházela v různých procesech určitým zpracováním a přenosem z jednoho subjektu jinému. Dalo by se říci, že v tomto kontextu není podstatné, zda se jedná o procesy v rámci prostoru vnitrostátního či prostoru přesahující hranice určitého státu [77].

Co je však základními důležitými aspekty těchto procesů a obecně pravidly nakládání s osobními údaji? Jednak bezesporu snaha o vykompenzování práva subjektů na ochranu soukromí každého a legální zásah do tohoto práva, poté bezesporu stanovení přesných a přísných pravidel pro případy zpracovávání osobních údajů subjektů a zmínit je vhodné též nutnost kvalitní právní úpravy na tomto úseku.

Tato kapitola, s obsahovým zaměřením zejména na teoretickou část, se bude věnovat hlavnímu jádru tématu celého zaměření diplomové práce a to – jakým způsobem zasáhlo Nařízení GDPR do prostoru veřejné správy (zejména územní samosprávy základních územních samosprávných celků i vyšších územně samosprávných celků).

Veškeré dění, jenž se ve veřejné správě odehrává (tedy veškeré činnosti veřejné správy v jejím materiálním hledisku), se děje pomocí nejrůznějších procesů, ve kterých dochází k manipulaci s rozmanitými údaji a daty, mezi která se nepochybně řadí právě i osobní údaje. Ať již se jedná o agendy spadající do dikce státní správy, jako jsou například určité oblasti školství, životního prostředí, dopravy, zdravotnictví, kultury, bezpečnosti obyvatelstva a další, či agendy na úseku samosprávy (zejména té územní, případně samozřejmě i profesní, eventuálně zájmové), s příchodem Nařízení GDPR tak bylo nutné se vypořádat s určitými změnami a vyvstalými úkoly.

6.1 Úskalí veřejné správy po účinnosti GDPR

Z povahy jádra věci tedy vyvstává několik základních, avšak zásadních a aktuálních otázek a problémů, se kterými se veřejná správa (včetně eGovernmentu) musela v souvislosti s přijetím Nařízení GDPR vypořádat. Níže autorka diplomové práce vybrala několik z nich -

[77] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9. Str. 8

základních, avšak nikterak zanedbatelných, které budou v následujících částech, případně dalších kapitolách práce blíže a detailněji popsány.

1. Zřízení efektivních Metodik pro aplikaci Nařízení pro jednotlivé orgány státní správy i samosprávy
2. Zabezpečení chodu informačních a komunikačních technologií, zejména softwarových systémů, potažmo webů a intranetů veřejné správy, kde budou osobní údaje ukládány, spravovány a kde s nimi bude operováno
3. Zabezpečení informovanosti klientů veřejné správy tak, aby dostála zásada efektivní a dobré správy svého standardu

6.2 Metodiky orgánů státní správy, samosprávy

Prvý okruh, kterým se tato podkapitola práce bude zabývat, se týká problematiky zpracovávání Metodik k aplikaci Nařízení GDPR. Metodiky by měly fungovat jako jakási pomocná vodítka, která pomohou zaměstnancům veřejné správy, kterých se problematika ochrany osobních údajů týká, při výkonu náplně jejich služebních činností. Jejich hlavním cílem je tak zjednodušit aplikaci Nařízení v konkrétní oblasti a mohou obsahovat i příklady nejčastějších možných praktických situací, které mohou v souvislosti s touto činností nastat. Tyto Metodiky jsou určeny všem (zaměstnancům či dalším dotčeným osobám), kteří v dané instituci provádí úkony spojené s osobními údaji subjektů.

Metodika Ministerstva školství, mládeže a tělovýchovy je například určena konkrétně pro [78]: *„Metodika je adresována všem osobám, které v rámci své činnosti v oblasti školství přicházejí do styku s problematikou osobních údajů. Může se jednat například o:*

- *ředitele škol a školských zařízení,*
- *rektory vysokých škol a další akademické pracovníky,*
- *učitele,*
- *hospodáře a účetní škol,*
- *zaměstnance krajských a obecních úřadů,*
- *správce sítě, jiné pracovníky IT a další.“*

Metodiky mohou obsahovat kromě základních informací, postupů a nejčastějších praktických příkladů také specifická doporučení, čemu se v případě ochrany osobních údajů

[78] http://www.msmt.cz/file/44569/ [online]. [cit. 2019-02-08]

raději vyvarovat, čemu věnovat zvýšenou pozornost, nebo jaká další opatření v případě zpracovávání a shromažďování údajů je třeba učinit.

Tyto pomocné dokumenty vytvářejí především orgány státní správy, není však vyloučeno, aby je zpracovávaly i jiné veřejnoprávní subjekty, jako například Svazy měst a obcí České republiky. Mezi orgány státní správy zpracovávající Metodiky aplikace se řadí především jednotlivá Ministerstva dle daného resortu [79].

V jednotlivých dokumentech, právě kupříkladu Ministerstev, se mohou vyskytovat i odkazy na užitečné webové adresy, které mohou uživatelům a adresátům Metodik pomoci v další orientaci problematiky ochrany osobních údajů.

Jedním z cílů Metodik je zejména také prevence a ochrana před sankcemi, které mohou být uloženy v případě porušení určité povinnosti dané právním předpisem. Sankce nemají být ukládány v likvidační výši, měly by být zejména ochranným prostředkem a důsledkem, který by měl vést k lepší prevenci, avšak i přes tuto teorii mohou být sankční částky ukládány v nemalé, naopak velmi citelné výši.

Shrnou-li se důvody, pro které orgány veřejné správy Metodiky vypracovávají, jsou to v kostce tyto:

- lepší informovanost zaměstnanců veřejné správy
- pomoc při aplikaci Nařízení GDPR
- předcházení negativním situacím – prevence
- praktické informace pro použití
- doporučení uživatelům (= zaměstnancům veřejné správy)

Přestože tyto dokumenty tvoří pomocný pilíř pro lepší orientaci a aplikaci v Nařízení, odborníky z praxe bývají kritizovány, jelikož nebyly poskytnuty svým adresátům jednak s dostatečným časovým předstihem a jednak byly i vzneseny názory, že sice tvoří pomocné nosiče informací, avšak značně neúplné, příliš obecné, někdy až údajně nepoužitelné [80].

[79] https://www.uoou.cz/zverejnene-metodiky/d-28765/p1=3938 [online]. [cit. 2019-02-08]

[80] „*Když si vezmeme v úvahu jenom zdravotnictví, které patří z pohledu GDPR k těm nejsložitějším oborům, tak jediné, na co se během tohoto roku ministerstvo zmohlo, bylo vydat metodiku, která je tak obecná, že je ve svém důsledku pro jednotlivé zdravotnické organizace nepoužitelná. Některá ministerstva či jiné státní instituce začínají až teď na konci roku 2017 prohlašovat, že je na přípravu spoustu času a metodiky poskytnou v průběhu prvního pololetí roku příštího. Takové prohlášení je pro mne pouze utvrzením v tom, že absolutně nechápou rozsah dopadu GDPR, protože jen samotná implementace pravidel nařízení ve složitějších organizacích může trvat i několik měsíců až let*“ – slova Mgr. Evy Šimáčkové, citováno online

6.3 ICT v prostředí veřejné správy v kontextu ochrany osobních údajů

6.3.1 Kyberprostor obecně

Prostředí veřejné správy se již několik let v procesu její modernizace globalizuje do virtuálního prostředí informačních a komunikačních technologií. Tento proces, který je ovlivněn celosvětovým technologickým pokrokem, by měl znamenat zejména zvýšení efektivnosti, rychlosti, přístupnosti a snižování nákladů (jak materiálních (finance), tak nemateriálních (čas)) veřejné správy vůči svým klientům. S těmito modernizačními procesy jsou ovšem spojena značná rizika. S rostoucí inteligencí moderních technologií úměrně roste i tzv. kyberkriminalita (dříve počítačová kriminalita). Jedná se trestné činy nejrůznějšího druhu nejen v prostředí internetu, ale i v prostředí informačních a komunikačních technologií v rámci veřejné správy (eGovernmentu).

Samotní odborníci v oboru kybernetické bezpečnosti namítají, že situace se nejvíce zhoršila kolem roku 2014, kdy počet a objem škod způsobených útoky v oblasti informačních a komunikačních technologií masově narostl a například v bankovním sektoru se řádově škody pohybovaly až ve stovkách milionů korun. Mimo to chybí České republice také dostatek odborníků v inkriminované oblasti, kteří by byli schopni dostatečným způsobem analyzovat situaci a navrhnout adekvátní a konstruktivní řešení, které by v určitém časovém horizontu mohlo vést ke zlepšení situace [81].

Mimo zákon o kybernetické bezpečnosti a vyhlášku provádějící tento zákon se spoléhá právě na Nařízení GDPR, které by teoreticky vzato mohlo mít za následek snížení kyberkriminality a mělo by přispět k větší prevenci před zneužíváním osobních údajů a dat v sektoru veřejném i soukromém [82].

