ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

General Data Protection Regulation

General Data Protection Regulation

Tadeáš Janda

Plzeň 2018

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta ekonomická
Akademický rok: **2017/2018**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tadeáš JANDA**
Osobní číslo:	**K15B0354P**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Systémy projektového řízení**
Název tématu:	**General Data Protection Regulation**
Zadávající katedra:	**Katedra podnikové ekonomiky a managementu**

Zásady pro vypracování:

1. Představte General Data Protection Regulation.
2. Analyzujte ostatní předpisy týkající se osobních údajů ve vztahu k České republice.
3. Analyzujte připravenost vybrané skupiny na implementaci General Data Protection Regulation.
4. Zhodnoťte výsledky analýz a vliv General Data Protection Regulation na situaci v České republice.

Rozsah grafických prací: **neuveden**

Rozsah kvalifikační práce: **40 - 60 stran**

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

Seznam odborné literatury:

- **EGER, Ludvík a Dana EGEROVÁ.** *Základy metodologie výzkumu: pro studenty ekonomických oborů.* **V Plzni: ZČU, 2014. ISBN 978-80-261-0418-6.**
- **JANEČKOVÁ, Eva a Václav BARTÍK.** *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi).* **Praha: Wolters Kluwer Česká republika, 2016. ISBN 978-80-7552-145-3.**
- **NULÍČEK, Michal.** *GDPR - obecné nařízení o ochraně osobních údajů.* **Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 9788075527653.**
- **ÚŘEDNÍ VĚSTNÍK EVROPSKÉ UNIE.** *Nařízení evropského parlamentu a rady (eu) 2016/679* **[online]. Úřední věstník Evropské unie, 2016 [cit. 2017-09-25]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=EN**

Vedoucí bakalářské práce: **Ing. Martin Januška, Ph.D.**
Katedra podnikové ekonomiky a managementu

Datum zadání bakalářské práce: **23. října 2017**

Termín odevzdání bakalářské práce: **23. dubna 2018**

Doc. Dr. Ing. Miroslav Plevný
děkan

L.S.

Doc. PaedDr. Dana Egerová, Ph.D.
vedoucí katedry

V Plzni dne 23. října 2017

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

General Data Protection Regulation

vypracoval samostatně pod odborným dohledem vedoucího bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni, dne …… ……

podpis autora

Poděkování

Chci poděkovat vedoucímu mé bakalářské práce panu Ing. Martinu Januškovi, Ph.D., za pomoc s výběrem náhradního tématu bakalářské práce. Dále bych chtěl poděkovat všem respondentům, kteří si našli chvíli ze svého času a pomohli mi vyplněním dotazníkového šetření získat podklady pro praktickou část mé bakalářské práce.

Obsah

Úvod

Ochrana osobních údajů je v dnešním světě aktuálním tématem. Lidé o sobě poskytují nezměrné množství informací, kupříkladu na sociálních sítích či při nástupu do zaměstnání. Mnoho lidí si však možná neuvědomuje, co se může stát v případě, kdy dojde k úniku jejich osobních údajů, či dokonce ke krádeži identity. Evropský parlament tedy vytvořil směrnici o ochraně osobních údajů (General Data Protection Regulation), která přijde v platnost 25. května 2018. Směrnice především slouží jako rozšíření práv subjektů údajů, tedy fyzických osob. S většími právy subjektů údajů jdou však ruku v ruce přísnější pravidla pro správce a zpracovatele, tedy ty, kteří jejich osobní údaje zpracovávají a uschovávají.

V první části si představíme a popíšeme General Data Protection Regulation jako takové a zároveň se seznámíme s nejdůležitějšími pojmy, které jsou s touto problematikou spojeny. Rozebereme si také jednotlivé zásady, kterými se budou muset od začátku platnosti směrnice řídit všechny firmy zpracovávající osobní údaje. Prostor věnujeme i jednotlivým právům subjektu údajů, ale i správců a zpracovatelů a také si uvedeme, jaké hrozí následky při porušení povinností směrnice.

A jelikož se ochranou osobních údajů v České republice nezabývá pouze jediný zákon, představíme si jich hned několik, včetně těch nejdůležitějších jako například zákona č. 101/2000 Sb., o ochraně osobních údajů, který bude právě novou směrnicí nahrazen.

Samotným cílem mé práce je analyzování připravenosti firem na implementaci směrnice za využití dotazníkového šetření. Sesbíraná data z tohoto šetření si rozebereme ve třetí části a vzhledem ke značně komplexní problematice směrnice, si uvedeme i nejdůležitější aspekty, které hrají roli právě při procesu přípravy.

V poslední části si zhodnotíme výsledky analýzy. V závislosti na těchto výsledcích budeme schopni případně i zmínit nějaká doporučení do budoucnosti. Nakonec si zhodnotíme, jaký vliv má zavedení General Data Protection Regulation na situaci v České republice.

1 General Data Protection Regulation

1.1 Představení General Data Protection Regulation

General Data Protection Regulation neboli Obecné nařízení o ochraně osobních údajů (dále jen „**Nařízení**“), plným názvem „*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)*“, je nařízení Evropské Unie, které si klade za cíl zvýšení ochrany osobních dat všech občanů. (Evropský parlament a Rada Evropské unie 2016, s. 1)

Jedná se tedy o právní rámec ochrany osobních údajů, chránící práva občanů žijících na území EU proti neoprávněné manipulaci s jejich osobními údaji. Zároveň také Nařízení přebírá zásady zpracování a ochrany dat tak, že jsou data chráněna i za hranicemi EU. Práva lidí dotčených zpracováním osobních údajů jsou za pomocí Nařízení dále posilována a rozvíjena ve smyslu mít informace o tom, jaké údaje jsou zpracovávány a z jakého důvodu, a také ve smyslu domáhání se dodržování daných pravidel či nápravy stavu. V případě zpracování zvláštních kategorií osobních dat obsahuje Nařízení náročnější a více propracovaná pravidla a také si v této věci žádá od zpracovatelů a správců aktivního přistupování, především se pak jedná o nutnost posouzení vlivu jednotlivého zpracování dat na ochranu osobních údajů a následný výběr vhodných opatření nebo nástrojů na ochranu údajů. V určitých případech je nutno vyžádat si konzultaci u samotného dozorového úřadu. Povinnosti pro jednotlivé správce jsou nastavovány za pomocí určení rizikovosti z rozsahu zpracovávání osobních údajů a také k tomu využívaných technologií. (www.uoou.cz 2017a)

V Nařízení se nově setkáváme s povinností nahlásit incidenty, při kterých došlo k porušení osobních údajů. Povinnost ukládá zpracovatelům a správcům údajů nahlásit tento incident do 72 hodin od obeznámení se se vznikem události dozorovému úřadu, ale také všem dotčeným osobám, kterých se toto narušení týká. Za specifických podmínek může pro zpracovatele a správce vzniknout povinnost jmenování pověřence pro ochranu osobních údajů. Povinnosti při zabezpečení zpracování jsou nyní podrobněji stanoveny. (www.uoou.cz 2017a)

„*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.*“ (www.uoou.cz 2017a)

Problematikou Nařízení se zabývají například publikace The EU General Data Protection Regulation (GDPR) od autorů Paul Voigt a Axel von dem Bussche, EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide, Second Edition jejíž autorem je IT Governance Privacy Team nebo také publikace od českého autora Luďka Nezmara s názvem GDPR: Praktický průvodce implementací.

1.2 Definice pojmů spojených s General Data Protection Regulation

V této kapitole si rozebereme jedny z nejdůležitějších pojmů, se kterými se v Nařízení setkáváme, a které jsou také nově Nařízením definovány. Znalost těchto pojmů nám poslouží k lepšímu pochopení textu v následujících kapitolách.

1.2.1 Osobní údaj

Veškeré informace o identifikovatelném či identifikovaném subjektu údajů (fyzická osoba, jíž se osobní údaje týkají) nazýváme osobním údajem. Fyzická osoba se stává identifikovatelnou ve chvíli, kdy je možné ji přímo či nepřímo identifikovat za pomocí tzv. identifikátoru (jméno, příjmení, číslo) nebo za pomocí až několika zvláštních prvků genetické, psychické, fyzické, ekonomické, kulturní, fyziologické nebo společenské identity tohoto subjektu. (www.uoou.cz 2017b)

Pod pojmem osobní údaj se setkáváme i s údajem anonymním, tedy údajem, který nelze vztáhnout k určenému subjektu údajů, a to ani v původním tvaru či po provedení zpracování. (Janečková & Bartík 2016)

1.2.2 Zpracování osobních údajů

„*Zpracováním je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.*“ (www.uoou.cz 2017b)

Ve zkratce se tedy jedná o sofistikovanou a v jistém směru i systematickou činnost prováděnou správcem osobních údajů za určitým účelem. Nelze jej však chápat jako jakékoliv nakládání s osobními údaji. V případě, že se nejedná o zpracování (tedy s osobními údaji je nakládáno jiným, než tímto způsobem), tak ochranu zajišťuje zákon č. 89/2012 Sb., občanský zákoník. (www.uoou.cz 2017b)

1.2.3 Správce

Správce je subjekt (pro který není určující jeho právní norma), který určuje prostředky a účely zpracování osobních údajů a také nese za zpracování odpovědnost. Údaje mohou být zpracovávány pro vlastní účely nebo pro účely vyplývající z jeho činnosti. Správcem může být i fyzická osoba za předpokladu, že způsob, kterým údaje zpracovává se vylučuje s výjimkou osobní či domácí činnosti. (www.uoou.cz 2017b)

Správce nemusí zpracování údajů provádět sám, ale může jím pověřit zpracovatele. To ovšem nemění nic na faktu, že správcem i nadále zůstává, jelikož určil účel a prostředky jeho zpracování. (Nulíček, et al. 2017)

1.2.4 Zpracovatel

Jak již bylo zmíněno v předešlé podkapitole, zpracovatel je subjekt, který si správce najímá za účelem zpracování osobních údajů. Zpracovatel však může s daty provádět pouze takové zpracovatelské operace, kterými byl pověřen nebo vyplývají z činnosti, kterou byl zpracovatel pověřen. Právní forma také není u zpracovatele určující. (www.uoou.cz 2017b)

Zpravidla platí, že zpracovatel musí disponovat vlastní právní identitou tzn. že jde o odlišnou osobu od správce. Příkladem zpracovatele může být firma poskytující cloudová řešení pro práci s osobními údaji či firma poskytující externí archivaci pro datové nosiče. (Nulíček, et al. 2017)

1.2.5 Pověřenec pro ochranu osobních údajů

„*Pověřenec pro ochranu osobních údajů (dále jen „pověřenec“) je specifická osoba, kterou bude muset dle Nařízení jmenovat část správců a zpracovatelů. Pověřenec bude dohlížet na soulad zpracování s Nařízením a radit správci ohledně různých skutečností spojených s ochranou osobních údajů. Pověřenec bude zároveň sloužit jako kontaktní místo pro subjekty údajů a dozorový úřad ohledně záležitostí týkajících se zpracování osobních údajů.*“ (Nulíček, et al., s. 332)

Pověřenec nenese za zpracování osobních údajů zodpovědnost, ta zůstává stále na straně správce a zpracovatele. Dále je nutné si uvědomit, že pověřenec musí zastávat specifické a nezávislé postavení, aby tak nedocházelo ke střetu zájmů. Pokud by pověřenec zjistil, že zpracovatel nebo správce jednají v rozporu s požadavky osobních údajů nebo Nařízení, je povinen se vůči tomuto jednání vymezit. (Nulíček, et al. 2017)

Jmenování pověřence se netýká každého zpracovatele a správce. Jmenování pověřence je povinné při naplnění alespoň jedné z podmínek, které vymezují situace s vyšším rizikem při zpracování osobních údajů. Celé znění podmínek je uvedeno v čl. 37 odst. 1 Nařízení. (Nulíček, et al. 2017)

1.3 Kategorie osobních údajů

Samotné osobní údaje dělíme na několik následujících kategorií. Jelikož jsem se v praktické části dotazovaných ptal, jaké druhy osobních údajů zpracovávají, bude dobré si každý typ údaje popsat.

1.3.1 Adresní a identifikační údaje

Jako prvního zástupce v kategorii máme adresní a identifikační údaje, a to zcela jednoduše proto, že se jedná o nejzpracovávanější typ osobních údajů. Je to vcelku logické, protože mezi tyto údaje se řadí například: jméno, příjmení, adresa trvalého bydliště, rodné číslo, rodinný stav, datum a místo narození, telefonní kontakty či státní příslušnost. (cs.wikipedia.org 2018)

1.3.2 Citlivé údaje

Mezi citlivé údaje řadíme následující údaje: o náboženství a filozofickém přesvědčení, o genetickém údaji, o odsouzení za trestný čin, o politických postojích, o zdravotním stavu nebo biometrickém údaji, o sexuálním životě, o členství v odborových organizacích či údaje vypovídající o národnostním, rasovém nebo etnickém původu. (cs.wikipedia.org 2018)

1.3.3 Popisné údaje

Do kategorie popisných údajů řadíme: mzdu, bankovní spojení, předchozí zaměstnání, bankovní spojení, číslo cestovního dokladu, odborné znalosti a dovednosti, obrazový záznam z kamerového systému, vzdělání, znalost cizích jazyků, počet dětí, vojenskou službu či zdravotní pojišťovnu. (cs.wikipedia.org 2018)

1.3.4 Údaje o jiné osobě

V poslední kategorii osobních údajů se setkáváme s následujícími údaji: o manželovi/manželce, dětech nebo adresních a identifikačních údajích člena rodiny. (cs.wikipedia.org 2018)

1.4 Zásady General Data Protection Regulation

Kapitola 1.4 pojednává o všech zásadách Nařízení. Jednotlivé zásady jsou zde ve shrnutí popsány a vysvětleny.