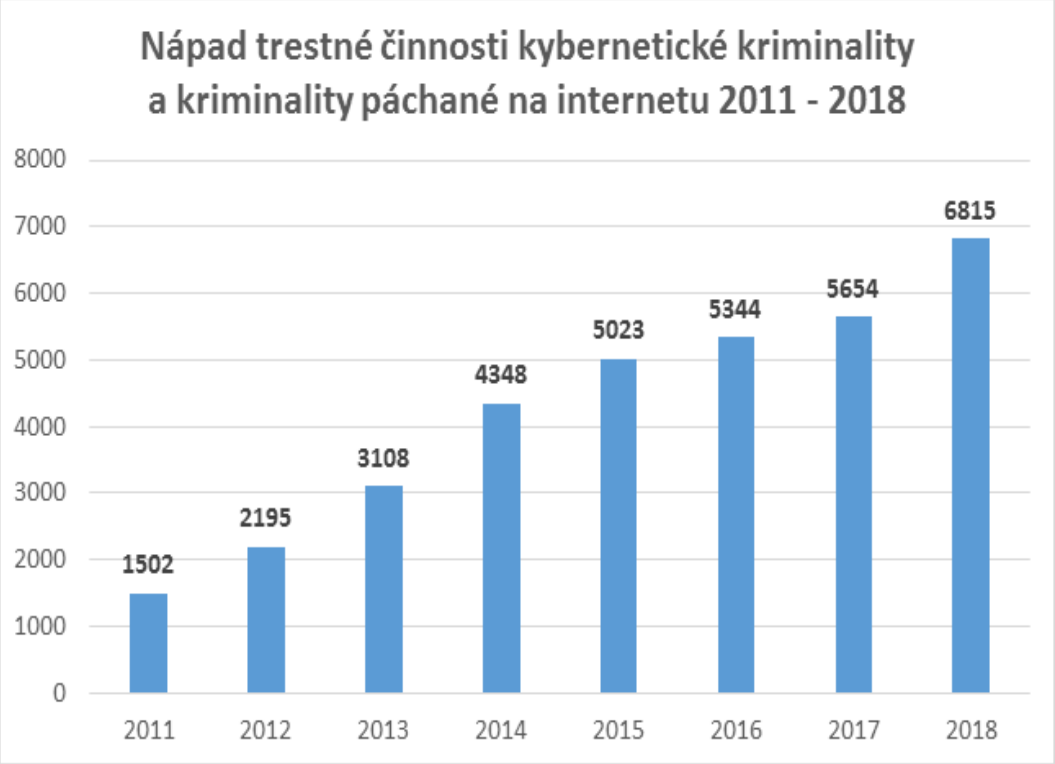
Podložit fakt, že kyberkriminalita je nebezpečným fenoménem, který markantně narostl mezi lety 2013-2014 a podruhé nejvíce meziročně i v letech 2017-2018, lze například ze zjištění Ministerstva vnitra (konkrétně Policie ČR) – viz graf na následující straně:

http://www.efektivnepodnikat.cz/gdpr/lucie-skornickova-v-zavadeni-gdpr-v-cr-selhala-statni-sprava [online]. [cit. 2019-02-08]

[81] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5 Str. 12

[82] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5 Str. 12

Graf číslo 4: Kyberkriminalita 2011-2018



Zdroj: https://www.policie.cz/clanek/kyberkriminalita.aspx

6.4 Ochrana osobních údajů v eGovernmentu

Co se ochrany osobních údajů týče, Nařízení GDPR se vztahuje na shromažďování, zpracování a ukládání osobních údajů v rámci své věcné působnosti na de facto „veškerý prostor“, tedy na nejen prostředí reálné, ale i to virtuální. Otázky související s tím, jak si poradil eGovernment s opatřeními, které vyvstaly s nutností zvýšené ochrany osobních údajů, budou analyzovány v této podkapitole.

Jelikož prostředí eGovernmentu čítá, stejně tak, jako institucionální veřejná správa, nesčetně oblastí a podoblastí, pro lepší a konkrétnější demonstraci si autorka diplomové práce vybrala otázky aktuálního fungování Czech POINTu [83] a základních registrů v souvislosti s přijetím Nařízení.

[83] (tedy Český Podací Ověřovací Informační Národní Terminál). – myšlenka CzechPOINTU spočívá v efektivitě elektronizace veřejné správy a tím pádem k lepšímu přístupu občana k jednotlivým dokumentům, potřebným k vyřizování nejrůznějších agend. Zdroj: ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 18

6.4.1 Czech POINT

Osobními údaji v rámci systému Czech POINT jsou převážně druh a číslo osobního dokladu subjektu (tedy typicky občanský průkaz), osobní údaje jako jméno a příjmení, trvalé bydliště a další jsou poté získávány pomocí přístupů v rámci propojení se základními registry. Důležité je zmínit, že osobní údaje subjektu, které jsou nutné k vyřízení požadovaného úkonu, nejsou tímto systémem nijak dále zpracovávány a ukládány. Výjimku tvoří komunikace přes datové schránky, kde se v tomto elektronickém úložišti schraňují údaje o subjektech po dobu 90 dní [84] . Funkce kontroly v tomto případě vykonává Úřad pro ochranu osobních údajů.

Souhlas s poskytováním osobních údajů nečiní subjekt zvlášť, informovanost je zajištěna prostřednictvím kontaktních míst veřejné správy a prostřednictvím webových stránek terminálu. Některé dokumenty však archivaci podléhají (například plné moci při žádostech o výpis z Rejstříku trestů). V zásadě jde o tři evidence, podléhající archivaci, podle zákonných ustanovení [85], jsou jimi:

- evidence vydaných výstupů (neevidují se samotné výpisy)
- evidence provedených konverzí
- evidence o zprostředkované identifikaci

Kontaktními místy veřejné správy jsou realizovány i další agendy [86]:

- Výpis z veřejného rejstříku
- Výpis z katastru nemovitostí
- Snímek z katastrální mapy
- Výpis z Rejstříku trestů pro právnické osoby
- Výpis z živnostenského rejstříku
- Výpis ze seznamu kvalifikovaných dodavatelů
- Provedení identifikace a sepsání veřejné listiny o identifikaci
- Autorizovaná konverze dokumentů z listinné do elektronické podoby
- Autorizovaná konverze dokumentů z elektronické do listinné podoby

Ani v těchto případech Czech POINT neukládá osobní údaje subjektů, identifikační údaje jsou zde ověřovány rovněž ze základních registrů. Zpracování osobních údajů se může

[84] https://www.czechpoint.cz/public/gdpr/ [online]. [cit. 2019-02-08]
[85] § 9b odst. 4 zákona č. 365/2000 Sb., § 26 odst. 1 zákona č. 300/2008 Sb., § 10 odst. 5 zákona č. 253/2008 Sb.
[86] https://www.czechpoint.cz/public/gdpr/ [online]. [cit. 2019-02-08]

týkat subjektu, žádá-li osobně na kontaktním místě veřejné správy, musí být však srozuměn, resp. musí být jednoznačné, za jakým účelem a v jakém rozsahu údaje poskytl [87].

6.4.2 Základní registry

Otázka základních registrů [88] je jednou z nejvíce rozsáhlých oblastí eGovernmentu, je tedy vhodné pokusit se zanalyzovat situaci i zde. Situace a dění okolo základních registrů jsou jedněmi z nejaktuálnějších. Do konce února tohoto roku, tedy do 28. 2. 2019, musely orgány veřejné moci zabezpečit a zkontrolovat nastavení agendových infomačních systémů, které využívají údaje ze základních registrů. Systémy tak musí odpovídat aktuálním zákonným limitům pro nakládání s osobními údaji, kdy hlavním cílem těchto opatření a kontrol je snížení rizik spojených s nezákonným, nelegitimním či nadměrným využívání těchto údajů subjektů [89].

Osobní údaje subjektů patří mezi tzv. referenční údaje, které orgány veřejné moci získávají ze základních registrů (ze základního registru obyvatel). V souvislosti s účinností Nařízení GDPR Ministerstvo vnitra podniklo kroky k většímu zabezpečení, zavedlo přísnější kontroly a doplnilo podmínky při využívání osobních údajů orgány veřejné moci ze základních registrů [90].

Mimo tuto výše popsanou povinnost kontroly je nutné do 29. 6. 2019 stanovit a připravit tzv. „Seznam údajů“, což je určitý rozsah požadovaných údajů, způsobem takovým, aby odpovídal konkrétnímu legitimnímu účelu, pro který jsou údaje získávány, a je s nimi poté dále nakládáno. Následně již nebude možné získávat o subjektech údaje v plném rozsahu, nýbrž jen v tomto, stanoveném daným seznamem[91]. Orgány veřejné moci, jak z tohoto odstavce plyne, musejí mít zákonné zmocnění proto, aby mohly údaje obsažené v základních registrech využívat.

Ministerstvo vnitra, ve spolupráci se správou základních registrů a registrem obyvatel, připravilo Manuál pro kontrolu nastavení oprávnění přístupů k údajům základních registrů,

[87] https://www.czechpoint.cz/public/gdpr/ [online]. [cit. 2019-02-08]
[88] Základní registry jsou specifickým typem informačních systémů veřejné správy fungujících na základě zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Viz. Http://www.szrcr.cz/uploads/Vyvojari/Manua_l_pro_kontrolu_nastaveni_opra_vne_ni_pr_i_stupu_k_u_daju_m_za_kladni_ch_registru_.pdf online [online]. [cit. 2019-02-08]
[89] http://www.szrcr.cz/opatreni-proti-nespravnemu-vyuzivani-udaju-ze-zakladnich [online]. [cit. 2019-02-08]
[90] http://www.szrcr.cz/opatreni-proti-nespravnemu-vyuzivani-udaju-ze-zakladnich [online]. [cit. 2019-02-08]
[91] http://www.szrcr.cz/opatreni-proti-nespravnemu-vyuzivani-udaju-ze-zakladnich [online]. [cit. 2019-02-08]

jehož účelem je nastínit postup kontroly nastavení přístupů k údajům základních registrů. Tento Manuál se vztahuje na neveřejné referenční údaje, kterými jsou v registrech [92]:

- Registr obyvatel (ROB) – všechny
- Registr osob (ROS) – údaje o fyzické osobě podnikatele podle § 61 odst. 2 zákona o základních registrech,
- Registr práv a povinností (RPP) – údaje o právech a povinnostech osob podle § 52 odst. 5 zákona o základních registrech.

[92]http://www.szrcr.cz/uploads/Vyvojari/Manua_l_pro_kontrolu_nastaveni_opra_vne_ni_pr_i_stupu_k_u_daju_m_za_kladni_ch_registru_.pdf [online]. [cit. 2019-02-08]

7. GDPR VE VEŘEJNÉ SPRÁVĚ II. – praktická část

Praktičtěji zaměřená část hlavního jádra práce se níže věnuje konkrétním oblastem veřejné správy, resp. především územní samosprávy, ve kterých jsou analyzována základní důležitá témata, se kterými se orgány veřejné moci (nejvíce úřady územních samospráv) musely vypořádávat, případně stále vypořádávají.

7.1 GDPR a územní samospráva obecně [93]

V rámci oblasti územní samosprávy byla Ministerstvem vnitra vypracována speciální Metodika pro obce, která poskytuje rychlou kontrolu pro organizační zabezpečení ochrany osobních údajů. Tento metodický dokument je složen ze tří následujících částí: *"Úvod a doporučení", "Obecný seznam" a "Seznam ke zpracování"*. Dokument je zpracován jakožto základní materiál, jež by měl poskytnout základní orientaci odpovědných osob v otázkách technických a organizačních, obce by na něj poté měli navázat svou další samostatnou prací [94].

Obrazový materiál č. 1: GDPR v České republice

Zdroj: https://www.aec.cz/cz/gdp

[93] ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 38

[94] http://www.mvcr.cz/gdpr/clanek/kontrolni-seznamy-checklisty-pro-obce.aspx, © 2010-2015 Správa základních registrů © [online]. [cit. 2019-02-08]

Metodické doporučení k činnosti obcí, vytvořené Ministerstvem vnitra, dává obcím pomocnou ruku v souvislosti s aplikací Nařízení GDPR v praxi. Jednou z materií obsažených v metodikách je úprava tzv. Pověřence pro ochranu osobních údajů. Dnem účinnosti, kdy je již Nařízení aplikovatelné ve všech členských státech Evropské unie, je povinností obcí (a obecně všech, kteří jsou uvedeni v článku 37 Nařízení) povinny zřídit Pověřence pro ochranu osobních údajů (dále jen Pověřenec).

Každá obec je v kontextu článku 37 orgánem veřejné moci, kdy tyto orgány mají povinnost zřizovat institut Pověřence pro ochranu osobních údajů [95]. Pověřence nemusí zajišťovat např. technické správy komunikací, spolky vykonávající běžnou činnost, městské knihovny nebo ty právnické osoby, jejichž hlavní činností není pravidelné a systematické monitorování subjektů údajů ve velkém měřítku, ani rozsáhlé zpracování citlivých údajů

Kdo je konkrétně oním Pověřencem pro ochranu osobních údajů? Mělo by se jednat o vysoce kvalifikovanou, nestrannou a nezávislou osobu, s kvalitní znalostí právních předpisů týkajících se této oblasti. Může se jednat buďto přímo o zaměstnance obce, nebo i externě spolupracující osoby. Dalším faktem je to, že Pověřenec nemusí vykonávat svou činnost jen v jedné instituci (v tomto případě obci), nýbrž i na více místech [96].

Úkoly Pověřence jsou podle Nařízení následující [97]:

„*1. Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly*:

a) poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;

b) monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;

c) poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle článku 35;

d) spolupráce s dozorovým úřadem a

[95]http://www.gdpr-verejna-sprava.cz/wp-content/uploads/2017/08/Metodicke_doporuceni_k_organizacne-technickemu_zabezpeceni_pro_OUU_-_k_19-02-2018.pdf [online]. [cit. 2019-02-08]
[96] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32761 [online]. [cit. 2019-02-08]
[97] Obecné Nařízení GDPR, článek 37-39

e) působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci.

2. Pověřenec pro ochranu osobních údajů bere při plnění svých úkolů patřičný ohled na riziko spojené s operacemi zpracování a současně přihlíží k povaze, rozsahu, kontextu a účelům zpracování.".

Orgánem veřejné moci, či správním orgánem jsou rovněž školy ve formě školské právnické osoby či příspěvkové organizace, jelikož tyto jsou také oprávněny rozhodovat o právech a povinnostech fyzických osob. Povinnost mít zřízený orgán Pověřence se podle Metodiky (výše zmíněné) vztahuje dále i na ty instituce nebo subjekty [98]: *jejichž hlavní činnost (a) vyžaduje pravidelné a systematické monitorování subjektů údajů ve velkém měřítku (např. provozovatelé městské hromadné dopravy, kteří provádí evidenci cestujících) nebo (b) spočívá v rozsáhlém zpracování citlivých údajů (např. nemocnice nebo sociální zařízení). Všechny tyto subjekty tedy budou muset mít s účinností od 25. května 2018 pověřence pro ochranu osobních údajů.*".

Úřad pro ochranu osobních údajů na úrovni obcí vypracoval souhrnný přehled Záznamů o činnostech zpracování ve veřejné správě, celá sekce je tedy zaměřena na vzorové dokumenty podle jednotlivých oblastí. Jedná se o například o kategorie školství, voleb, přestupků, správních řízení, personalistiky, ověřování, matriky, místní poplatky, hospodaření obce, evidence obyvatel, atp. [99]. Vzorové formuláře jsou vloženy v závěrečné části diplomové práce, v kapitole Přílohy – formuláře.

7.1.1 GDPR a územní samospráva – Praha

V případě Hlavního města Prahy byla vydána stručná Metodika [100], která přináší pomoc pracovníkům různých oblastí veřejné správy – v tomto případě územního samosprávného celku a to na úseku samostatné působnosti (sociální služby, školství – zřizovatelem Hlavní město Praha, kulturní činnost, cestovní ruch, atp.) i přenesené působnosti (sociálně-právní ochrana dětí, některá přestupková řízení, státní občanství, matriční záležitosti, nakládání s komunálním odpadem, evidence obyvatel, atp.). S osobními údaji mohou operovat jak zaměstnanci tohoto územně samosprávného celku, tak mimo ně

[98] http://www.gdpr-verejna-sprava.cz/wp-content/uploads/2017/08/Metodicke_doporuceni_k_organizacne-technickemu_zabezpeceni_pro_OUU_-_k_19-02-2018.pdf [online]. [cit. 2019-02-08]
[99] https://www.mvcr.cz/gdpr/clanek/vzorove-dokumenty.aspx [online]. [cit. 2019-02-08]
[100] K metodikám v předchozí podkapitole

příspěvkové organizace, případně i obchodní partneři. Údaje se zpracovávají buďto klasicky v evidencích, případně též automatizovaně, pomocí informačních a komunikačních technologií, využívá se zde i služeb a možností eGovernmentu [101].

Metodika nezapomíná ani na možnost zapojení 3. osob do procesu nakládání s osobními údaji, a v případě takového outsourcingu upravuje povinnosti těchto subjektů jakožto zpracovatelů. Může jít o nejrůznější pomocné činnosti – výzkumy veřejného mínění, či o marketingové a propagační činnosti typu vydávání informačních časopisů městských částí, elektronické newsletterů, atp. Hlavní město mělo také provést zpracování tzv. datové mapy, tedy základní a kompletní audit osobních údajů, aby bylo jasné, do jaké míry se pražské územní samosprávy Nařízení dotkne. V neposlední řadě též musela Praha zajistit důkladné proškolení svých zaměstnanců, což bylo, je a nadále bude zcela automatickým krokem, a to nejen zde, ale i v činnosti dalších (nejen) územních samospráv [102].

V dokumentu, v závěrečné pasáži, je velmi stručně, avšak konstruktivně popsán samotný audit osobních údajů (viz výše), který je složen celkem z 3 jednotlivých fází. První fází se rozumí zanalyzování oblasti osobních údajů u daného orgánu a vytvoření tzv. datové mapy (viz výše), to za provedení posouzení a určení požadavků GDPR a jejich dopadů na dané subjekty a jejich osobní údaje (tzv. GAP analýza). V této fázi se posuzují i možné negativní dopady. Dle slov samotné Metodiky je shrnutí první fáze následné [103]: „*První fáze přináší odpověď na otázky: které oblasti činnosti kontrolovaného subjektu podléhají GDPR, jaké má GDPR relevantní požadavky a jaké bezpečnostní mezery (gaps) je nezbytné odstranit*.“

Druhá, prostřední fáze je zaměřena na efektivní řešení konkrétních situací nakládání s osobními údaji subjektů. Můžou se též navrhovat různé postupy a vylepšení služeb informačních a komunikačních technologií. Poslední fáze je především již kontrolní/revizní. Pozornost se klade na právní předpisy, metodiky, formuláře, kodexy, webové stránky úřadu [104].

[101]https://www.praha1.cz/cps/fotoalbum/Metodika_GDPR_pro_MC_a_PO_hl._m._Prahy.pdf, str. 8 [online]. [cit. 2019-02-28]
[102]https://www.praha1.cz/cps/fotoalbum/Metodika_GDPR_pro_MC_a_PO_hl._m._Prahy.pdf, , str. 8 [online]. [cit. 2019-02-82]
[103] https://www.praha1.cz/cps/fotoalbum/Metodika_GDPR_pro_MC_a_PO_hl._m._Prahy.pdf, str. 8 [online]. [cit. 2019-02-28]
[104] https://www.praha1.cz/cps/fotoalbum/Metodika_GDPR_pro_MC_a_PO_hl._m._Prahy.pdf, str. 8 [online]. [cit. 2019-02-28]

7.1.2 GDPR a územní samospráva – Magistrát města Plzeň

Jak se orgány územní samosprávy v rámci statutárního města Plzně vypořádaly s otázkou přijetí a následné nutnosti aplikace obsahu Nařízení GDPR se autorka pokusí objasnit a přiblížit v této části. Zaměření je zde cíleno na hlavní orgán (úřad) města a to na samotný Magistrát města Plzně.

Magistrát města Plzně připravil pro své zaměstnance [105], kteří při výkonu své činnosti využívají elektronické informační systémy (IS), tzv. *Pravidla pro uživatele IS systémů*. Jedná se ve své podstatě taktéž o jistou metodiku, která pomáhá zaměstnancům tohoto úřadu s výkonem jejich každodenních a rutinních, v určitých případech však i ojedinělých profesních činností.

Tento podpůrný dokument je vypracován zejména na zkvalitnění a zvýšení ochrany a bezpečnosti informací (tedy logicky i osobních údajů), se kterými se pracuje. Obsahuje základní pravidla, zásady, postupy a požadavky na zaměstnance, aby nedocházelo k tzv. Bezpečnostním incidentům (krádeže informací nebo jejich nedovolená modifikace, neoprávněné přístupy, apod.) [106]. Důraz se proto klade především na dostatečně silná přihlašovací jména a hesla k těmto systémům; v některých situacích je dokonce vyžadováno tzv. dvoufázové ověření přihlašování. Při výkonu veškerých úkonů v rámci informačních systémů se dbá na základní zásadu společnou pro všechny orgány veřejné moci a to „co není právním předpisem výslovně dovoleno, to je zakázáno“, tedy na zásadu enumerativnosti veřejnoprávních pretenzí.