1.4.1 Zásady zpracování osobních údajů

„*1. Osobní údaje musí být:*

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);

b) shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely („účelové omezení“);

c) přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);

d) přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“); 4.5.2016 L 119/35 Úřední věstník Evropské unie CS (1)Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

e) uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, a to za

předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);

f) zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“);

2. Správce odpovídá za dodržení odstavce 1 a musí být schopen toto dodržení souladu doložit („odpovědnost“).“ (Evropský parlament a Rada Evropské unie 2016, s. 35-36)

1.4.2 Zásada zákonnosti, korektnosti a transparentnosti

Jedním z nejdůležitějších principů ochrany osobních dat je zákonnost, která stanovuje, že zpracování údajů musí vždy probíhat na základě minimálně jedné z podmínek definovaných v čl. 6, odst. 1 Nařízení. Tato zásada také stanovuje, že se zpracování osobních údajů nesmí uskutečňovat za nelegitimními či nelegálními účely. K porušení zásady zákonnosti však může dojít i při rozporu s právním řádem (např. občanský zákoník). (Nulíček, et al. 2017)

Zásada korektnosti a transparentnosti nám uděluje povinnost transparentního a otevřeného přístupu ke způsobu, jakým je s osobními údaji nakládáno, ale také povinnost postupovat férově vůči subjektům údajů, ve smyslu samotného zpracování dat. Nedostatečné či nesprávné splnění informační povinnosti nebo například uvádění subjektu údajů v omyl, by vedlo k porušení této zásady. (Nulíček, et al. 2017)

1.4.3 Zásada účelového omezení

Považuje se za jednu z hlavních zásad zpracování osobních údajů, jelikož určuje, jakým způsobem může správce s osobními údaji nakládat. Správce si vymezením účelu určí, z jakého důvodu osobní údaje zpracovává, a až na výjimky, může osobní údaje zpracovávat pouze za tímto účel. Výjimkou se pak rozumí například případy dalšího zpracování osobních údajů. Samotný účel buď vychází ze zákona nebo musí být definován nejpozději při shromažďování osobních údajů a musí být legitimní, určitý a výslovně podaný. Legitimita nám říká, že účel musí být v souladu nejen se samotným Nařízením, ale i s právními předpisy. Účel by neměl být stanoven příliš „úzce“, jelikož by se tím mohl správce vystavovat riziku rozporu se samotnou zásadou účelového omezení. Musí být stanoven určitě, z čehož bude jasné, k jakému zpracování dat dochází

a k jakému naopak ne. Výslovně podaný účel vyjadřuje povinnost sdělení účelu subjektům údajů a zároveň je důležité, aby jej všechny zúčastněné strany chápaly stejně. (Nulíček, et al. 2017)

1.4.4 Zásada minimalizace údajů

Zásada minimalizace údajů nám ukládá povinnost zpracovávat pouze ty osobní údaje, které jsou relevantní vzhledem k určenému účelu zpracování, a to pouze v rozsahu nezbytném k naplnění tohoto účelu. Tato zásada reflektuje princip záměrné ochrany, kterou si můžeme představit jako zajištění (např. za pomocí SW a HW) sběru pouze nezbytných údajů a likvidaci údajů nepotřebných. Dále se zásada minimalizace odráží i v principu standardní ochrany, tedy že sběr údajů službami a produkty bude probíhat pouze v již zmiňovaném rozsahu. (Nulíček, et al. 2017)

1.4.5 Zásada přesnosti

Dle této zásady musí být zpracované údaje přesné, tedy údaje musí odpovídat skutečnosti. V případě potřeby by pak měli být aktualizovány. Míra požadované přesnosti se odvíjí od vztahu k účelům zpracování osobních údajů. Pokud by například pro účel dostačoval pouze přibližný údaj, nejednalo by se o porušení této zásady. Avšak v případě, že by údaje byly nepřesné, je správce povinen údaje opravit, potažmo vymazat. Za nepřesné údaje lze ku příkladu považovat údaje formálně nesprávné, údaje, jež obsahují výpočetní chyby nebo údaje, které nevypovídají o pravdivém stavu. Zásada přesnosti má vliv také na práva subjektů údajů. Subjekt má právo požádat správce o aktualizaci či opravu jeho osobních údajů a správce je povinen této žádosti vyhovět, údaje ověřit a případně je opravit. (Nulíček, et al. 2017)

1.4.6 Zásada omezení uložení

„*Zásada omezení uložení vyjadřuje povinnost uschovávat osobní údaje pouze po dobu, jež je nezbytná pro účely, pro které jsou zpracovány.*“ (Nulíček, et al. 2017, s. 113)

Pokud se ve zpracování osobních údajů nalezne kategorie, pro kterou již není zpracování nezbytné, musí správce údaje z dané kategorie smazat nebo anonymizovat. Subjekt musí být informován, po jak dlouhou dobu budou jeho údaje zpracovávány, pokud je to nezbytné k zajištění transparentnosti zpracování. Definování doby nesmí být neurčité, což si žádá alespoň relativní stanovení doby zpracování, například ke konkrétní rozhodné události. Určité stanovení doby se vyjadřuje konkrétním datem. (Nulíček, et al. 2017)

V předchozím odstavci byl zmíněný pojem anonymizace. Definice dle Nulíčka a spol. zní následovně: „*Anonymizace je proces, kterým jsou osobní údaje upraveny takovým způsobem, že z nich již nelze identifikovat fyzickou osobu, které se týkají, a to ani sloučením s jinými údaji, ke kterým má správce či kdokoliv další v rámci rozumného předpokladu přístup*.“ (Nulíček, et al. 2017, s. 115)

Anonymizováním osobních údajů je správce schopen dosáhnout obdobného efektu, jako kdyby údaje vymazal. Techniky anonymizace dělíme na techniku randomizace a techniku generalizace. Pod první zmíněnou techniku spadá například permutace, diferenciální utajení a noise addition. Druhá technika zahrnuje L-diverzitu, t-blízkost, agregaci a k-anonymitu. Samotný proces anonymizace je však velmi náročný a v některých případech dokonce nemožný z důvodu komplexnosti datových souborů. Nutno podotknout, že pokud správce odstraní pouze jedinečný identifikátor fyzické osoby (příjmení a jméno), nejedná se o anonymizaci, ale o tzv. pseudonymizaci, která svou funkcí připomíná šifrování. (Nulíček, et al. 2017)

1.4.7 Zásada integrity a důvěrnosti

Zásada stanovuje, že osobní údaje musí být zpracovány stylem, který je schopný zajistit jejich řádné zabezpečení před protiprávním nebo neoprávněným zpracováním, před zničením, poškozením nebo náhodnou ztrátou. (Nulíček, et al. 2017)

1.4.8 Zásada odpovědnosti

Dle této zásady má správce dvě významné povinnosti:

a) správce odpovídá za dodržování všech výše zmíněných zásad, a
b) správce musí být schopen dodržení zásad nově také doložit.

Povinnost doložit dodržení daných zásad pro správce znamená zavedení adekvátních systémů ochrany a vše řádně dokumentovat. Od této změny si legislativa slibuje dodržování všech povinností a také efektivní uplatňování samotného Nařízení v praxi. (Nulíček, et al. 2017)

1.5 Právní ochrana, odpovědnost a sankce

Na následujících několika stránkách najdete shrnutí práv, odpovědnosti a také sankcí.

1.5.1 Právo podat stížnost u dozorového úřadu

Každý subjekt údajů, který má důvodné podezření, že dochází k porušení Nařízení při zpracování jeho osobních údajů, se může obrátit se stížností na dozorový úřad. Dozorové úřady dokáží subjektům podání stížnosti usnadnit, například poskytnutím papírového či elektronického formuláře pro podávání stížností. Jak již bylo zmíněno v předchozích podkapitolách, k porušení Nařízení může dojít několika způsoby, mimo jiné třeba při nesouladu rozsahu zpracování údajů s účelem nebo, když zpracovatel/správce nereaguje na uplatnění práv subjektu údajů. (Nulíček, et al. 2017)

Výběr dozorového úřadu pro podání stížnosti je zcela v kompetencích subjektu údajů, ten však může i samotné podání přenechat na neziskovou organizaci. Subjekt údajů má právo být informován dozorovým úřadem o průběhu a výsledku stížnosti. Vyřízení stížnosti pak vyplývá z pravomocí dozorového úřadu, uvedených v čl. 58 Nařízení. (Nulíček, et al. 2017)

1.5.2 Právo na účinnou soudní ochranu vůči dozorovému úřadu

Toto právo slouží k ochraně před činností dozorového úřadu, a to v souvislosti s vyřizováním stížnosti subjektu údajů nebo vydáváním obligatorních rozhodnutí. (Nulíček, et al. 2017)

Každá fyzická i právnická disponuje právem obrátit se na soudy, pokud nesouhlasí s obligatorním rozhodnutím dozorového úřadu a jsou tímto rozhodnutím dotčeni. Prostřednictvím soudního řádu správního se lze domáhat soudní ochrany proti těmto rozhodnutím. (Nulíček, et al. 2017)

Za předpokladu, že dozorový úřad postupuje nesprávným způsobem (neinformuje subjekt o průběhu řízení stížnosti, stížností se vůbec nezabývá), má subjekt údajů právo na účinnou právní ochranu před tímto dozorovým úřadem. Možnost podat žalobu na správní orgán za nečinnost je rozšíření práv subjektu údajů. (Nulíček, et al. 2017)

1.5.3 Právo na účinnou soudní ochranu vůči správci nebo zpracovateli

Právo na využití prostředků soudní ochrany proti zpracovateli nebo správci má subjekt údajů v případě domněnky o zpracování jeho osobních údajů, které probíhá v rozporu s Nařízením. Ochranou i v tomto případě chápeme podání žaloby, a to buď na náhradu újmy způsobenou zpracováním dat nebo na zdržení se dalšího zpracovávání. Pokud se

subjekt údajů rozhodne využít soudní ochrany, neznamená to, že by byla ostatní práva, jako využití správních či mimosoudních prostředků, vyloučena. (Nulíček, et al. 2017)

Výjimka zde vzniká pro orgány veřejné moci, kde nemá subjekt údajů právo uplatnit nárok u soudu podle svého bydliště. Nárok musí být uplatněn u českých soudů (soudů členského státu), kterým přísluší řešení porušení zpracování osobních údajů, kterých se dopustí správní úřady v rámci výkonu veřejné moci. (Nulíček, et al. 2017)

1.5.4 Zastupování subjektů údajů

Subjekt údajů má právo nechat se zastupovat neziskovým subjektem, což posiluje jeho postavení v rámci ochrany osobních údajů. Neziskovým subjektem nesmí být komerční organizace/sdružení a musí být založen v souladu s právy daného členského státu. Může však působit i ve více státech nebo dokonce v celé EU. (Nulíček, et al. 2017)

Definice zastupování subjektů údajů dle (Evropský parlament a Rada Evropské unie 2016, s. 81) zní následovně:

„*1.Subjekt údajů má právo pověřit neziskový subjekt, organizaci nebo sdružení, jež byly řádně založeny v souladu s právem některého členského státu, jejichž statutární cíle jsou ve veřejném zájmu a jež vyvíjejí činnost v oblasti ochrany práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů, aby jeho jménem podal stížnost, uplatnil práva uvedená v článcích 77, 78 a 79 a, pokud tak stanoví právo členského státu, uplatnil právo na odškodnění podle článku 82.*

2.Členské státy mohou stanovit, že jakýkoliv subjekt, organizace nebo sdružení uvedené v odstavci 1 tohoto článku má bez ohledu na pověření od subjektu údajů právo podat v daném členském státě stížnost u dozorového úřadu příslušného podle článku 77 a vykonávat práva uvedená v článcích 78 a 79, pokud se domnívá, že v důsledku zpracování byla porušena práva subjektu údajů podle tohoto nařízení.“

1.5.5 Přerušení řízení

Jedná se o článek upravující postup v řízení před soudem, který je uplatněn v případě, kdy v jiném členském státu již probíhá řízení týkající se zpracování údajů prováděné stejným zpracovatelem či správcem. (Nulíček, et al. 2017)

V situaci, kdy se soud dozví, že zde již probíhá řízení, má možnost řízení přerušit. O probíhajícím řízení informuje soud z jiného členského státu, kde řízení probíhá. Možnost přerušení se však nevztahuje na soudy, kde bylo řízení zahájeno jako první. Jelikož se

nejedná o povinnost, soud nemusí (při splnění podmínek) řízení vždy přerušovat. (Nulíček, et al. 2017)

Na základě návrhu jednoho z účastníků řízení může soud vyslovit svou nepříslušnost, pokud probíhá související řízení v jiném členském státu. (Nulíček, et al. 2017)

„*Na rozdíl od přerušení řízení je vyslovení nepříslušnosti podmíněno splněním dalších podmínek. Související řízení musí probíhat v jiném členském státu u soudu prvního stupně, tento soud musí být příslušný i pro vedení řízení původně vedeného u soudu v jiném členském státu a spojení těchto řízení musí umožňovat právo členského státu soudu, u kterého bylo řízení zahájeno jako první.*“ (Nulíček, et al. 2017, s. 477)

1.5.6 Právo na náhradu újmy a odpovědnost

Každému, komu je způsobena újma v důsledku porušení Nařízení, vzniká právo na náhradu této újmy. Právo je přiznáno i v případě porušení právního předpisu vydaného v přenesené pravomoci, také při porušení předpisu členského státu, upřesňujícího pravidla Nařízení nebo při porušení prováděcího předpisu, který je též v souladu s Nařízením. (Nulíček, et al. 2017)

Odpovědnost správce a zpracovatele za způsobenou újmu se liší. Správce je totiž odpovědný za jakékoliv porušení Nařízení, a to i v případě, pokud dojde k porušení bez jeho zavinění. Odpovědnost zpracovatele za újmu vzniká pouze při porušení povinnosti, která je mu Nařízením přímo uložena nebo pokud jedná v rozporu (nebo nad rámec) se zákonnými pokyny správce. (Nulíček, et al. 2017)

Ke zproštění odpovědnosti zpracovatele či správce může dojít za předpokladu, kdy je schopen prokázat, že nenese za událost, která vedla ke vzniku újmy, žádnou odpovědnost. Samotnou žalobu pak projedná kompetentní soud členského státu, kde zpracovatel či správce provozuje svůj podnik. (Nulíček, et al. 2017)

1.5.7 Obecné podmínky pro ukládání správních pokut

Při ukládání správních pokut jsou zohledněny především tři vlastnosti, které si níže uvedeme.

a) **Účinnost** – správní pokuty by měly být dostatečně účinné, což povede ke druhé vlastnosti a to sice;
b) **Schopnost odradit** – jde o snahu „odradit“ (za pomocí sankcí) od dalšího případného porušovaní (i ostatní zpracovatele a správce) což logicky vyústí

v efektivnější ochranu osobních údajů. Výše sankcí dosahuje až 20 000 000 EUR nebo 4 % celosvětového ročního obratu (bere se vyšší z těchto dvou částek).

c) **Přiměřenost –** tedy přihlížení k faktu, zda k porušení Nařízení došlo od právnické či fyzické osoby, ekonomické situaci dané osoby a také úrovni příjmů v daném státě. Nutno podotknout, že výše pokuty by neměla být likvidační, ale musí disponovat již zmíněnou „schopností odradit". (Nulíček, et al. 2017)

Pokutu ukládá dozorový úřad. Ten může ale využít i jiných prostředků, jako například omezení zpracování (částečné či trvalé) nebo napomenutí správce/zpracovatele. Při ukládání správní pokuty je úřad povinen zohlednit následující okolnosti:

a) **povaha, závažnost a délka porušení;**
b) **rozsah a účel zpracování;**
c) **počet poškozených a míra způsobené škody;**
d) **zavinění;**
e) **zmírňování škod;**
f) **odpovědnost;**
g) **předchozí porušení;**
h) **spolupráce s dozorovým úřadem;**
i) **kategorie osobních údajů;**
j) **hlášení incidentů;**
k) **splnění nařízených opatření;**
l) **dodržování schváleného kodexu chování nebo mechanismu pro vydávání osvědčení;**
m) **jakékoliv jiné přitěžující nebo polehčující okolnosti.** (Nulíček, et al. 2017)

Článek dále pojednává také o maximální výši správních pokut, a to následovně:

„*4. Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:*

a) povinnosti správce a zpracovatele podle článků 8, 11, 25 až 39, 42 a 43;

b) povinnosti subjektu pro vydávání osvědčení podle článků 42 a 43;

c) povinnosti subjektu pro vydávání osvědčení podle čl. 41 odst. 4.

5. Za porušení následujících ustanovení lze v souladu s odstavcem 2 uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší:

a) základní zásady pro zpracování, včetně podmínek týkajících se souhlasu podle článků 5, 6, 7 a 9;

b) práva subjektů údajů podle článků 12 až 22;

c) předání osobních údajů příjemci ve třetí zemi nebo mezinárodní organizaci podle článků 44 až 49;

d) jakékoli povinnosti vyplývající z právních předpisů členského státu přijatých na základě kapitoly IX;

e) nesplnění příkazu nebo dočasné či trvalé omezení zpracování nebo přerušení toků údajů dozorovým úřadem podle čl. 58 odst. 2 nebo neposkytnutí přístupu v rozporu s čl. 58 odst. 1.

6. Za nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 lze v souladu s odstavcem 2 tohoto článku uložit správní pokuty až do výše 20 000 000 EUR, nebo jedná-li se o podnik, až do výše 4 % celkového ročního obratu celosvětově za předchozí rozpočtový rok, podle toho, co je vyšší." (Evropský parlament a Rada Evropské unie 2016, s. 82-83)

1.5.8 Sankce

Článek Sankce, se zaměřuje na jiné sankce, které se ukládají, pokud nelze udělit správní pokutu. Uložení správní pokuty veřejným subjektům nebo orgánům veřejné moci může být příkladem, kdy nelze správní pokutu udělit. Dle čl. 87 odst. 7 si může každý členský stát stanovit, zdali může být pokuta veřejnému subjektu udělena či nikoliv. Pokud ano, využije se zmíněných jiných sankcí z tohoto článku. (Nulíček, et al. 2017)

Udělení jiných sankcí je také možné osobám, na které se Nařízení nevztahuje, ale jejichž jednání vedlo k přímému porušení Nařízení. Takovou osobou může být zaměstnanec zpracovatele nebo správce. Udělení jiných sankcí je v tomto případě zakotveno v § 44 odst. 1 zák. o ochraně osobních údajů. (Nulíček, et al. 2017)

V úvahu zde přichází i uplatnění trestní odpovědnosti právnických osob, (dle zákona o trestní odpovědnosti právnických osob) v souvislosti se zpracováním osobních údajů. Trestní odpovědnost právnických osob se uplatňuje na principu přičitatelnosti, což

v překladu znamená, že pokud její zaměstnanec spáchá trestný čin, lze jej přičítat právě právnické osobě, a to v případě, došlo-li ke spáchání trestného činu na pokyn orgánu právnické osoby anebo neprovedla-li právnická osoba patřičná opatření dle právního předpisu. (Nulíček, et al. 2017)

„*Za účelem provedení takových opatření, která lze po právnické osobě spravedlivě požadovat, se vypracovávají programy slučitelnosti, tzv. compliance programy, které zahrnují analýzu a úpravu vnitřních procesů, vzdělávání a školení zaměstnanců a pracovníků. Cílem compliance programů je ochrana před situacemi, kdy bude v důsledku jednání jednotlivce nést nepříznivé následky právnická osoba.*“ (Nulíček, et al. 2017, s. 492)

2 Ostatní předpisy týkající se ochrany osobních údajů v České republice

2.1 Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Zákon o ochraně osobních údajů rozlišuje, taktéž jako Nařízení, osoby správce a zpracovatele osobních údajů, kterým ukládá určité povinnosti. Dále rozlišuje osoby subjektu údajů, kterým dává patřičná práva. Pro kontrolu plnění povinností správce a zpracovatele a na ochranu práv subjektu údajů vznikl Úřad pro ochranu osobních údajů. (www.oou.cz 2014)

„Čl. 10

§ 1

Předmět úpravy

Tento zákon v souladu s právem Evropské unie, 1) mezinárodními smlouvami, kterými je Česká republika vázána, 1a) a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

§ 2

(1) Zřizuje se Úřad pro ochranu osobních údajů se sídlem v Praze (dále jen „Úřad“).

(2) Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem1), mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropských společenství.

(3) Úřad vykonává působnost dozorového úřadu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu.

§ 51

Tento zákon nabývá účinnosti dnem 1. června 2000, s výjimkou ustanovení § 16, 17 a 35, která nabývají účinnosti dnem 1. prosince 2000.“ (www.zakonyprolidi.cz 2017)

Citát výše vyjadřuje v § 1význam zákona a § 2 pojednává o zřízení a účelu Úřadu pro ochranu osobních údajů. Zákon se dělí na čtyři části. První část obsahuje hlavy I až VII

(obsahuje např. úvodní ustanovení, práva a povinnosti při zpracování osobních údajů, postavení a působnost úřadu atd.), část druhá byla zrušena, třetí část obsahuje změnu o novele zákona o svobodném přístupu k informacím a část čtvrtá vyjadřuje účinnost zákona a přechodná ustanovení. (www.zakonyprolidi.cz 2017)

2.2 Listina základních práv a svobod

„*VYBRANÁ USTANOVENÍ USNESENÍ předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky*

Čl. 7

(1) Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.

Čl. 10

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“ (Redakce Sagit 2017, s. 3)

2.3 Zákon č. 40/2009 Sb., trestní zákoník

„*§180*

Neoprávněné nakládání s osobními údaji

(1) Kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají.

(3) Odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) spáchá-li takový čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem,

c) způsobí-li takovým činem značnou škodu, nebo

d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.

(4) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.“ (Parlament České republiky 2009, s. 393-394)

„*§ 421*

Účinnost

Tento zákon nabývá účinnosti dnem 1. ledna 2010.“ (Parlament České republiky 2009, s. 451)

2.4 Zákon č. 329/1999 Sb.

„*ÚPLNÉ ZNĚNÍ VYBRANÝCH USTANOVENÍ ZÁKONA č. 329/1999 Sb., o cestovních dokladech, ve znění pozdějších předpisů a zákona č. 183/2017 Sb.*

§ 34a

Přestupky na úseku cestovních dokladů

(1) Fyzická osoba se dopustí přestupku tím, že

j) neoprávněně zpracovává údaje zpracované v nosiči dat s biometrickými údaji.

(4) Správním orgánem příslušným k řízení o přestupcích podle odstavce 1 písm. j) je Úřad pro ochranu osobních údajů.

§ 34b

(1) Právnická nebo podnikající fyzická osoba se dopustí přestupku tím, že neoprávněně zpracovává údaje zpracované v nosiči dat s biometrickými údaji

§ 34c

(1) Přestupky podle § 34b odst. 1 projednává Úřad pro ochranu osobních údajů.

§ 45

Účinnost

Tento zákon nabývá účinnosti dnem, kdy nabude účinnosti zákon, kterým se zavede informační systém evidence obyvatel, nejpozději však dnem 1. července 2000.“ (Redakce Sagit 2017, s. 103)

2.5 Zákon č. 133/2000 Sb.

„ÚPLNÉ ZNĚNÍ VYBRANÝCH USTANOVENÍ ZÁKONA č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů a zákona č. 183/2017 Sb.

§ 17e

(1) Přestupku se dopustí právnická osoba, která

a) neoprávněně nakládá s rodným číslem (§ 13 odst. 9), nebo

b) neoprávněně využívá rodná čísla (§ 13c odst. 1).

(2) Za přestupek podle odstavce 1 písm. a) lze uložit pokutu do 1 000 000 Kč a za přestupek podle odstavce 1 písm. b) pokuta do 10 000 000 Kč.

(3) Přestupky podle tohoto zákona projednává Úřad pro ochranu osobních údajů 14h*) (dále jen "Úřad").*

§ 29

Tento zákon nabývá účinnosti dnem 1. července 2000. Ustanovení § 1 písm. b) a c), § 3 odst. 3, § 6 písm. c), § 13 až 17, § 25 písm. b), § 26 a § 28 body 2 a 3 nabývají účinnosti dnem 1. ledna 2003.“ (Redakce Sagit 2017, s. 104)

2.6 Zákon č. 159/2006 Sb.

„*ÚPLNÉ ZNĚNÍ VYBRANÝCH USTANOVENÍ ZÁKONA č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů a zákonů č. 14/2017 Sb. a č. 183/2017.*

§ 23

Přestupky fyzických osob

(2) Fyzická osoba se dopustí přestupku tím, že

c) v rozporu s § 13 odst. 5 sdělí třetí osobě uživatelské jméno a přístupové heslo k nahlížení do registru oznámení, nebo

d) v rozporu s § 13 odst. 8 používá nebo dále zpracovává údaje vedené v registru oznámení k jinému účelu než ke zjištění případného porušení povinností při výkonu funkce veřejného funkcionáře stanovených tímto zákonem.