Zásadním krokem po přijetí Nařízení GDPR v oblasti zabezpečení osobních údajů je bezpodmínečná nutnost úřadu zřídit dostatečný počet uzamykatelných prostorů k dočasnému, krátkodobému odkládání či přímo trvalejšímu ukládání dokumentů, které obsahují osobní údaje. Ať se jedná o dokumenty, které obsahují osobní údaje v klasické „papírové formě“ či elektronická multimédia – USB flash disky, CD, a další externí úložiště, je bezpodmínečně nutné jejich dostatečné zabezpečení a tím pádem i provedení jednotlivých ustanovení GDPR. V praxi je tato podmínka nazývána jako tzv. „Zásada prázdného stolu“. Nejedná se o kategorickou nutnost mít na pracovišti vždy zabezpečené všechny dokumenty obsahující

[105] Jedná se o zaměstnance tzv. spadající pod zákon č. 312/2002 Sb. - *Zákon o úřednících územních samosprávných celků a o změně některých zákonů.* Nikoli o pracovníky úřadu, s nimiž je uzavřená běžná pracovněprávní smlouva, a tito pod výše uvedený zákon svým profesním postavením nespadají.

[106] Bezpečnostním incidentem se rozumí: *událost v informačním systému, která způsobila narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky*.“. Viz Pravidla pro uživatele IS, Magistrát města Plzně, 2018, str. 2

osobní údaje ve smyslu absolutním – tedy absurdní a leckdy nemožné situace jako např. pracovat samostatně v oddělených a zabezpečených prostorech. V praxi se jedná o případy, kdy by k osobním údajům mohla mít přístup i třetí, nezainteresovaná osoba.

Tato zásada, mimo zakotvení fyzicky uzamykatelných úložišť, v sobě obsahuje [107]:

- využívání síťových tisků pouze s tzv. řízeným přístupem (tiskne se až po autentizaci uživatele na tiskárně)
- odebrání dokumentů z tiskárny ihned po vytištění, zejména pokud jde o tiskárnu umístěnou v prostorách, kde je možný přístup více, než jen zainteresovaných osob
- a jako poslední důležitý bod - nenechávat zdrojové dokumenty mimo tiskáren také v dalších vstupních i výstupních zařízeních (kopírky, skenery, apod.)

Co se předávání informací týče, je přesně vymezen negativní okruh, přes které nosiče informací není možné tyto předávat [108]:

- tzv. Instant Messaging - např. Facebook, Twitter, What's app, ICQ, Miranda, SIM, Yahoo, Jabber, Skype, Viber, FaceTime, Instagram, imessage a další
- veřejná úložiště - např. Uložto.cz
- soukromé e-mailové schránky a freemailové služby - např. seznam, centrum, volny, gmail a podobně
- veřejné webové diskusní skupiny
- není možné odpovídat na nevyžádanou poštu
- veřejné blogy
- sociální sítě obecně - „zeď na Facebooku", Twitter, atp.

Pokud by přece jen k tzv. bezpečnostnímu incidentu došlo, zaměstnanci jsou povinni jej nahlásit (i jen podezření, že k incidentu došlo nebo by mohlo dojít) na určené kontaktní místo, tzv. HelpDesk. Stejně tak musí hlásit i zjištěné programové chyby v informačních systémech [109].

[107] Pravidla pro uživatele IS, Magistrát města Plzně, 2018, str. 5
[108] Pravidla pro uživatele IS, Magistrát města Plzně, 2018, str. 7
[109] Pravidla pro uživatele IS, Magistrát města Plzně, 2018, str. 8

Co se týče jiného fungování Magistrátu města Plzně (konkrétně odboru matrik), nelze v souvislosti s přijetím Nařízení GDPR mluvit o razantních změnách. Úřad splňoval veškeré zákonem a jinými právními předpisy dané podmínky již před účinností tohoto, v souvislosti s jeho přijetím poté docházelo jen k dílčím změnám - viz silnější zabezpečení elektronické komunikace a informačních systémů obecně a nutnost zřízení více fyzicky uzamykatelných úložišť pro dokumenty obsahující osobní údaje.

7.2 GDPR v praxi veřejné správy – shrnutí vybraných otázek

Poslední částí této kapitoly je věnována analýze odpovědí na otázky, které byly položeny již v předchozích, úvodních částech práce. Jedná se o určité shrnutí celého jádra práce a celé myšlenky jejího tématu *GDPR ve veřejné správě*. Otázky byly následující:

1. **Jakým přínosem je Nařízení GDPR pro veřejnou správu v České republice?**
2. **Je (bylo) v České republice možné již od samého počátku účinnosti Nařízení GDPR jeho plné dodržování a aplikování?**
3. **Jsou sankce za porušení Nařízení GDPR přiměřené?**
4. **Jak se od května 2018 vypořádaly samosprávy s účinností Nařízení GDPR a jak funguje Nařízení GDPR po půlročním fungování**?

ad 1) Hlavní přínosy by se daly shrnout jak pro veřejnou, tak i pro soukromou správu společně a to zejména: posílení ochrany osobních údajů jako takové, detailnější právní úprava, zavedení nových kontrolních a výkonných pozic – pokud všechny tyto pozice budou zastoupeny kvalitními odborníky, zvládající jak teorii, tak zejména praxi, bude možné smýšlet v pozitivních souvislostech a o kvalitním fungování ochrany osobních údajů v důsledku přijetí Nařízení GDPR v rámci veřejné správy (i mimo ni).

Další pozitivum autorka práce spatřuje v kompletní, jednotné právní úpravě pro celou Evropskou unii, a možnost se zřetelem k historickým sociálním, kulturním i právním odlišnostem každého členského státu některé instituty upravit a přizpůsobit možnostem jednotlivé země.

Negativními aspekty jsou zejména neinformovanost o dopadu Nařízení GDPR - nejen neinformovanost veřejnosti, ale i institucí samých (státních i samosprávných). Subjekty soukromého i veřejného práva a právních vztahů tento právní předpis pod jeho názvem znají, avšak neumí se v něm konkrétněji a hlouběji orientovat, neumí ho aplikovat v rámci českého právního prostoru. V případě České republiky to je, resp. byla i velmi nízká aktivita, pomalý

a vlažný přístup státních orgánů v případě příprav na přijetí anebo přílišně obecné zpracování Metodik. Vezme-li se v potaz dvouletá legisvakanční lhůta, od května 2016 do května 2018, o Nařízení GDPR se začala odborná i laická veřejnost zajímat téměř až těsně před nabytím účinnosti.

Úřad pro ochranu osobních údajů evidující v České republice stížnosti na činnosti státní správy i samosprávy avizuje jejich nemalé penzum. Pokud by se měly vyčlenit ty nejzásadnější, jde například o *Zveřejňování adresních či jiných identifikačních údajů žadatele ve zveřejněných odpovědích na žádost o informace* (podle zákona č. 106/1999 Sb.). Tyto informace nemají být zveřejňovány v celém svém rozsahu. V důsledku toho se tak jedná o nesprávný proces, kdy se veškeré informace v dokumentu vyvěsí na internetové stránky, případně dojde k jeho oskenování bez toho, aby byly vypuštěny dané údaje [110].

Dalším proviněním ze strany veřejné správy je například *Nedůvodné zpřístupňování v rozhodné době neaktuálních dokumentů*, jež obsahují osobní údaje subjektů. To odporuje jedné ze základních zásad Nařízení GDPR – důvodnosti zpracování, v tomto případě dokonce volného uveřejňování. Neméně závažným problémem je *Neoprávněné nahlížení úředníků do registrů* – typicky registr obyvatel (ROB). V tomto případě jde též o porušení zásady legitimního důvodu pro účel nahlížení do osobních údajů subjektů. Posledním negativním aspektem, který je uveden na webových stránkách Úřadu pro ochranu osobních údajů, je *Nezabezpečení osobních údajů, jejich zpřístupnění nepovolaným osobám* [111]. V tomto případě jde o nutnost zabezpečení pracovního prostředí, zejména elektronického, se kterým operují zaměstnanci veřejné správy – k tomuto tématu více viz předchozí podkapitola věnující se činnostem Magistrátu města Plzně.

ad 2) Pokud jde o přípravu českého státu na přijetí Nařízení GDPR, je nutné konstatovat, že tyto kroky neproběhly ve zrovna ideálním duchu. Podle subjektivního názoru autorky diplomové práce Česká republika (konkrétně její veřejná správa) podcenila zejména prevenci v této přípravě, a přestože bylo Nařízení platné od roku 2016, a v účinnost vešlo v roce 2018, veškeré podpůrné kroky byly učiněny téměř „na poslední chvíli“, právě až od počátku tohoto roku, kdy během cca 4 měsíců logicky nebylo možné uskutečnit veškerá potřebná opatření v plné kvalitě i kvantitě.

[110]https://www.uoou.cz/poznatky-ze-nbsp-stiznostni-agendy-v-nbsp-oblasti-obci-a-nbsp-statni-spravy/d-31687/p1=2619 [online]. [cit. 2019-02-08]
[111]https://www.uoou.cz/poznatky-ze-nbsp-stiznostni-agendy-v-nbsp-oblasti-obci-a-nbsp-statni-spravy/d-31687/p1=2619 [online]. [cit. 2019-02-08]

Tento negativní jev je autorkou spatřován zejména v prakticky téměř absolutní neinformovanosti klientů (zejména občanů) různých oblastí veškeré veřejné správy o faktu, že Nařízení vůbec mělo vejít (a samozřejmě vešlo) v květnu roku 2018 v platnost a jaké důsledky to pro ně znamená [112]. Pokud se pomine mediální komunikace a masmédia obecně (kde docházelo k prvním informacím převážně až na počátku roku 2018), téměř žádná iniciativa v tomto směru od samotné veřejné správy, případně i státu samotného, byť v nejširším možném měřítku − ve všech oblastech, neproběhla.

Negativní pohled plyne i ze slov odbornice v tomto oboru Mgr. Evy Škorníčkové [113], členky Pracovní skupiny Úřadu vlády ČR k legislativě v oblasti ochrany osobních údajů, kdy jejími slovy: „*Zásadní problém vidím v tom a praxe mi to bohužel jenom potvrzuje, že drtivá většina institucí nedodržovala několik let platnou legislativu jak v oblasti ochrany osobních údajů, tak v IT bezpečnosti. Zákon č. 101 máme z roku 2000 a některé společnosti ani neví, že existuje Úřad pro ochranu osobních údajů a některé se teprve teď v souvislosti s přípravami na GDPR seznamují s tím, co je osobní údaj a jaké z nich vlastně zpracovávají. Pro tyto instituce je GDPR jakýmsi tsunami, které na ně navalí takové množství pro ně nových, několik let zanedbávaných povinností… Z mého pohledu naprosto selhala státní správa a její představitelé zodpovědní za tuto agendu. Ani půl roku před účinností nařízení nebyla jednotlivá ministerstva schopna napsat Kodexy, které by jednotlivým institucím daného oboru výrazně pomohly v nastavení pravidel odpovídajícím nařízení*“.

Podle slov odbornice je stav dokonce natolik vážný, že většina institucí nejen že, dá se říci, ignorovala přijetí evropského právního předpisu a důsledky s ním spojené, ale dokonce ani neregistrovala plně dosavadní vnitrostátní právní úpravu. Vinu připisuje ve velkém měřítku státní správě, která nebyla schopna těmto situacím adekvátně čelit.

Toto mohlo být jedněmi z důvodů, které mohly zapříčinit potenciální počáteční chaosy i v dalších otázkách týkajících se zavádění Nařízení do praxe veřejné správy a tím pádem právě do (ne)informovanosti jejích klientů.

ad 3) Otázka ukládaných sankcí byla v procesu před přijetím a účinností, a také těsně po nich velice diskutována, možná až lehce dramatizována. Je sice pravdou, že sankce

[112] Tento názor vychází z vlastního dotazníkového šetření autorky, kdy pomocí internetového portálu pro výzkum veřejného mínění – www.survio.cz proběhlo dotazování stovky respondentů - žen a mužů ve věku cca 20-55 let, středoškolsky až vysokoškolsky vzdělaných, převážně již pracujících v oborech zdravotnictví, územní samosprávy – obecní a krajské úřady, školství, bankovní sektor a finance, Policie ČR.
[113] http://www.efektivnepodnikat.cz/gdpr/lucie-skornickova-v-zavadeni-gdpr-v-cr-selhala-statni-sprava [online]. [cit. 2019-02-08]

ukládané při porušení určité povinnosti se mohou vyšplhat do velmi vysokých částek, ovšem ukládání pokut v nejvyšší možné výši však rozhodně není apriori automatickým postupem při zjištění určitého pochybení.

Sankce by měly být vždy přiměřené, a jak už bylo v práci zmíněno – spíše preventivního charakteru, nikoli tedy přemrštěné až likvidační. Pokuty nemusejí být ukládány okamžitě při zjištění porušení, v tomto primárním kroku může být správce „pouze" upozorněn, že jedná v určitém kontextu protiprávně a jaké hrozí následky, součástí toho je i důsledné poučení o nápravě – tedy uvedení do právně nezávadného stavu [114].

Maximální výše pokuty se může vyšplhat do výše 20 000 000 EUR (nebo až do 4% celkového ročního celosvětového obratu, jde-li o podnik). Pokud by sankční částka dosáhla v kterémkoli státě opravdu takovéto výše, je pravděpodobné, že poté by mohla pro řadu institucí, ať veřejných či soukromých, znamenat sankci opravdu likvidačního charakteru.

Pro instituce veřejnoprávního charakteru – tedy pro orgány veřejné správy však při ukládání sankcí a jejich výše platí v rámci české právní úpravy podle adaptačního zákona mírná odlišnost. Pokud poruší povinnost osoba veřejnoprávního charakteru, například orgán územní samosprávy nebo i státní správy, pokuta může být ve výši s horní hranicí maximálně do 10 00 000 Kč [115]. Pokuty vybírá Úřad pro ochranu osobních údajů.

ad 4) Otázka vypořádání územních samospráv (jak základních územních samosprávných celků – obcí, tak vyšších územních samosprávných celků – krajů) se změnami v důsledku účinnosti Nařízení GDPR byla rozebrána v nejzákladnějších a zároveň nejzásadnějších bodech v předchozí podkapitole. Autorka práce rozebrala situaci jinak v Hlavním městě Praze, které v rámci samosprávy zaujímá i postavení samosprávného kraje a též situaci ve statutárním městě Plzni.

[114] https://www.uoou.cz/11-sankce-pokuty/d-27287 [online]. [cit. 2019-02-28]
[115] Prezentace Mgr. Evy Škorníčkové, dostupné pdf online, http://sokolik-po.cz/data/soubory/GDPR-prezentace.pdf , [online]. [cit. 2019-02-28]

8. Srovnání ochrany osobních údajů ve veřejné správě v ČR a v EU

8.1 EU a veřejná správa obecně

Česká republika se roku 2004 spolu s dalšími devíti státy zařadila mezi členské státy Evropské unie. Stalo se tak na základě celostátního referenda, kdy sami občané rozhodovali o dalším osudu České republiky v rámci Evropské unie. Veřejná správa (a zejména její zaměstnanci) touto skutečností tak získala další rozměr, musela se začít řídit nejen vnitrostátní právní úpravou, ale rovněž tou unijní.

Vývojové tendence veřejné správy jako takové procházely v zemích Evropské unie rozdílně – v každé členské zemi je odlišný politický systém a vedení, každá země má svá specifika. Co je však zemím Unie společné, jsou snahy o zvýšení efektivity, modernizace veřejné správy a jejích orgánů. Základním společným rysem státní správy, jako dílčí části veřejné správy, je existence centrálního vládnoucího orgánu (vlády či obdobné instituce). Od 60. do 80. let minulého století probíhaly v některých, zejména zakládajících, zemích (Velká Británie, země Beneluxu, Irsko, Dánsko, Skandinávie, Francie, Spolková republika Německo) reformní procesy veřejné, resp. státní správy. Uvést lze například [116]:

- decentralizační procesy
- procesy vertikální dekoncentrace
- snahy o zvýšení efektivity státní správy
- zavádění moderních manažerských technik v rámci řízení veřejné správy
- zavedení tzv. principu dobré správy – vstřícnost vůči klientům
- důraz na transparentnost veřejné správy
- postupné zavádění informačních a komunikačních technologií
- postupné sjednocování systémů řízení veřejné správy jednotlivých členských států Evropské unie
- důraz na zvyšování kvalifikace a odborných znalostí zaměstnanců veřejné správy

[116] RÝZNAR, Ladislav a Andrea ŠIMONOVÁ. *Evropská veřejná správa*. 2., dopl. vyd. Kunovice: Evropský polytechnický institut, 2006. ISBN 80-7314-102-7. Str. 12

8.2 Ochrana osobních údajů v EU

Základním právním pramenem pro ochranu osobních údajů v rámci Evropské unie je Listina základních práv EU, která ve svém článku 8, odstavci 1 zakotvuje zásadu, že každý má právo na ochranu osobních údajů, které se ho týkají.

Zásadní změnu zaznamenala oblast ochrany osobních údajů v rámci celé Evropské unie přijetím Nařízení GDPR. Nařízení GDPR je sjednocujícím faktorem celé této oblasti a její problematiky. Jeho přijetím však nezanikly právní úpravy jednotlivých států, naopak – státy musely sladit své právní předpisy, aby nedocházelo ke kolizi vnitrostátní a evropské úpravy. Na stránkách Úřadu pro ochranu osobních údajů je uvedeno v rámci základních informací následující [117]: „*Obecné nařízení výslovně upravuje nezávislost, obecné podmínky pro členy, úkoly a pravomoci dozorových úřadů v členských státech Evropské unie, EHP i Švýcarska a vzájemnou spolupráci těchto dozorových úřadů. Jednotný je také přístup k sankcím*.“. Všechny členské státy by tedy měly dodržovat obecné zásady vyplývající z Nařízení [118].

Půl roku po nabytí účinnosti Nařízení GDPR došlo ve dvou zemích Evropské unie, konkrétně v Portugalsku a ve Francii, k prvotním opatřením a uložením sankcí za porušení povinnosti z tohoto plynoucí. Subjekty, jimiž byly tyto sankce uloženy, jsou jednak poskytovatel zdravotních služeb[119] a jednak také společnost Google LLC. V těchto případech se jednalo o porušení jedněch ze základních zásad zpracování osobních údajů a to - nedostatečná transparentnost a informovanost subjektů osobních údajů. V případě společnost Google LLC se jednalo o nelegitimně získaný souhlas ke zpracování osobních údajů subjektů [120].

Je tedy zřejmé a evidentní, že dodržování ochrany osobních údajů bude při zjištění porušení důrazně kontrolováno a následně napravováno, není tedy jen „šedým univerzálním prostředkem“ teorie, nýbrž i účinným nástrojem pro praktické uplatnění.

---

[117] https://www.uoou.cz/gdpr/ds-3938/p1=3938 [online]. [cit. 2019-02-15]

[118] Maximální výše pokut činí 20 000 000 euro, či 4% z celkového obratu společnosti. Pokuty tedy mohou dosahovat až likvidační úrovně.