§ 24

Přestupky právnických a podnikajících fyzických osob

(1) Právnická nebo podnikající fyzická osoba se dopustí přestupku tím, že

a) v rozporu s § 13 odst. 5 sdělí třetí osobě uživatelské jméno a přístupové heslo k nahlížení do registru oznámení, nebo

b) v rozporu s § 13 odst. 8 používá nebo dále zpracovává údaje vedené v registru oznámení k jinému účelu než ke zjištění případného porušení povinností při výkonu funkce veřejného funkcionáře stanovených tímto zákonem.

§ 25

Společná ustanovení k přestupkům

(1) Přestupky podle § 23 odst. 1 projednává obecní úřad obce s rozšířenou působností, v jejímž územním obvodu má veřejný funkcionář pobyt. Přestupky podle § 23 odst. 2 písm. a) a b) projednává obecní úřad obce s rozšířenou působností, v jejímž územním obvodu má fyzická osoba, která byla veřejným funkcionářem, trvalý pobyt. Přestupky podle § 23 odst. 2 písm. c) a d) a podle § 24 odst. 1 projednává Úřad pro ochranu osobních údajů.“ (Redakce Sagit 2017, s. 105)

2.7 Zákon č. 40/1995 Sb. a doplnění zákona č. 468/1991 Sb.

„*ÚPLNÉ ZNĚNÍ VYBRANÝCH USTANOVENÍ ZÁKONA č. 40/1995 Sb., o regulaci reklamy a o změně o doplnění zákona č. 468/1991 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů a zákonů č. 180/2016 Sb.*

§ 7

Dozor nad dodržováním zákona

Orgány příslušnými k výkonu dozoru nad dodržováním tohoto zákona (dále jen "orgán dozoru") jsou

f) Úřad pro ochranu osobních údajů pro nevyžádanou reklamu šířenou elektronickými prostředky[10a]) podle zvláštního právního předpisu 32), je-li způsob šíření této reklamy nekalou obchodní praktikou,

Čl. III

Tento zákon nabývá účinnosti dnem 1. dubna 1995.“ (Redakce Sagit 2017, s. 106)

2.8 Zákon č. 480/2004 Sb.

„VYBRANÁ USTANOVENÍ ZÁKONA č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

§ 10

(1) Orgánem příslušným k výkonu dozoru nad dodržováním tohoto zákona (dále jen "orgán dozoru") je

a) pro šíření obchodních sdělení podle § 7 Úřad pro ochranu osobních údajů.

§ 18

Tento zákon nabývá účinnosti dnem jeho vyhlášení.“ (Redakce Sagit 2017, s. 107)

2.9 Zákon č. 127/2005 Sb.

„*Ochrana údajů, služeb a sítí elektronických komunikací*

Díl 1

Ochrana osobních, provozních a lokalizačních údajů a důvěrnost komunikací

§ 87

((1) Práva a povinnosti související s ochranou osobních údajů neupravené v tomto dílu se řídí zvláštním právním předpisem34).

(2) Souhlasem podle zvláštního právního předpisu35) se pro účely tohoto dílu rozumí rovněž souhlas učiněný pomocí elektronických prostředků, zejména vyplněním formuláře v obsahu stránky poskytované na síti internet.

(3) Dozor nad dodržováním povinností při zpracování osobních údajů podle tohoto zákona vykonává Úřad pro ochranu osobních údajů podle zvláštního právního předpisu34).“ (Parlament České republiky 2010, s. 3728)

„*§ 179*

Tento zákon nabývá účinnosti prvním dnem druhého kalendářního měsíce následujícího po dni jeho vyhlášení (1. května 2005).“ (Parlament České republiky 2010, s. 3756)

2.10 Směrnice Evropského parlamentu a Rady 95/46/ES

Z této směrnice vychází zákon č. 101/2001 Sb., o ochraně osobních údajů. Uvedu zde pouze pár výňatků z celé směrnice, které mi přijdou důležité.

„*ze dne 24. října 1995*

o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů“ (Evropský parlament a Rada Evropské unie 1995, s. 355)

„*Článek 1*

Předmět směrnice

1. Členské státy zajišťují v souladu s touto směrnicí ochranu základních práv a svobod fyzických osob, zejména jejich soukromí, v souvislosti se zpracováním osobních údajů.

2. Členské státy nemohou omezit ani zakázat volný pohyb osobních údajů mezi členskými státy z důvodů ochrany zajištěné podle odstavce 1.

Článek 2

Definice

Pro účely této směrnice se rozumí:

a) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity;

b) „zpracováním osobních údajů“ („zpracování“) jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace;

c) „rejstříkem osobních údajů“ („rejstřík“) jakýkoli uspořádaný soubor osobních údajů přístupných podle určených kritérií, ať již je tento soubor centralizován, decentralizován nebo rozdělen podle funkčního či zeměpisného hlediska;

d) „správcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů; jsou-li účel a prostředky zpracování určeny právními a správními předpisy na úrovni jednotlivých států či Společenství, je možné určit správce nebo zvláštní kritéria pro jeho určení právem jednotlivých států nebo Společenství;

e) „zpracovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce;

f) „třetí osobou“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt jiný než subjekt údajů než správce, než zpracovatel a než osoby přímo podléhající správci nebo zpracovateli, které jsou oprávněny ke zpracování údajů;

g) „příjemcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, kterým jsou údaje sdělovány, ať se jedná či nikoli o třetí osobu; orgány, které mohou získávat údaje v rámci zvláštního šetření, však nejsou považovány za příjemce;

h) „souhlasem subjektu údajů“ jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování.

Článek 3

Oblast působnosti

1. Tato směrnice se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů, jakož i na neautomatizované zpracování osobních údajů, které jsou obsaženy v rejstříku nebo do něj mají být zařazeny.

2. Tato směrnice se nevztahuje na zpracování osobních údajů:

— prováděné pro výkon činností, které nespadají do oblasti působnosti práva Společenství a jsou uvedeny v hlavě V a VI Smlouvy o Evropské unii, a v každém případě na zpracování, které se týká veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské stability státu, pokud jsou tato zpracování spojená s otázkami bezpečnosti státu) a činnosti státu v oblasti trestního práva,

— prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností.

Článek 4

Použitelné vnitrostátní právo

1. Každý členský stát použije na zpracování osobních údajů vnitrostátní ustanovení, která řijme na základě této směrnice, pokud:

a) zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je stejný správce usazen na území několika členských států, musí přijmout opatření nezbytná pro dodržování povinností stanovených použitelným vnitrostátním právem každou ze svých provozoven;

b) správce není usazen na území členského státu, ale v místě, kde se vnitrostátní právní předpisy daného členského státu platňují na základě mezinárodního práva veřejného;

c) správce není usazen na území Společenství a používá za účelem zpracování osobních údajů prostředků, automatizovaných či nikoli, umístěných na území zmíněného členského státu, ledaže jsou tyto prostředky použity pouze pro účely tranzitu přes území Společenství.

2. V případě uvedeném v odst. 1 písm. c) správce musí určit zástupce usazeného na území zmíněného členského státu, aniž je tím dotčena možnost podniknout právní kroky proti správci samotnému.“ (Evropský parlament a Rada Evropské unie 1995, s. 362-363)

2.11 Směrnice Evropského parlamentu a Rady 2002/58/ES

„*ze dne 12. července 2002*

o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)“ (Evropský parlament a Rada Evropské unie 2002, s. 514)

„*Článek 1*

Oblast působnosti a cíl

1. Touto směrnicí se harmonizují předpisy členských států, požadované pro zajištění rovnocenné úrovně ochrany základních práv a svobod, zejména práva na soukromí, se zřetelem na zpracování osobních údajů v odvětví elektronických komunikací, a pro zajištění volného pohybu těchto údajů a elektronických komunikačních zařízení a služeb ve Společenství.

2. Ustanovení této směrnice upřesňují a doplňují směrnici 95/46/ES pro účely uvedené v odstavci 1. Navíc poskytují ochranu oprávněných zájmů účastníků, kteří jsou právnickými osobami.

3. Tato směrnice se nevztahuje na činnosti, které nespadají do oblasti působnosti Smlouvy o založení Evropského společenství, jako činnosti uvedené v hlavě V a VI Smlouvy o založení Evropské unie, a v žádném případě na činnosti týkající se veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a na činnosti státu v oblasti trestního práva.

Článek 3

Dotčené služby

1. Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství.

2. Články 8, 10 a 11 se vztahují na účastnické linky připojené k digitálním ústřednám a v případě, že je to technicky možné a nevyžaduje to neúměrné ekonomické zatížení, se vztahují na účastnické linky připojené k analogovým ústřednám.

3. Členské státy uvědomí Komisi o případech, ve kterých by splnění požadavků podle článků 8, 10 a 11 bylo technicky nemožné nebo by vyžadovalo neúměrné ekonomické zatížení.“ (Evropský parlament a Rada Evropské unie 2002, s. 519-520)

3 Analýza připravenosti vybrané skupiny na implementaci General Data Protection Regulation

3.1 General Data Protection Regulation Compliance Checklist

Vzhledem k tématu mého výzkumu, by bylo dobré si vysvětlit, jaké kroky musí organizace v České republice a zbytku celé Evropské unie při implementaci Nařízení podniknout. Následující odstavce tedy představují jakýsi seznam rad, které by měly organizacím pomoci při implementaci Nařízení. Je důležité zmínit, že nároky nařízení na každou organizaci se liší, a neexistuje tedy jeden vhodný návod pro všechny.

3.1.1 Správa dat

Jedním ze základních principů Nařízení je zajistit to, že organizace staví správu dat na první místo. Nařízení zavádí řadu požadavků k zajištění dodržování předpisů, a chce, aby toto dodržování braly všechny společnosti vážně. V rámci organizace je důležité zvýšit povědomí o problémech s ochranou soukromí především u zaměstnanců, například formou školení. Také je důležité mít jasně stanovené role a zodpovědnost při spravování dat, či může být vhodné přezkoumat pojistné krytí (pokud jej firma využívá) a případně jej upravit s přihlédnutím k výši sankcí a pokut. (Latham & Watkins 2017)

3.1.2 Odpovědnost

Od organizací je požadováno disponovat dokumentací prokazující, že firma splňuje podmínky Nařízení. Ve společnosti bude vhodné globálně zastřešit ochranu údajů, která sdruží všechny příslušné zásady, včetně procesu ochrany soukromí, vytvoření a vedení záznamů o zpracovatelských činnostech. Ochrana dodržování soukromí by měla být začleněna v rámci auditu, k zajištění fungování zásad a procesů. (Latham & Watkins 2017)

3.1.3 Spravedlivé zpracování a souhlas

Nařízení ukládá nové požadavky na získání platného souhlasu. Souhlas může být kdykoliv zrušen a firemní systém musí být schopen tyto žádosti o zrušení zvládnout. Je třeba zkontrolovat existující důvody firmy pro zákonné zpracování a pak i potvrdit, že tyto údaje jsou pro v souladu s Nařízením. Firma by měla též zvážit (pokud se jí to týká), zda jsou splněny zvláštní požadavky týkající se souhlasu od dětí. Dále je dobré zhodnotit, jestli firma zpracovává i citlivé údaje a následně v tomto ohledu podniknout patřičné kroky. (Latham & Watkins 2017)

3.1.4 Oznámení a prověření – HR

Důraz je kladen na transparentnost GDPR. Oznámení musí být jasná, stručná a informativní. Zaměstnanci musí být odpovídajícím způsobem informováni o všech činnostech zpracování údajů a přenosu údajů a musí jim být poskytnuty informace uvedené v článcích 13 až 14. Záznamy o trestních činech nelze dále zpracovávat, pokud to nepovoluje zákon členského státu. (Latham & Watkins 2017)

3.1.5 Oznámení – zákazníci

Oznámení musí být opět jasná, stručná a informativní. Zákazníci musí být dostatečně informováni o všech činnostech zpracování údajů a přenosu údajů a musí jim být poskytnuty informace uvedené v článcích 13 až 14. Oznámení musí být rovněž v souladu s novými požadavky na souhlas, pokud využívají souhlas jako zákonný důvod zpracování. (Latham & Watkins 2017)

3.1.6 Děti

Nařízení vyžaduje rodičovský souhlas se zpracováním údajů týkajících se služeb informační společnosti nabízených "dítěti" (v rozmezí od 13 do 16 let v závislosti na členském státě). Jak by s dětmi mělo být zacházeno podle tohoto ustanovení však Nařízení ponechává z velké části na uvážení členských států. Zvážit lze i alternativní ochranu pomocí výpočetních systémů na ověření věku. (Latham & Watkins 2017)

3.1.7 Práva a postupy subjektu údajů

Subjektům údajů jsou v rámci Nařízení poskytována rozsáhlejší práva. Současná práva požadovat přístup k údajům, opravu anebo odstranění údajů doznala značného rozšíření, především pak v právu požadovat smazání ("právo být zapomenut") nebo právu na přístup a poskytnutí vašich údajů ve strojově čitelném formátu ("přenositelnost dat"). Právo vznést námitky proti jakémukoli zpracování provedenému na základě oprávněných zájmů nebo pro přímý marketing a právo nepodléhat rozhodnutí založenému na automatizovaném zpracování jsou rovněž zahrnuty a výslovně odkazují na právo vznášet námitky proti profilování. Tyto informace musí být firmou jasně sděleny v oznámeních poskytnutých subjektům údajů, např. v zásadách ochrany osobních údajů. (Latham & Watkins 2017)