[119]„ *Francouzský úřad na ochranu osobních údajů uložil 21. ledna 2019 pokutu ve výši 50 miliónů EUR americkému IT gigantovi Google LLC. Dané řízení bylo zahájeno na základě podnětu sdružení zastupujícího přibližně 10.000 subjektů údajů“* citováno online viz https://www.epravo.cz/top/clanky/prvni-pokuty-za-poruseni-gdpr-jsou-na-svete-108915.html [online]. [cit. 2019-02-10]

[120] „*Souhlas měl být dán neplatně také proto, že byl udělen prostřednictvím dopředu označeného nástroje, a současně proto, že souhlas mohl být dán pouze souhrnně pro všechny v něm uvedené zpracovatelské operace bez možnosti vynětí některých operací. Postup tak nesplňoval požadavek, aby byl souhlas udělený pro každý účel zpracování samostatně*.“ citováno online viz. http://www.epravo.cz/top/clanky/prvni-pokuty-za-poruseni-gdpr-jsou-na-svete-108915.html [online]. [cit. 2019-02-10]

8.3 Srovnání problematiky v ČR a SRN

Veřejná správa ve Spolkové republice Německo byla a neustále je modernizována zejména na těchto pilířích:

- správní politika a strategické plánování
- přeměny úkolů veřejné správy
- změny v organizaci veřejné správy
- optimalizace plánování a procedurálních postupů
- nové formy řízení – management ve veřejné správě
- personální politika
- optimalizace regulací, zejména právních – legislativa
- eGovernment [121]

Jednotlivé koncepce se ve Spolkové republice Německo, stejně tak jako v České republice, vzájemně prolínají a soustavný proces modernizace nestojí na vývoji každého pilíře odděleně, nýbrž na vzájemném prolínání těchto pilířů.

Co se týče problematiky ochrany osobních údajů, zejména ve světle GDPR, zřejmě největším rozdílem je funkce takzvaného Pověřence pro ochranu osobních údajů (DPO – Data Protection Officer – viz článek 37 a následující Nařízení GDPR; dále jen „Pověřenec“). Role Pověřence vychází a je značně inspirována právě německým modelem ochrany osobních údajů, kde tento institut funguje již od roku 1977 [122].

V roce 2017 německý Parlament schválil nový zákon o ochraně osobních údajů, který v souvislosti s přijetím Nařízení GDPR zpřísňuje některá původní ustanovení, či zavádí nová. Přísnější režim se objevil právě u jmenování Pověřence, a dále se v tomto zákoně objevil i zcela nový trestněprávní delikt a to vědomý převod nebo zpřístupnění osobních údajů velkého množství osob. Pachateli, který se dopustí takovéhoto protiprávního jednání, může být udělena sankce trestu odnětí svobody s horní hranicí trestní sazby 3 roky [123].

[121] Německý eGovernment je systematicky rozdělen do 3 dílčích částí a to na část **federální** (komplexní pro všech 16 spolkových zemí), **státní** (každý jednotlivý stát) a **místní** (na úrovni místi správy). Viz ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc. Str. 63

[122] http://www.uni-passau.de/gdpr/ [online]. [cit. 2019-02-10]

[123] http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/[online]. [cit. 2019-02-10]

8.3.1 Konkrétní dílčí rozdíly

Pokud by se měly rámcově srovnat zákony upravující ochranu osobních údajů v České republice (stále ještě zákon č. 101/2000 Sb. – o ochraně osobních údajů, než vejde v účinnost tzv. adaptační zákon) a ve Spolkové republice Německo, lze si již na první pohled všimnout několika rozdílných faktů [124].

Německá úprava je značně rozsáhlejší, než ta česká

- v paragrafovém znění 85:51 (na části však stejné 4:4)

Německá úprava disponuje celkově širší materií jednotlivých institutů. Uvést lze například Kapitolu (= Část) 5. zákona – Zastoupení Evropské rady pro ochranu údajů, její ústřední kontaktní místo a spolupráce se spolkovými úřady, dále dozorčí orgány federace a spolkových zemí v oblasti ochrany osobních údajů, v § 17: Zastoupení v Evropském výboru pro ochranu osobních údajů, § 18: Postup spolupráce mezi orgány dohledu federace a spolkových zemí a další.

- Tento jev je dán mimo jiné velikostí státu a státním uspořádáním. Česká republika je unitárním státem, zatímco Spolková republika Německo je státem uspořádaným na federativní úrovni, kde každá z 16 zemí má vlastní zemské sněmy a zemské vlády. Pro celý stát pak funguje úřad Prezidenta – Bundespräsident, úřad tzv. Bundesrat – tedy spolkové rady a Bundestag – tedy spolkového sněm.

Dalším rozdílem, tentokrát v procesu **harmonizace unijního práva s právem vnitrostátním v oblasti ochrany osobních údajů,** je postoj státu k samotné problematice. Zatímco ve Spolkové republice Německo došlo k přijetí nového zákona v této oblasti již v roce 2017, tedy kalendářní rok po platnosti Nařízení GDPR a v účinnost vešel souběžně s účinností tohoto Nařízení, v České republice byla aktuálně nová právní úprava na úseku ochrany osobních údajů kompletně dořešena a přijata teprve nedávné v době. K 31. 1. 2019 byla právní úprava ve stavu podaného *Usnesení Senátu k návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů*, které přineslo následující kroky [125]:

[124] http://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf [online]. [cit. 2019-02-10]
[125] 86. Usnesení Senátu k návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, senátní tisk 26, 139/14, konané dne 30. 1. 2019

- Senát vrátil návrh zákona Poslanecké sněmovně ve znění přijatých pozměňovacích návrhů a pověřil senátorku Annu Hubáčkovou a senátora Miloše Vystrčila odůvodněním usnesení Senátu na schůzi Poslanecké sněmovny, ta poté zákon hlasováním ve znění pozměňovacích návrhů přijala a ten v brzké době bude vyhlášen, čímž se stane platným a zároveň účinným [126].

Spolková republika Německo navíc ve svém zákoně na ochranu osobních údajů, konkrétně v 5. Kapitole, §64, výslovně zakotvuje bezpečnostní opatření, která mají vést k lepšímu zabezpečení osobních údajů subjektů. Konkrétní opatření mají přihlédnout ke stavu techniky v daném okamžiku, k nákladům na realizaci, rozsah, okolnosti a účel zpracování. Úroveň ochrany má být přiměřená riziku zpracování.

Rok po nabytí účinnosti Nařízení, v roce 2017, bylo Německo jedinou zemí, jež se rozhodla jít směrem většího zpřísnění povinností z Nařízení vyplývajících (na rozdíl například od Slovenské republiky, která novelizaci zákona na ochranu osobních údajů pojala v celkovém souladu a plynulé návaznosti na Nařízení GDPR bez větších odchylek). Takové reakce rozhodně neměly být prvoplánovým záměrem Evropské unie [127]. Primárním úmyslem byla a nadále zůstává jednotnost právní úpravy ochrany osobních údajů v celé Evropské unii a naopak snižování rozdílů mezi jednotlivými státy. Striktnost Spolkové republiky Německo, alespoň z pohledu teorie, nebyla tedy zcela na místě.

Dalším rozdílem v německé materii zákona, a v této části práce posledním, je zavedení nového druhu trestněprávního deliktu. Tímto trestným činem je vědomý převod nebo zpřístupnění osobních údajů velkého množství osob. Aby se o takovýto trestněprávní čin mohlo jednat, musí v kontextu daného případu jít o osobní údaje, které však nejsou veřejně marketingově dostupné. Za tento delikt může být udělen trest odnětí svobody s horní hranicí trestní sazby 3 roky [128].

[126] Zde se projevuje výjimka z klasické 15 denní legisvakanční lhůty, a právní předpis v závěrečných ustanoveních výslovně stanoví dobu platnosti a účinnosti na jeden společný den.
[127] https://www.gdpr.cz/blog/nemecky-parlament-schvalil-novy-zakon-o-ochrane-osobnich-udaju/ [online]. [cit. 2019-02-10]
[128] https://www.gdpr.cz/blog/nemecky-parlament-schvalil-novy-zakon-o-ochrane-osobnich-udaju/ [online]. [cit. 2019-02-10]

9. Závěr

Diplomová práce s tématem *GDPR ve veřejné správě* měla za cíl přinést komplexní, souhrnný a přehledný pohled na problematiku souvislostí s přijetím obecného Nařízení GDPR a v důsledku tohoto přijetí změn nastalých v České republice. Zaměření bylo markantně cíleno na veřejný sektor, konkrétně na veřejnou správu. Co se týče prostředí samotné veřejné správy, bylo analyzováno nejen z pohledu jejích institucí, tedy z formálního hlediska, ale i z pohledu konkrétních činností, které vykonává – tedy z pohledu materiálního.

Z důvodu existence tohoto relativně nového právního i faktického institutu ochrany osobních údajů a zavedení právní úpravy centrálně na evropské úrovni, a to jak v soukromém, tak ve veřejném právu a správě, nebylo vždy jednoduché nalézt kvalitní zdroje poznání a nosiče odborných informací. Stále ještě nelze mluvit o zcela ustálené praxi, co se jednotlivých právních úprav členských států týče. Viz situace právě v České republice, kdy přípravy před přijetím a i po nabytí účinnosti tohoto Nařízení probíhaly poněkud laxním způsobem.

Práce byla koncipována (mimo Úvod, Závěr, Cizojazyčné resumé) na dvě pomyslně větší části a to na část teoretickou (Kapitoly 2-6) a dále na část praktickou (7-8). Teoretická část zaujímá rozsáhlejší prostor obsahu práce z důvodu samotného jádra tématu – Nařízení GDPR v kontextu fungování veřejné správy. Jevilo se tedy vhodným věnovat určitou část obecným tématům, jako je veřejná správa, ochrana osobních údajů obecně, právní pohled na ochranu soukromí a ochranu osobních údajů, dále byl již velký celek věnován samému evropskému právnímu předpisu.

V praktické části, která byla mimo jiné zaměřena převážně na územní samosprávy, byly zodpovězeny odpovědi na následující otázky, které byly vysloveny již v průběhu vypracovávání práce:

1. **Jakým přínosem je Nařízení GDPR pro veřejnou správu v České republice?**
2. **Je (bylo) v České republice možné již od samého počátku účinnosti Nařízení GDPR jeho plné dodržování a aplikování?**
3. **Jsou sankce za porušení Nařízení GDPR přiměřené?**
4. **Jak se od května 2018 vypořádaly samosprávy s účinností Nařízení GDPR a jak funguje Nařízení GDPR po půlročním fungování**?

Dále byla nastíněna situace v Evropské unii a srovnána právní úprava ochrany osobních údajů (v rámci právních předpisů na státní úrovni a po přijetí Nařízení GDPR) v České republice a ve Spolkové republice Německo.