3.1.8 Záznam o zpracování

Nařízení vyžaduje, aby organizace udržovaly podrobný záznam o všech zpracovatelských činnostech, včetně účelů zpracování, popisu kategorií dat, bezpečnostních opatření, komplexní mapy datových toků atd. Řada zainteresovaných stran bude muset být zapojena do vytváření a udržování těchto datových záznamů. (Latham & Watkins 2017)

3.1.9 Ochrana osobních údajů dle návrhu a výchozího nastavení

Nařízení vyžaduje vzít v úvahu požadavky na ochranu osobních údajů při navrhování nových technologií nebo pokud jsou zvažovány nové projekty využívající údaje. Pro zajištění shody by se mělo použít posouzení vlivu na soukromí. Posouzení jsou vyžadovány u projektů, které zahrnují rozsáhlé zpracování citlivých osobních údajů nebo odsouzení za trestné činy, sledování veřejného prostoru nebo systematické a rozsáhlé hodnocení automatizovanými prostředky, včetně profilování. (Latham & Watkins 2017)

3.1.10 Smluvní zadávání a zajišťování zakázek

Procesy zadávání zakázek a smlouvy o prodeji budou muset být aktualizovány tak, aby odráželi jak nové požadavky Nařízení, tak závazky plynoucí z postupů, které musí dodržovat strany zpracovávající evropské osobní údaje ve vašem zastoupení. (Latham & Watkins 2017)

3.1.11 Postup při porušení dat

Nařízení zavádí nový režim oznamování porušení údajů. Organizace musí při porušení dat jednat rychle, zmírňovat ztráty a informovat dozorový úřad a dotčené subjekty údajů. Přezkoumání pojistného krytí při porušení údajů a jeho aktualizace je s ohledem na vyšší pokuty a peněžité poplatky namístě. (Latham & Watkins 2017)

3.1.12 Exportování dat

Nařízení povoluje export dat pouze subjektům své skupiny a obchodníkům třetích stran mimo Evropský hospodářský prostor, pokud země, ve které je příjemce těchto údajů zřízen, poskytuje odpovídající úroveň ochrany. U některých firem tedy může být třeba určit všechny přeshraniční datové toky a přezkoumat mechanismy exportu dat. (Latham & Watkins 2017)

3.2 Dotazníkové šetření

K analyzování připravenosti firem na implementaci Nařízení jsem využil kvantitativní výzkum, který jsem realizoval za pomocí online dotazníku vytvořeného

nástrojem Google Docs. Tento typ dotazování jsem zvolil především proto, že jeho vyhodnocení probíhá za využití statistických přístupů. Před rozesláním dotazníku proběhl předvýzkum na malém vzorku respondentů, abych se ujistil, zda výzkumný nástroj funguje a jak. (Eger a Egerová 2014)

Z hlediska typologie bych dotazník charakterizoval jako strukturovaný. Dotazník se skládal z úvodní části, která obsahovala oslovení respondentů, zkráceně vysvětlený účel výzkumu, popis problematiky a na závěr výzvu k vyplnění. V druhé části se již nacházely všechny otázky (demografické a následně náročnější otázky k tématu Nařízení) a po vyplnění dotazníku následovalo poděkování za vyplnění. (Eger a Egerová 2014)

Otázky byly pevně rozděleny do patřičných sekcí a zároveň na sebe navazovaly. Dotazník tvořily ve většině případů uzavřené otázky. Dichotomická otázka, tedy výběr ze dvou odpovědí (ano/ne) byla využita v dotazníku třikrát, a to především na konci jednotlivých sekcí. To pomohlo k následnému rozdělení respondentů a přesměrování na patřičný oddíl dotazníku, který byl pro dotazované relevantní. Z polytomických otázek jsem využil otázky výběrové, kdy respondent musel vybrat jednu z více nabízených možností a otázky výčtové, kde měl na výběr z vícero možností. Největší zastoupení v dotazníku pak měly otázky formou sémantického diferenciálu, tedy bipolárně škálované otázky. Zde jsem využil 6. stupňové škály, jelikož jsem se chtěl vyhnout zaškrtávání neutrálních odpovědí, které představují střed 5. stupňové a 7. stupňové škály. Dále jsem využil několika polootevřených otázek, kde mohli respondenti vybrat z nabízených odpovědí a případně dopsat odpověď vlastní. V poslední řadě jsem do dotazníku zařadil také jednu otevřenou otázku, která se zaměřovala na určení pracovní pozice osoby, která je v dané firmě zodpovědná za zpracování Nařízení. (Eger a Egerová 2014)

Dotazník naleznete v příloze A.

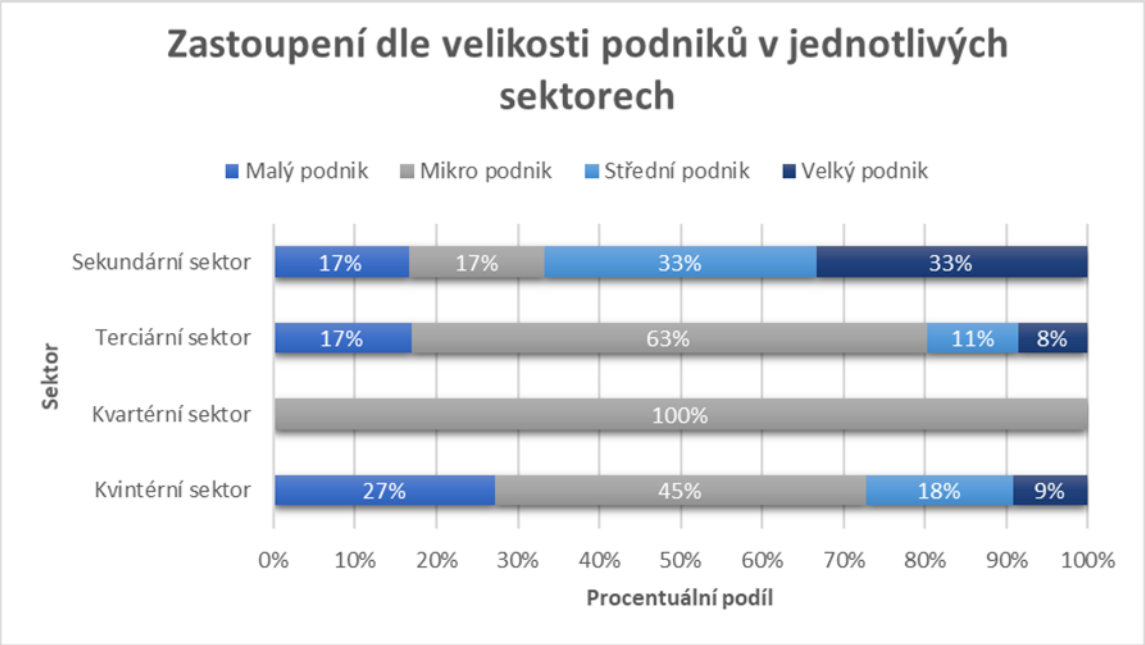
3.3 Analýza

Cílem dotazníkového šetření bylo zjistit, jak moc jsou firmy v České republice připraveny na plnění požadavků, které jim bude Nařízení od 25. května 2018 nově ukládat. Dotazník byl otevřen po dobu jednoho měsíce, a to sice od 30. listopadu do 31. prosince 2017, kdy se mi podařilo získat odpovědi od 96 respondentů. Po vyčistění chybných dat, jsem se dostal na číslo 95 respondentů. Jak jsem již v předchozí části zmínil, dotazník byl

rozdělen do několika částí. Postupně zde budu interpretovat výsledky šetření těchto jednotlivých částí.

V první části dotazníku jsem se dotazoval na demografické údaje, jako je například velikost firmy nebo sektor, ve kterém daná firma podniká. Spojení těchto dvou otázek demonstruje obrázek č. 1. Bohužel se mi nepodařilo získat žádná data z primárního sektoru, a proto je z této analýzy vynechán. Můžeme si povšimnout, že až na sekundární sektor (zde převažují střední a velké podniky), všude převažují mikro podniky. Mikro podniky (do 10 zaměstnanců) mají i největší celkové zastoupení, a to téměř z 60 %. Nejmenší celkové zastoupení je pak na straně velkých podniků s více než 250 zaměstnanci se pohybuje kolem 11,6 %. V celkovém zastoupení všech velikostí podniků v rámci jednotlivých sektorů je nejsilněji zastoupen sektor terciární a to z 74,7 %, sekundární a kvintérní sektor se pohybují kolem 12 %, nejnižší zastoupení má sektor kvartérní a to pouhých 1,1 %.

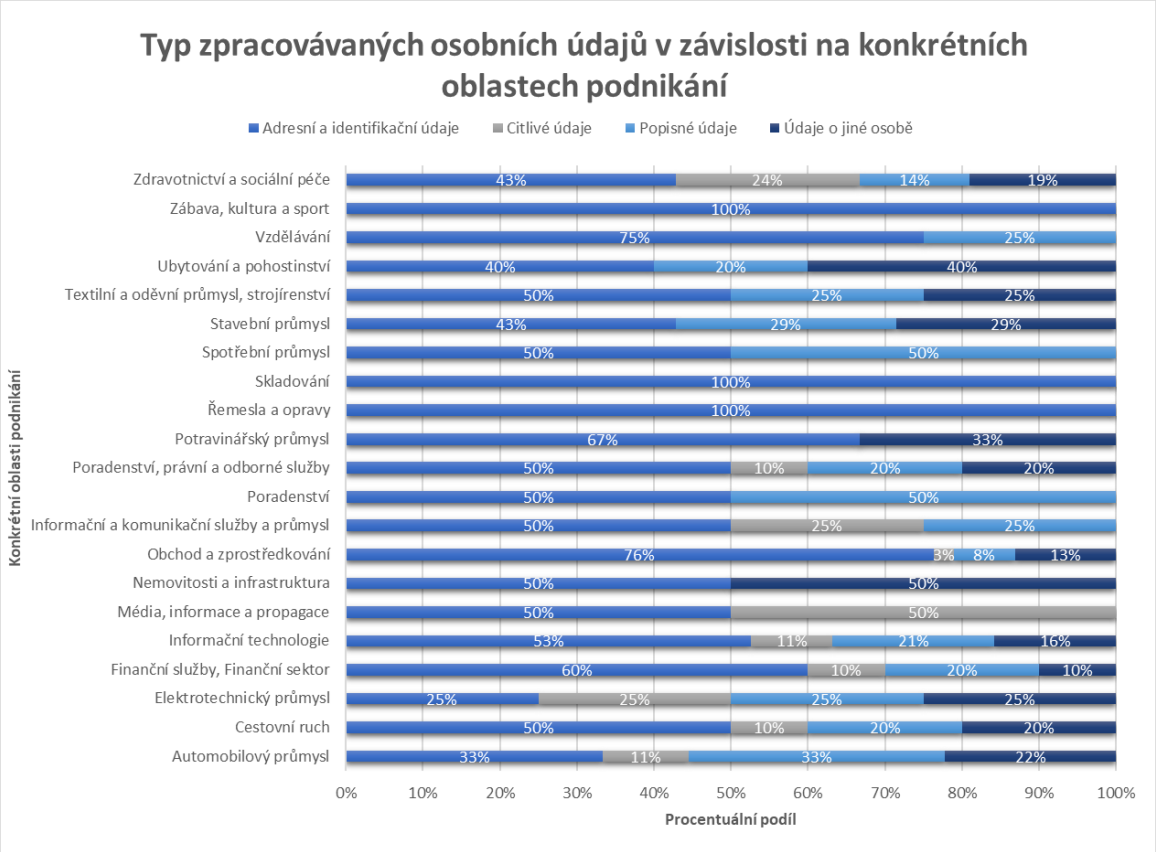
Obrázek č. 1: Zastoupení dle velikosti podniků v jednotlivých sektorech



Zdroj: vlastní zpracování, 2018

V následujícím obrázku č. 2 se podíváme na typy zpracovávaných údajů v závislosti na konkrétní oblasti podnikání firem. Firmy nejvíce zpracovávají adresní a identifikační údaje, a to až v 56,8 % z celkového součtu. Popisné údaje a údaje o jiné osobě zpracovává kolem 17 % dotazovaných a citlivé údaje zpracovává 9,3 % ze všech oblastí. Z výsledků šetření je například zajímavé, že se v elektrotechnickém průmyslu zpracovávají všechny druhy osobních údajů, stejně jako například automobilovém průmyslu.