Shrnutí všech těchto otázek souvisejících s praktickou stránkou přijetí Nařízení GDPR a jeho aplikací v české veřejné správě lze stručně popsat na jednu stranu jako velmi progresivní, inovativní a zároveň nutný krok pro posílení ochrany osobních údajů, avšak na druhou stranu prozatím poněkud chaotický, nesystematizovaný a hlavně leckdy i jako desinformační přístup ke změnám, které toto Nařízení přináší. Veřejná správa ani její klienti nebyli na přijetí předem dostatečně připraveni a obě strany jsou stále ve fázi poznávání a učení/vzdělávání. Situace by se mohla (resp. měla) postupem času zlepšovat a to jednak s brzkým nabytím nového tzv. adaptačního zákona a také s postupným vzděláváním jak zaměstnanců veřejné správy, tak klientů (občanů České republiky) obecně.

Cizojazyčné resumé

Diese Diplomarbeit behandelt hauptsächlich das Problem der GDPR-Verordnung in der öffentlichen Verwaltung in der Tschechische Republik. Die öffentliche Verwaltung enthält Kontext der Staatsverwaltung und auch der territorialen Selbstverwaltung. Weil die Problematik der GDPR-Verordnung ganz neu ist, war es sehr schwierig entsprechende Informationsquellen zu finden.

Alle Fakten, die in der Diplomarbeit beschrieben sind, wurden durch das Gesetz de lege lata beschrieben (Hier gibt es fast keine de lege ferenda Regelungen, nur die allgemeine Vision in die Zukunft). In der Diplomarbeit gibt es theoretisches Teilen (Kapitolen 2-6) und praktisches Teilen (Kapitolen 7-8), die sind:

- die öffentliche Verwaltung und das eGovernment
- die Schutz den personenbezogenen Daten
- die Gesetzgebung zum Schutz personenbezogener Daten
- die GDPR-Verordnung Nummer I. – theoretisches Teil
- die GDPR-Verordnung Nummer II. – praktisches Teil
- die Komparation der GDPR-Verordnung in der öffentlichen Verwaltung – Tschechische Republik und die Europäische Union (Bundes Republik Deutschland)

Der Kernarbeit enthaltet die Problematik der GDPR-Verordnung in der öffentlichen Verwaltung (die Theorie und auch die Praxis) und die Komparation der GDPR-Verordnung in der öffentlichen Verwaltung in der Europäischen Union, hauptsächlich die Komparation den Schutz personenbezogener Daten zwischen der Tschechische Republik und der Bundes Republik Deutschland.

Methoden die in der Diplomarbeit benutzen wurden sind:

- Methode der Abstraktion
- Methode der Expertenanalyse
- Methode der Komparation
- Methode der professionellen Forschung – zu vervollständigen

Die Quellen, die in der Diplomarbeit benutzen wurden, sind die folgenden:

- die Fachliteratur – juristische Literatur, öffentlich-rechtliche Literatur,
- die Gesetzgebungen – die Gesetze, Europäischen Recht, die Verordnungen usw.
- die Internetquellen – zum Beispiel: www.uoos.cz, www.gdpr.cz, www.gesetze-im-internet.de, www.zakonyprolidi.cz, www.psp.cz, und so weiter

Die öffentliche Verwaltung orientiert sich auf den modernen Techniken in dieser Zeit. Das ist der Grund, weil die Autorin der Arbeit beschreibt nicht nur die klassische öffentliche Verwaltung, sondern auch den eGovernment und andere elektronische-systemen. In der Arbeit sind folgende Fragen stellen und die Autorin bemühe alle Fragen zu antworten

Die Fragen sind zum Beispiel diese folgenden:

- Welche Positiven und welche Negativen hat die GDPR-Verordnung für die öffentliche Verwaltung?
- Wurde es in der Tschechischen Republik seit Beginn der GDPR-Verordnung möglich alles nachzukommen?
- Sind die Sanktionen der GDPR-Verordnungen angemessen?
- Wie sind die kommunalen und regionalen Gebietskörperschaften seit Mai 2018 mit der Wirksamkeit der GDPR-Verordnung umgegangen und wie funktioniert es nach sechs (und mehr) Monaten des Funktionierens?

Eine Zusammenfassung all dieser Fragen im Zusammenhang mit den praktischen Aspekten der Verabschiedung der GDPR-Verordnung und ihrer Anwendung in der tschechischen öffentlichen Verwaltung kann kurz als sehr guter und innovativer Schritt zur Stärkung des Schutzes personenbezogener Daten bezeichnet werden, andererseits aber als etwas chaotisch, unsystematisch und vor allem manchmal ein Desinformationsansatz für die Änderungen, die diese Verordnung mit sich bringt. Weder die öffentliche Verwaltung noch ihre Kunden waren im Voraus ausreichend auf eine Zulassung vorbereitet, und beide Seiten befinden sich noch im Lern- und Lernprozess. Die Situation könnte sich im Laufe der Zeit verbessern, sowohl durch die frühzeitige Einführung eines neuen so genannten Anpassungsgesetzes als auch durch die schrittweise Schulung sowohl von Mitarbeitern der öffentlichen Verwaltung als auch von tschechischen Bürgern im Allgemeinen.

Seznam použité literatury a odkazů

<u>Knižní publikace, odborné práce</u>:

1) ČECHUROVÁ, Barbora. *ELEKTRONIZACE VEŘEJNÉ SPRÁVY v ČR - eGOVERNMENT*. Plzeň, 2018. Diplomová. Západočeská univerzita v Plzni. Vedoucí práce JUDr. Tomáš Louda, CSc.

2) DONÁT, Josef a Jan TOMÍŠEK. *Právo v síti: průvodce právem na internetu*. V Praze: C. H. Beck, 2016. ISBN 978-807400-610-4.

3) HENDRYCH, Dušan. *Správní právo: obecná část*. 9. vydání. V Praze: C. H. Beck, 2016. Academia iuris (C. H. Beck). ISBN 978-80-7400-624-1.

4) KLÍMA, Karel. *Veřejná správa a lidská práva*. Praha: Metropolitan University Prague Press, 2015. ISBN 978-80-87956-27-4.

5) LOUDA, Tomáš, Jiří GROSPIČ a Lenka VOSTRÁ, ed. *Modernizace veřejné správy v Evropě a České republice: sborník příspěvků z workshopu s mezinárodní účastí: Praha 22. - 23. 11. 2005*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006. ISBN 80-7380-001-2.

6) MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2.

7) NOVOTNÝ, Vladimír. *Elektronizace veřejné správy – Soubor vědeckých statí*. Praha, Metropolitní univerzita Praha, 2011. CD-ROM

8) Pravidla pro uživatele IS, Magistrát města Plzně, 2018

9) RÝZNAR, Ladislav a Andrea ŠIMONOVÁ. *Evropská veřejná správa*. 2., dopl. vyd. Kunovice: Evropský polytechnický institut, 2006. ISBN 80-7314-102-7.

10) ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

11) VANÍČEK, Zdeněk a Stanislav A. MARCHAL. *Právní aspekty eGovernmentu v ČR*. Praha: Linde, 2011. ISBN 978-80-7201-855-0.

12) VAVROCHOVÁ, Simona. *Vzdělávání v eGovernmentu*. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. ISBN 978-80-86847-74-0.

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

Právní předpisy, judikatura:

1) Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

2) Zákon č. 2/1993 Sb., Listina základních práv a svobod

3) Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

4) Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

5) zákon č. 111/2009 Sb., o základních registrech

6) Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

7) zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)

8) zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)

9) zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

10) zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů

11) zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů

12) zákon č. 365/2000 Sb., o informačních systémech veřejné správy

13) Zákon č. 480/2004 Sb., o některých službách informační společnosti

14) zákon č. 89/2012 Sb., občanský zákoník

15) Nález Ústavního soudu České republiky, Pl. ÚS 1/12 ze dne 27. 11. 2012437/2012 Sb. N 195/67 SbNU 333

16) Rozsudek Evropského soudu pro lidská práva – případ Godelli proti Itálii, ze dne 13. 3. 2013

17) Rozsudek Evropského soudu pro lidská práva – případ KH a dalších proti Slovensku, ze dne 6. 11. 2009

18) Rozsudek Evropského soudu pro lidská práva – případ KU proti Finsku, ze dne 2. 3. 2009

19) Rozsudek Evropského soudu pro lidská práva – případ S. a Marper versus Spojené království, ze dne 4. 12. 2008

20) Rozsudek Evropského soudu pro lidská práva – případ Satakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku, ze dne 27. 6. 2017

21) Usnesení Ústavního soudu České republiky III. ÚS 381/01 ze dne 17. 10. 2001

22) Usnesení Ústavního soudu České republiky, I. ÚS 28/02 ze dne 16. 3. 2004

23) Usnesení Ústavního soudu České republiky, IV. ÚS 4041/16 ze dne 12. 1. 2017

Internetové zdroje – odborné webové stránky, pdf dokumenty dostupné online:

1) http://www.efektivnepodnikat.cz/gdpr/lucie-skornickova-v-zavadeni-gdpr-v-cr-selhala-statni-sprava

2) http://www.gdprbezobav.cz/novy-nemecky-zakon-ochrane-osobnich-udaju/

3) http://www.gdpr-verejna-sprava.cz/wp-content/uploads/2017/08/Metodicke_doporuceni_k_organizacne-technickemu_zabezpeceni_pro_OUU_-_k_19-02-2018.pdf

4) http://www.gesetze-im-internet.de/bdsg_2018/BDSG

5) http://www.msmt.cz/file/44569/

6) *http://www.mvcr.cz/clanek/co-je-egovernment.aspx*

7) http://www.mvcr.cz/gdpr/clanek/kontrolni-seznamy-checklisty-pro-obce.aspx

8) http://www.mvcr.cz/soubor/3-zasedani-rvis-zapis-rvis-09-09-2016.aspx

9) http://www.sokolik-po.cz/data/soubory/GDPR

10) Http://www.szrcr.cz/uploads/Vyvojari/Manua_l_pro_kontrolu_nastaveni_opra_vne_ni_pr_i_stupu_k_u_daju_m_za_kladni_ch_registru_.pdf

11) http://www.uni-passau.de/gdpr/

12) https://drive.google.com/file/d/1DSF-HPQyLAPD65Ke5pZ_rpwPpNDEBSmZ/view

13) https://www.czechpoint.cz/public/gdpr/

14) https://www.epravo.cz/top/clanky/prvni-pokuty-za-poruseni-gdpr-jsou-na-svete-108915.html

15) https://www.gdpr.cz/blog/nemecky-parlament-schvalil-novy-zakon-o-ochrane-osobnich-udaju/

16) https://www.gdpr.cz/gdpr/osobni-udaje/

17) https://www.mvcr.cz/gdpr/clanek/vzorove-dokumenty.aspx

18) https://www.praha1.cz/cps/fotoalbum/Metodika_GDPR_pro_MC_a_PO_hl._m._Prahy.pdf

19) https://www.uoou.cz/11-sankce-pokuty/d-27287

20) https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32761

21) https://www.uoou.cz/gdpr/ds-3938/p1=3938

22) https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938,

23) https://www.uoou.cz/kodexy-chovani/d-29493/p1=4753

24) https://www.uoou.cz/oblasti-zpracovani-osobnich-udaju/ds-1267/p1=1267

25) https://www.uoou.cz/poznatky-ze-nbsp-stiznostni-agendy-v-nbsp-oblasti-obci-a-nbsp-statni-spravy/d-31687/p1=2619

26) https://www.uoou.cz/urad/ds-1059/p1=1059

27) https://www.uoou.cz/ustavni-soud/ds-2854/archiv=0

28) https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=28603&n=schvalene- pokyny&p1=4720

29) https://www.uoou.cz/vismo/zobraz_dok.asp?n=evropsky-soud-pro-lidska-prava&archiv=0&id_ktg=2853&tzv=1&pocet=25&stranka=1
https://www.uoou.cz/pravni-predpisy/ds-1257

30) https://www.uoou.cz/zverejnene-metodiky/d-28765/p1=3938

Seznam příloh

Obrazový materiál:

1) GDPR v České republice

Grafy:

1) Pojem eGovernment
2) Co znamená pojem Právo na ochranu osobních údajů
3) Co znamená pojem GDPR
4) Kyberkriminalita 2011-2018

Oficiální formuláře:

1) Zpracování dle GDPR – Czech POINT
2) Působnost pověřence dle GDPR

Přílohy - formuláře

Formulář č. 1: zpracování dle GDPR – Czech POINT

Záznam o činnostech zpracování – Czech POINT
čl. 30 odst. 1 obecného nařízení o ochraně osobních údajů (GDPR)

Správce: *... (název, adresa, datová schránka) ...*
Pověřenec pro ochranu osobních údajů: *... (jméno, příjmení, e-mail) ...*

I. Účely zpracování

ZAJIŠTĚNÍ AGEND KONTAKTNÍHO MÍSTA VEŘEJNÉ SPRÁVY

Čl. 6 odst. 1 písm. c) GDPR - zpracování nezbytné pro plnění právní povinnosti:

zákon č. 365/2000 Sb., o informačních systémech veřejné správy,

zvláštní právní předpisy upravující podání správním orgánům prostřednictvím kontaktních míst veřejné správy, například:

zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon),

zákon č. 269/1994 Sb., o Rejstříku trestů,

zákon č. 111/1999 Sb., o základních registrech,

zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel),

zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu),

zákon č. 500/2004 Sb., správní řád,

zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

(Tento záznam o činnostech upravuje pouze poskytování služby kontaktního místa veřejné správy veřejnosti, nikoli využívání Czech POINT pro vlastní činnost úřadu – takováto zpracování osobních údajů jsou součástí jednotlivých agend, jimž jsou věnovány ostatní záznamy o činnostech.

Na obec se při poskytování služby Czech POINT pohlíží z hlediska GDPR jako na správce osobních údajů – záznam se týká údajů, které obec získává od subjektu údajů pro účely poskytnutí služby CzechPoint, popřípadě je předává subjektu údajů. Záznam se netýká datového obsahu informačního systému Czech POINT, jehož správcem není obec a pro obec nelze dovodit ani roli zpracovatele.)

II. Kategorie subjektů údajů

Fyzická osoba, která činí podání na kontaktním místě veřejné správy.

III. Kategorie osobních údajů

Údaje nezbytné pro účely ověření totožnosti fyzické osoby, která činí podání na kontaktním místě veřejné správy, a k elektronickému zpracování jejího podání, včetně referenčních údajů ze základního registru obyvatel a údaje o rodném příjmení z informačního systému evidence obyvatel. Údaje, které jsou obsahem výpisů, ověřených výstupů z informačních systémů veřejné správy a podobných výstupů pořizovaných prostřednictvím Czech POINT. Údaje nezbytné pro doručování písemností ve formě výstupů autorizované konverze dokumentů podle správního řádu. Údaje nezbytné pro vedení evidence žádostí o výpis z Rejstříku trestů.
IV. Kategorie příjemců
Správce informačního systému kontaktních míst veřejné správy.
V. Plánované lhůty pro výmaz kategorií osobních údajů
Žádost o vydání výpisu z Rejstříku trestů uchovává kontaktní místo veřejné správy po dobu dvou let od jejího podání.
VI. Obecný popis technických a organizačních bezpečnostních opatření
Přístup k informačnímu systému je zabezpečen hesly v souladu s nastavením přístupových práv vnitřními předpisy obce. Fyzické prostředky jsou spravovány v uzamykaných prostorách. Výstupy z informačních systémů veřejné správy se subjektům údajů předávají tak, aby byly odpovídajícím způsobem skryty před třetími osobami. Obec neuchovává kopie podání učiněných prostřednictvím Czech POINT ani výpisů pořízených z informačních systému veřejné správy. *Datové připojení k informačnímu systému kontaktních míst veřejné správy je zajištěno… (doplní obec dle své praxe).*

Zdroj: https://www.mvcr.cz/gdpr/soubor/vzor-czech-point.aspx

Formulář č. 2: Působnost pověřence dle GDPR

Působnost/Pracovní náplň pověřence pro ochranu osobních údajů **Čl. 37 obecného nařízení o ochraně osobních údajů (GDPR)**
I. Organizační zařazení
Pověřenec pro ochranu osobních údajů (dále jen „pověřenec“) je zařazen do …*odboru/oddělení*… Zaměstnanec, který vykonává činnost pověřence, je při výkonu této činnosti podřízen přímo vedoucímu úřadu. Případné úkoly ukládané pověřenci vedoucím úřadu nesmějí být v rozporu s postavením a úkoly pověřence podle GDPR.
II. Úkoly pověřence podle čl. 39 odst. 1 a čl. 38 odst. 4 GDPR
Pověřenec: a) poskytuje zaměstnavateli a ostatním zaměstnancům informace a poradenství o jejich povinnostech podle GDPR a dalších předpisů v oblasti ochrany osobních údajů, b) monitoruje soulad s GDPR, dalšími právními předpisy a vnitřními předpisy a další dokumentací zaměstnavatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců, c) poskytuje poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů a monitorování jeho uplatňování podle čl. 35 GDPR, d) spolupracuje s Úřadem pro ochranu osobních údajů, e) působí jako kontaktní místo pro Úřad pro ochranu osobních údajů v záležitostech týkajících se zpracování, včetně předchozí konzultace podle čl. 36 GDPR, a případně vedení konzultací v jakékoli jiné věci, a f) působí jako kontaktní osoba zaměstnavatele pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR.
III. Další činnosti pověřence při plnění úkolů podle bodu II
Pověřenec dohlíží na soulad činnosti zaměstnavatele s GDPR a dalšími předpisy v oblasti ochrany osobních údajů podle vlastního plánu dohledové činnosti a na základě vyhodnocení podnětů zaměstnavatele, ostatních zaměstnanců, kontrolních orgánů a subjektů údajů. Pověřenec poskytuje zaměstnavateli a ostatním zaměstnancům informace z oboru své působnosti podle aktuálních potřeb, v souladu s vlastním plánem zvyšování povědomí zaměstnanců o ochraně osobních údajů a také formou vyjádření a připomínek ke konkrétním otázkám a dokumentům předloženým mu

zaměstnavatelem.

Pověřenec sleduje vývoj právní úpravy, stanoviska Úřadu pro ochranu osobních údajů a orgánů Evropské unie a rozhodovací činnost soudů v oblasti ochrany osobních údajů a přiměřeným způsobem o těchto skutečnostech informuje zaměstnavatele a ostatní zaměstnance.

Pověřenec sleduje vývoj technologií souvisejících s ochranou osobních údajů a přiměřeným způsobem o něm informuje zaměstnavatele a ostatní zaměstnance.

Pověřenec posuzuje návrhy významných dokumentů zaměstnavatele týkajících se ochrany osobních údajů, zejména politik ochrany osobních údajů, bezpečnostních směrnic a dalších vnitřních předpisů, vzorů souhlasů se zpracováním osobních údajů, návrhů smluv o zpracování osobních údajů, vzorů podání a vyřízení, pokud jde o uplatňování práv subjektů údajů.

Pověřenec posuzuje soulad navrhovaných řešení v oblasti informačních a komunikačních technologií s pravidly ochrany osobních údajů.

Pověřenec přijímá a vyhodnocuje podání subjektů údajů v záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle GDPR. V případě, že nemůže podání vyřídit sám, postupuje je v souladu s vnitřními předpisy zaměstnavatele k vyřízení příslušným útvarům, popřípadě si vyžádá od příslušných útvarů podkladová stanoviska a následně podání vyřizuje.

Pověřenec vede záznamy o činnostech zpracování podle čl. 30 GDPR.

Pověřenec navrhuje zaměstnavateli opatření k dosahování plného souladu s GDPR a dalšími předpisy v oblasti ochrany osobních údajů.

Pověřenec se podílí na plnění povinností zaměstnavatele hlásit porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů (čl. 33 GDPR) a oznamovat porušení zabezpečení osobních údajů subjektům osobních údajů (čl. 34 GDPR).

Zdroj: https://www.mvcr.cz/gdpr/soubor/vzor-priklad-pracovni-naplne-poverence.aspx