Obrázek č. 2: Typ zpracovávaných osobních údajů v závislosti na konkrétních oblastech podnikání



Zdroj: vlastní zpracování, 2018

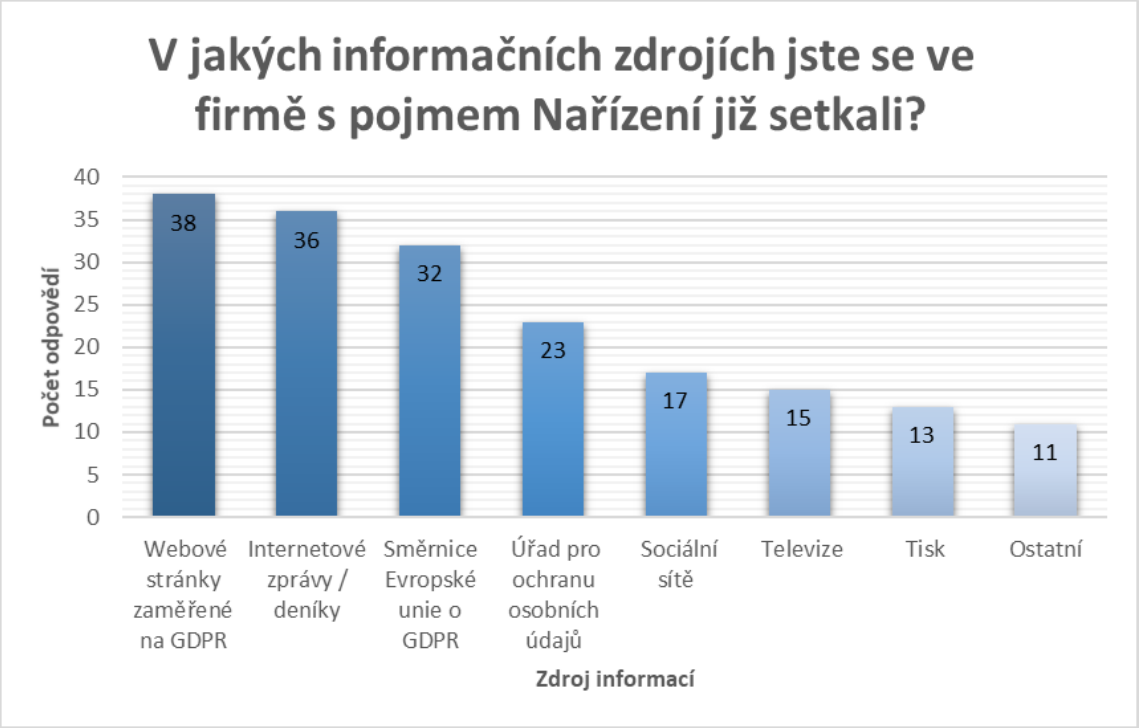
Na otázku, zdali se firmy již setkaly s únikem osobních údajů odpovědělo 96 %, že nikoliv a 4 % firem odpovědělo ano. Osobně jsem předpokládal procento firem postižených únikem údajů nižší.

Poslední otázka první části dotazníku sloužila ke zjištění, zdali respondenti vůbec vědí, co je to Nařízení, a také k rozdělení respondentů podle odpovědi a následnému přesměrování na adekvátní část dotazníku. Z šetření vyplývá, že 32 % respondentů se s pojmem Nařízení vůbec nesetkalo, což je velmi alarmující číslo, s přihlédnutím k faktu, že dotazování probíhalo přibližně půl roku před naplněním jeho platnosti. Jako důvod této neznalosti bych viděl fakt, že v době sběru dat nebylo téma Nařízení až tak moc diskutované, jako začalo být v prvních měsících tohoto roku. Ti, co odpověděli, že se s pojmem Nařízení nesetkali, byli přesměrováni na konec dotazníku. Zbylých 68 % pak pokračovalo na další část.

Ve druhé části jsem se dotazoval, z jakých zdrojů respondenti vědí o Nařízení, viz obrázek č. 3. Na výběr bylo z několika možností (mohlo být zaškrtnuto více odpovědí), ale respondenti využili také možnost písemné odpovědi, ty jsou zařazeny do kategorie

ostatní. V této kategorii zmiňovali kupříkladu školení, rádio, poradenství nebo konzultace s právníky. Respondenti se s Nařízením setkali v nejvíce případech na webových stránkách o Nařízení, jako další nejzastoupenější zdroj jsou internetové zprávy, následované samotnou směrnicí o Nařízení.

Obrázek č. 3: V jakých informačních zdrojích jste se ve firmě s pojmem Nařízení již setkali?



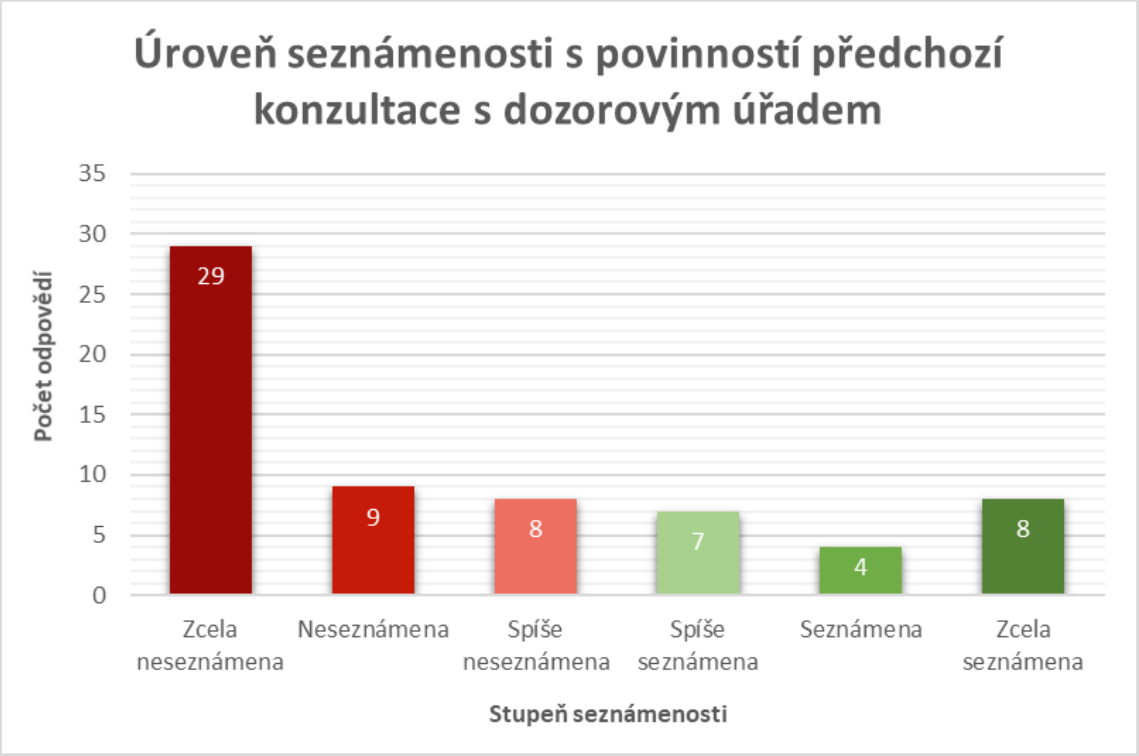
Zdroj: vlastní zpracování, 2018

Dále jsem se snažil zjistit, na kolik jsou firmy seznámeny s určitými novými povinnostmi, které Nařízení přináší, a to formou hodnocení na škále 1 (zcela neseznámeny) až 6 (zcela seznámeny). Ohodnoceny byly následující povinnosti:

- povinnost vést záznamy o činnostech zpracování,
- posouzení vlivu na ochranu osobních údajů,
- předchozí konzultace s dozorovým úřadem,
- ohlašování případu porušení zabezpečení osobních údajů dozorovému úřadu,
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů,
- ustavení pověřence pro ochranu osobních údajů.

Zde bylo zajímavé zjištění, že téměř 45 % procent dotazovaných je zcela neseznámeno s povinností předchozí konzultace s dozorovým úřadem, viz obrázek č. 4. Důvodem může být fakt, že tato povinnost není ve většině materiálů zmíněna nebo jednoduše není mezi nejdiskutovanějšími částmi Nařízení.

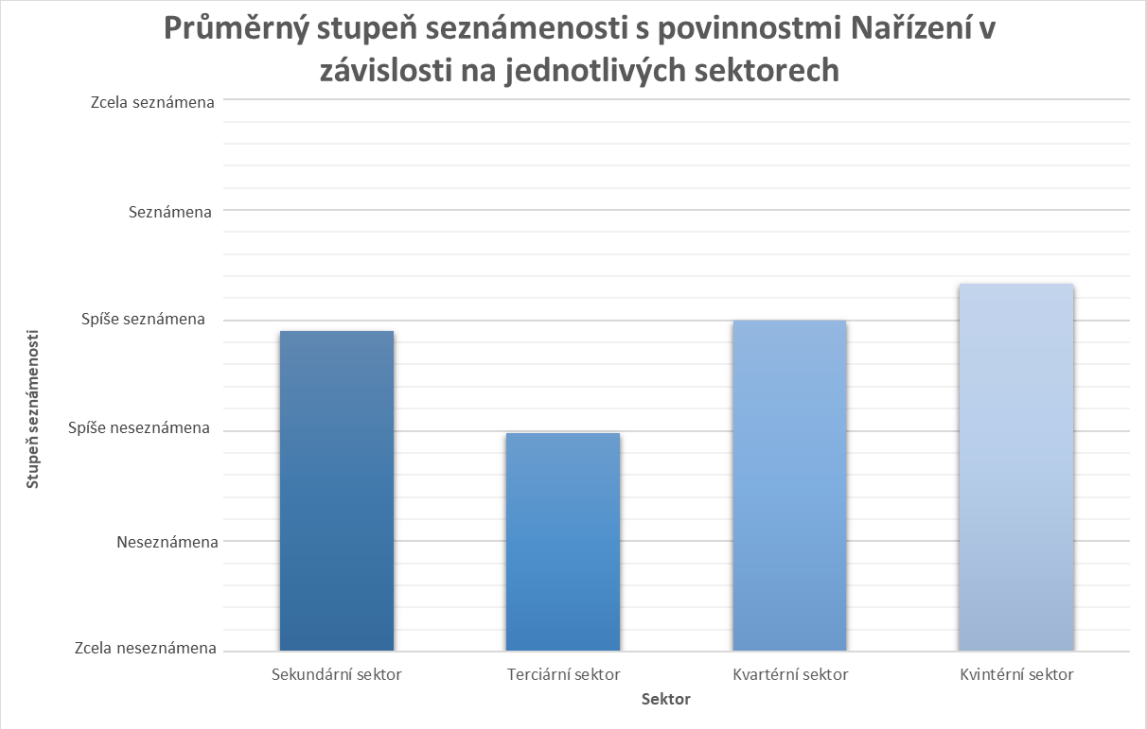
Obrázek č. 4: Úroveň seznámenosti s povinností předchozí konzultace s dozorovým úřadem



Zdroj: vlastní zpracování, 2018

Povinnost ohlašování porušení zabezpečení údajů jak dozorovému úřadu, tak subjektu údajů skončilo hned za předchozí povinností, a to v obou případech s 32 % zcela neseznámených, což je poněkud překvapující, protože tato povinnost je jednou z nejvíce diskutovaných a pokud firmy porušení neoznámí, mohou dostat pokutu až do výše 20 milionů EUR nebo do výše 4 % ročního obratu firmy. Hodnocení ostatních povinností bylo vcelku vyrovnané, a v průměru se pohybovalo mezi možnostmi „spíše neseznámena“ a „spíše seznámena“. Následující obrázek č. 5 demonstruje, jak moc jsou v průměru jednotlivé sektory seznámeny se všemi šesti vybranými povinnostmi, které hodnotily. Dle očekávání má nejvyšší skóre kvintérní sektor, který zastupují IT firmy a u nichž jsem očekával vyšší míru seznámenosti, to stejné platí i pro kvartérní sektor, který zastupovalo poradenství. Překvapující je ale rozdíl mezi sekundárním a terciárním sektorem, kde jsem rozdíl předpokládal znatelně menší. Zároveň jsem čekal, že terciární sektor bodově převýší sekundární a ne naopak. Zde je možným vysvětlením zastoupení sektorů. Sekundární sektor obsahuje více středních a velkých firem (lze předpokládat lepší připravenost), kdežto sektor terciární zastupuje velké množství malých a mikro podniků.

Obrázek č. 5: Průměrný stupeň seznámenosti s povinnostmi Nařízení v závislosti na jednotlivých sektorech



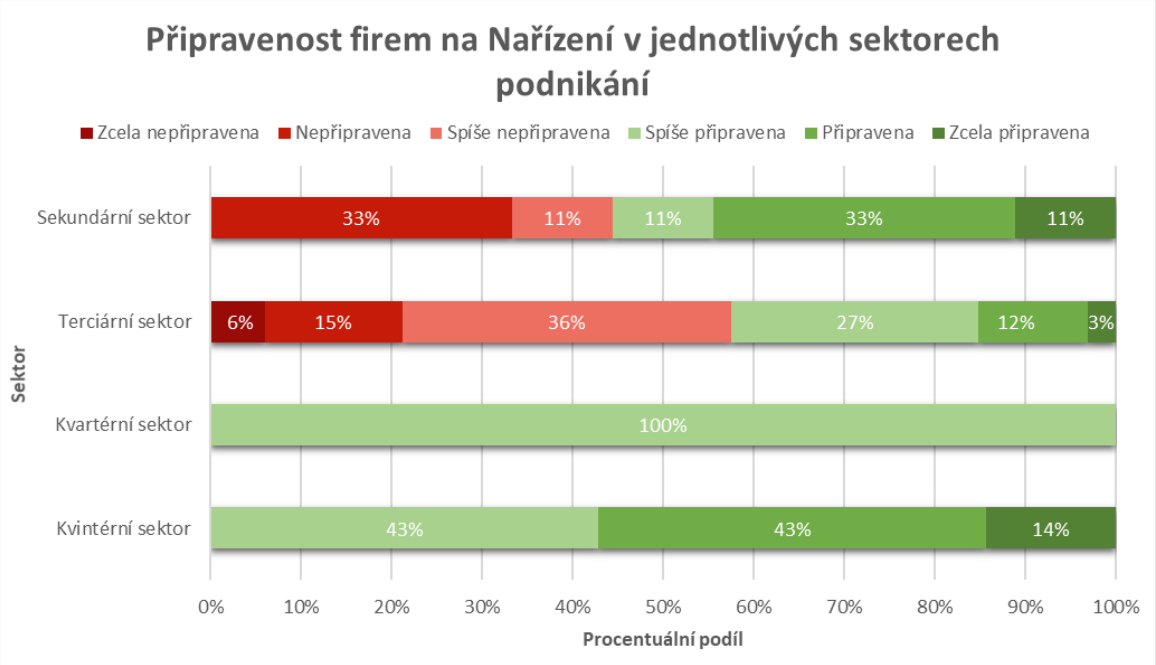
Zdroj: vlastní zpracování, 2018

V následující otázce jsem zjišťoval, zdali se již daná firma začala zabývat otázkou přípravy na Nařízení. Jelikož tohle byla poslední otázka druhé části dotazníku, plnila opět rozdělovací funkci. Pokud respondenti uvedli, že se firma ještě přípravou na Nařízení nezabývá, byli přesměrováni na jinou část dotazníku než respondenti, kteří uvedli opak. Z otázky vyplývá, že lehce přes 23 % firem se přípravou nezačalo v době sběru dat zabývat. Předpokládal jsem však, že se toto procento bude pohybovat výše, a to zhruba na úrovni kolem 30 %. V následující sekci dotazníku jsme se ptal, z jakých důvodů se ještě ve firmě přípravou nezačali zabývat. Na výběr bylo ze tří odpovědí a jedné otevřené, přičemž šlo zaškrtnout více odpovědí najednou. Jako nejčastější důvod byla uváděna časová vytíženost firmy a to v 11 případech následované nedostatkem informací k problematice v 6 případech a nedostatečnou srozumitelností informací v 5 případech. Otevřené odpovědi využil pouze jeden dotazovaný a jako důvod uvedl, že je jeho firma příliš malá (má jednoho zaměstnance). Respondenti, kteří se přípravou začali zabývat (77 %), byli přesměrováni na poslední část dotazníku.

V poslední sekci dotazníku jsem se zaměřil na konkrétní dotazy v ohledu Nařízení a jeho implementace. Na obrázku č. 6 můžeme vidět, na kolik jsou firmy z jednotlivých sektorů připravené na plnění povinností Nařízení. Připravenost firmy byla hodnocena na škále

„zcela nepřipravena“ (1) až „zcela připravena“ (6). Můžeme si všimnout, že v každém ze sektorů převládají spíše stupnice připravené (tedy stupnice spíše připravena až zcela připravena), což vypadá poměrně optimisticky, ale i přesto se v některých sektorech vyskytuje poměrně velké procento nepřipravených firem. Příkladem může být výskyt 6,06 % zcela nepřipravených firem v terciárním sektoru. V celkovém součtu je ale pak pouhých 6 % firem „zcela připraveno“ a 48 % (spíše připravena a připravena) už má větší část příprav za sebou. Na druhé straně máme 4 % „zcela nepřipravených“ firem a 42 % firem, které jsou „spíše nepřipraveny“ či „nepřipraveny“.

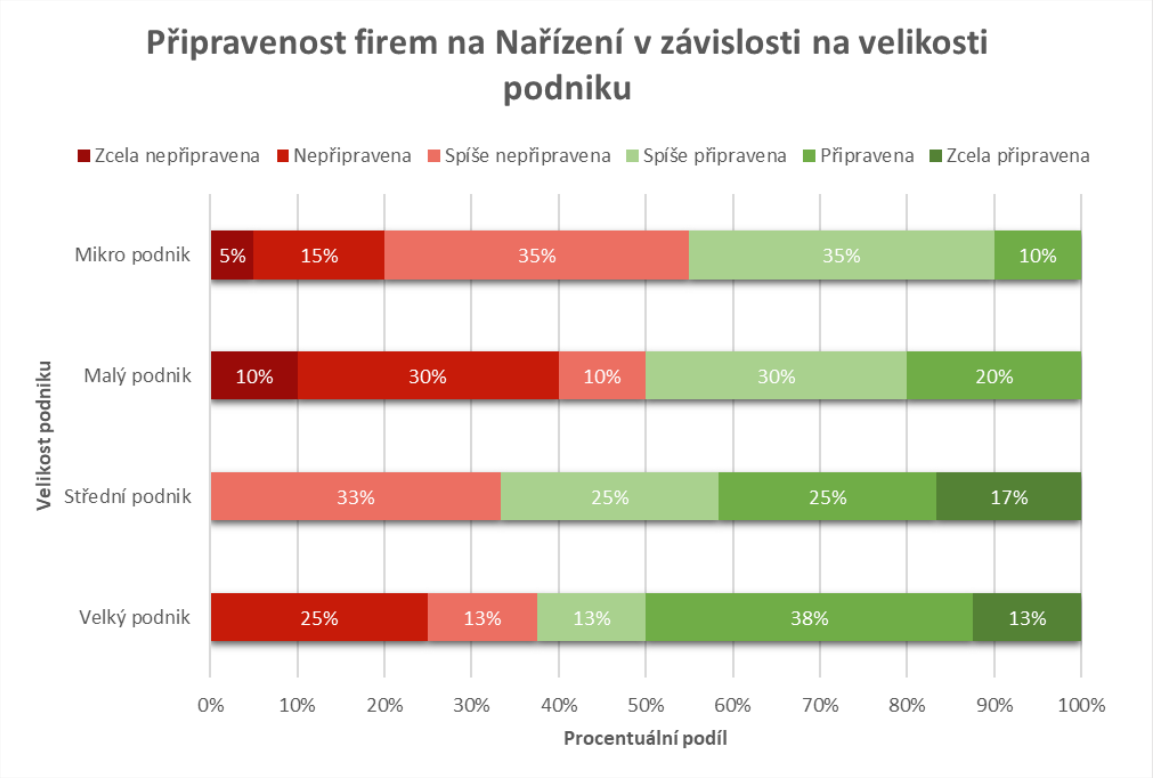
Obrázek č. 6: Připravenost firem na Nařízení v jednotlivých sektorech podnikání



Zdroj: vlastní zpracování, 2018

Zajímavá je též aplikace celkové připravenost firem v závislosti na velikosti podniku, viz obrázek č. 7. Zde můžeme vidět, že zcela připravené firmy se nacházejí pouze mezi středními a velkými podniky. Zde též převládají firmy „spíše připravené“ a „připravené“. U mikro podniků naopak převažují „zcela nepřipravené“ až „spíše nepřipravené“ firmy. U malých podniků je tento poměr vyrovnaný na 50 %.

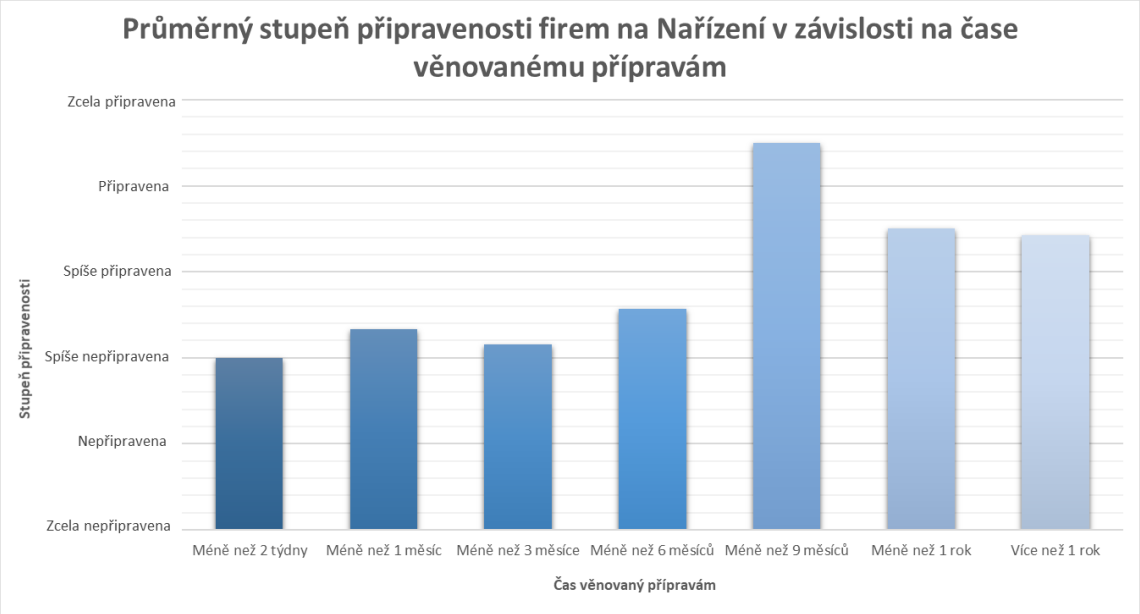
Obrázek č. 7: Připravenost firem na Nařízení v závislosti na velikosti podniku



Zdroj: vlastní zpracování, 2018

Na obrázku č. 8 můžeme vidět závislost mezi připraveností firmy na Nařízení a časem vynaloženým na přípravu. Připravenost firmy byla hodnocena opět na škále „zcela nepřipravena“ (1) až „zcela připravena“ (6), kdežto čas příprav jsem rozdělil do 7 intervalů. Jak si můžeme z obrázku č. 8 povšimnout, stupeň připravenosti značně ovlivňuje doba, která je potřebná na samotnou přípravu. Z šetření se nám jeví jako nejvíce adekvátní doba implementace od 6. do 9. měsíců, kde je průměrný stupeň připravenosti nejvyšší a pohybuje se mezi „připravena“ a „zcela připravena“. Zároveň ale z šetření vyplývá, že čas věnovaný přípravám delší než 9 měsíců ovlivňuje celkovou připravenost spíše negativně a připravenost klesá. Můžeme také konstatovat, že až na výjimku (méně než 3 měsíce), stupeň připravenosti roste až po interval 9. měsíce.

Obrázek č. 8: Průměrný stupeň připravenosti firem na Nařízení v závislosti na čase věnovanému přípravám

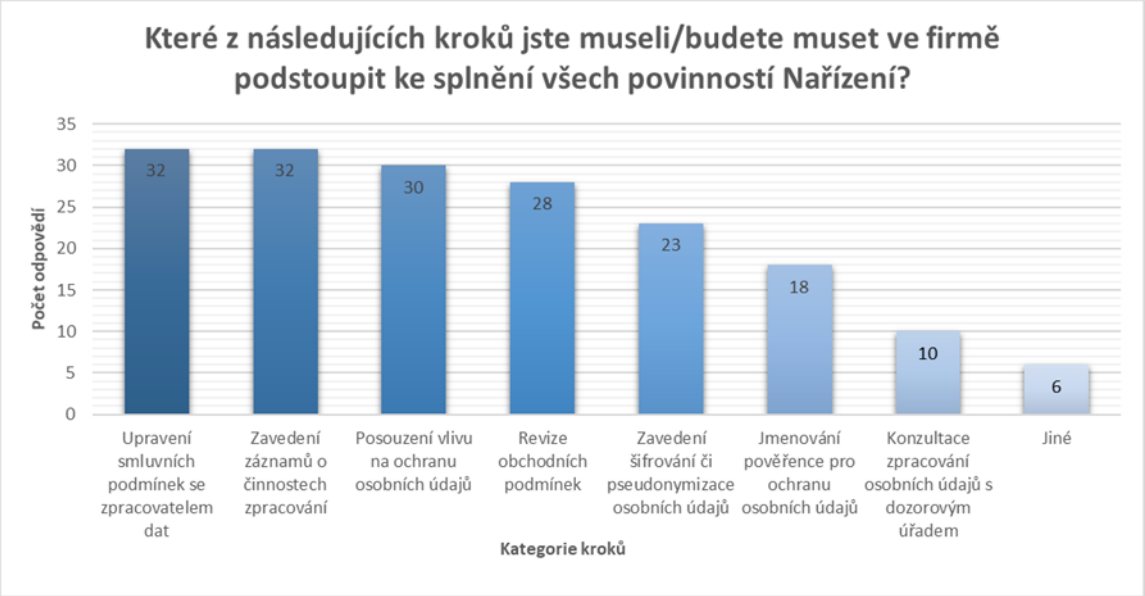


Zdroj: vlastní zpracování, 2018

Dotazovaní též uváděli formou otevřené odpovědi, na jakých pracovních pozicích se nachází osoby pověřené implementací Nařízení. Největší zastoupení zde zastupují manažeři vyšší úrovně, jako například majitelé, ředitelé či jednatelé společnosti. O polovinu nižší, avšak stále významné zastoupení reprezentují HR a IT specialisti a také různí vedoucí pracovníci. Dva dotazovaní uvedli, že nikoho pověřeného ve firmě nemají.

Další otázka byla zaměřena na zjištění, jaké z uvedených kroků musí firma podstoupit, aby plnila všechny povinnosti, které jí Nařízení ukládá. Zde bylo opět možné vybrat více předepsaných odpovědí a také uvést odpověď vlastní. Obrázek č. 9 nám tedy ukazuje sestupně seřazené kroky, které jsou pro firmy nezbytné pro splnění všech povinností. Můžeme si například všimnout, že jmenování pověřence či konzultace s dozorovým úřadem nejsou tak časté, což se dá předpokládat vzhledem k faktu, že tato povinnost vzniká firmám pouze v určitých případech, které se až tak často nevyskytují. Do kategorie jiné byly opět zařazeny otevřené odpovědi, například zrevidování souhlasu zaměstnanců s uchováním osobních údajů, skartace smluv nebo konzultace s právníky.

Obrázek č. 9: Které z následujících kroků jste museli/budete muset jako firma podstoupit ke splnění všech povinností Nařízení?



Zdroj: vlastní zpracování, 2018

Poslední dvě otázky z dotazníku zjišťovali, jak firmy hodnotí na škále 1 až 6 srozumitelnost informací o Nařízení („zcela nesrozumitelné“ až „zcela srozumitelné“) a jejich dostupnost („velmi špatná“ až „velmi dobrá“). Firmy, které se ještě nezačaly zabývat přípravou, hodnotily srozumitelnost i dostupnost v průměru na 2,3 bodu z maxima 6. bodů. Firmy, které se již přípravou zabývaly, hodnotily srozumitelnost průměrně na 2,7 bodu a dostupnost na 3,0 bodu z maxima 6. bodů. Z těchto výsledků si lze vyvodit, že ani jedna skupina dotazovaných nehodnotí srozumitelnost a dostupnost zcela kladně, což může mít na jedné straně za následek jak odkládání přípravy na Nařízení, tak dlouhou dobu implementace na straně druhé.

4 Zhodnocení výsledků analýzy

4.1 Zhodnocení výsledků analýzy

Analyzoval jsem data od 95 respondentů zastupujících firmy napříč různými sektory. První zajímavé zjištění, které z analýzy vyplývá je, že 32 % z celkového počtu dotazovaných se s pojmem Nařízení ve firmě doposud nesetkalo, což je poměrně alarmující výsledek. Můj osobní odhad se před rozesláním dotazníku pohyboval kolem 20 %, už vzhledem k tomu, že se toto téma objevovalo v nejčtenějších internetových denících či v televizi, ještě před rozesláním dotazníku. Výzkum nám však ukazuje, že je neznalost tohoto pojmu je 1,6krát vyšší, než jsem předpokládal.

Zbylých 68 % dotazovaných se dále snažilo zhodnotit, na kolik je jejich firma seznámena s vybranými povinnostmi. S většinou povinností jsou firmy lehce nadprůměrně seznámeni. Zde vynikala především povinnost předchozí konzultace s dozorovým úřadem, a to z toho důvodu, protože obdržela nejvyšší počet hodnocení od firem jako „zcela neseznámena“. Jak jsem již zmínil předešle, tato povinnost není jednou z těch často skloňovaných, a proto pravděpodobně dopadlo její hodnocení takto špatně.

V další z hlavních otázek jsem se snažil zjistit, které firmy se již samotnou přípravou na implementaci začaly zabývat, a které nikoliv. Zde již bylo procento nižší než u otázky ohledně pojmu Nařízení, a to sice 23,8 %. I když se procento nejeví až tak vysoké, po sečtení firem, které se s pojmem Nařízení ještě nesetkaly a firem, které se ještě nezačaly nijak připravovat, se dostaneme na 47,4 %. Téměř polovina dotazovaných firem se tedy doposud vůbec nezabývala problematikou implementace opatření vůči Nařízení, což je vzhledem k blížícímu se datu platnosti směrnice vskutku překvapivé. To, že se firmy přípravou doposud nezabývaly, připisovaly především jejich časové vytíženosti. Respondenti, kteří se přípravou již zabývat začali, přešli na poslední část dotazníku.

Nutno podotknout, že se i v této části se mohly vyskytnout nepřipravené firmy, což by ještě zvýšilo jejich procentuální podíl. Abych zjistil, které firmy jsou připravené, a které ne, položil jsem jim otázku hodnocení připravenosti firmy, na škále „zcela nepřipravena“ (1) až „zcela připravena“ (6). I když jsem si nemyslel, že by se zde vyskytla nějaká zcela nepřipravená firma, opak byl pravdou. Konkrétně se 4 % firem ohodnotilo jako zcela nepřipravených. Firmy, které se na škále ohodnotily jako „nepřipravené“ bylo 16 % a jako „spíše nepřipravené“ se ohodnotilo 26 % dotázaných. Škálu jsem volil 6. stupňovou,

a to proto, abych se v odpovědích vyhnul střední hodnotě, tedy že firma není „ani připravena, ani nepřipravena“. Z logiky věci můžeme konstatovat, že všechny firmy, které se ohodnotili na prvních třech stupních nepřipravenosti, nejsou dostatečně připravené. Celkový podíl firem, které se přípravou již zabývají, ale jsou nepřipraveny je 46 %, což je znovu téměř polovina. Ještě bych zde rád zmínil, že pouhých 6 % firem se cítí být zcela připraveno. Jako „připravena“ se ohodnotilo na 20 % firem a 28 % se na stupnici hodnotí jako „spíše připravených“.

Pokud bychom tedy znovu dali dohromady podíl všech dotazovaných firem jak z předminulého odstavce (firmy, které se s pojmem Nařízení nesetkaly nebo se přípravou na něj ještě nezačaly zabývat), tak firem „nepřipravených“ z minulého odstavce, dostaneme celkové procento firem nepřipravených na plnění povinností Nařízení. Celkový podíl nepřipravených firem je 72 % a reprezentuje jej obrázek č. 10, kde můžete zároveň vidět i zastoupení z jednotlivých částí dotazníku.

Obrázek č. 10: Celkové výsledky dotazníkového šetření

Zdroj: vlastní zpracování, 2018

4.2 Doporučení

Vzhledem k výsledkům výzkumu by bylo dobré uvést si nějaká obecná doporučení, a to především pro firmy, které se otázkou Nařízení doposud nezabývaly.

Jako první z kroků, který by měla firma podstoupit, je zjistit si, jaký typ osobních údajů zpracovává a případně provést posouzení vlivu na ochranu osobních údajů. Na základě výsledků těchto zjištění bude třeba aplikovat náležitá opatření. Těmito opatřeními může být kupříkladu upravení smluvních podmínek se zpracovatelem (vymezení odpovědnosti) nebo revize obchodních podmínek – zde je důležité subjekt údajů informovat jaké osobní údaje firma zpracovává, za jakým účelem či na jak dlouhou dobu je hodlá uschovat. Pokud má firma nějaké zaměstnance, je určitě na místě zrevidovat jejich souhlasy se zpracováním osobních údajů. Každá firma též bude muset vést záznamy o činnostech zpracování, jejich zavedení by měl být tedy jeden z dalších kroků.

I přes velké množství článků a návodů na internetu nebo v publikacích, jak se na Nařízení připravit, není pro firmy lehké se v celé problematice zorientovat. Zde se naskýtá příležitost využít různých poradenských firem, které se specializují například na audity či školení v oblasti problematiky Nařízení. Po provedení auditů, jsou pak firmám poradenské společnosti schopny sdělit, jaká nápravná opatření podniknout. Je však samozřejmé, že práce poradenské firmy bude něco stát, na což je také třeba brát ohled. Firmy by ale měly brát v potaz výši sankcí, které mohou být uloženy při neplnění uložených povinností. Sankce jsou totiž opravdu vysoké a troufám si tvrdit, že pro většinu firem mohou být i likvidační.

4.3 Vliv General Data Protection Regulation na situaci v České republice

Z výsledků dotazníkového šetření jsem zjistil, že pouze necelá třetina dotázaných firem je připravena na plnění povinností Nařízení. Naskýtá se nám tedy otázka, zda je situace v České republice opravdu tak kritická? Pokusím se otázku zodpovědět na následujících řádcích.

Jakmile Nařízení vejde v platnost, nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů, dle kterého se měly firmy při zpracování údajů doposud řídit. Je důležité podotknout, že Nařízení nerozšiřuje svoji působnost ani neprovádí žádné změny v základních zásadách zpracování údajů oproti současnému zákonu. Pojmy jako správce,

zpracovatel nebo osobní údaj a další zůstávají také beze změny. Nařízení především klade větší důraz na zpracování osobních údajů, ale typicky bude tento důraz kladen na velké správce údajů, kteří zpravidla zpracovávají velké množství údajů a tyto údaje jsou zároveň rizikové, tedy že zde vzniká při zpracování riziko pro svobody a práva fyzických osob. Pokud se ale zaměříme na drobné živnostníky, zjistíme, že pro ně Nařízení žádné zásadní změny nepřinese, jelikož zpracovávají osobní údaje zákazníků pouze pro účely poskytnutí výrobku či služeb. V jejich případě pak bude především potřeba sledovat dodržování základních zásad zpracování. (www.uoou.cz 2017c)

Pokud tedy dáme dohromady informace z předchozího odstavce a výsledky mého výzkumu, zjistíme, že se situace nejeví natolik kriticky, jak se na první pohled zdálo. Jelikož 60 % mého výzkumu tvořily mikro podniky, tedy firmy s maximem deseti zaměstnanců, je velmi pravděpodobné, že ani žádné zásadnější přípravy nebudou muset podstoupit – jedná se o drobné živnostníky. Pravděpodobně také nebudou potřebovat na zajištění dodržování základních zásad zpracovaní více jak několik měsíců. Samozřejmě firmy s většími počty zaměstnanců nebo firmy zpracovávající rizikové osobní údaje budou muset podstoupit více přípravných opatření, což logicky zabere také větší množství času. Největší vliv tedy bude mít Nařízení právě na větší správce a zpracovatele.

Závěr

V první teoretické části jsme si představili a vysvětlili pojem Nařízení. Seznámili jsme se s dalšími nejdůležitějšími pojmy spojenými s tímto tématem. Zásady a práva jsme si také podrobněji rozebrali. Posledním pojmem v této časti byly sankce, kde jsme se dozvěděli, jak vysoké sankce může dozorový úřad uložit za porušení Nařízení, jaký je jejich smysl, či co všechno musí dozorový úřad brát při ukládání pokuty v potaz.

Dále jsme si představili jedenáct zákonů, které se alespoň z malé části týkají osobních údajů. Zjistili jsme, z jaké směrnice vychází doposud využívaný zákon o ochraně osobních údajů, který má být nahrazen právě Nařízením. Také jsme zjistili, jak se k tématu osobních údajů staví například listina práv a svobod či trestní zákoník, kde jsou uvedené postihy za narušení osobních údajů.

Jak již bylo zmíněno, cílem této práce bylo zjistit připravenost firem na Nařízení v České republice. Nejdříve jsme si ukázali, na jaké aspekty by se firmy při přípravě na Nařízení měly zaměřit. Charakterizovali jsme si dotazník, který jsem vytvořil za pomocí nástroje Google Docs, a který my posloužil pro sběr odpovědí od 96 respondentů. Po vyčistění dat jsme se pak dostali na číslo 95. Data byla statisticky zpracována tak, aby bylo možné zjistit různé závislosti mezi otázkami v dotazníku. Tyto závislosti byly demonstrované za pomocí grafů a také slovního komentáře.

Při vyhodnocování výsledků v poslední části této práce jsme se dozvěděli, jestli jsou firmy, které dotazník vyplnily připravené či nikoliv, a také do jaké míry se cítí být připraveny. Dotazník byl záměrně rozdělen do tří částí, abych zajistil, že budu pracovat pouze s validními daty. Z první části, která se zaměřovala spíše na demografické údaje, se nám takto vyselektovalo hned necelých 32 % respondentů, kteří se ve firmě s pojmem Nařízení ještě nesetkali. V další části jsme zjistili, jak jsou na tom firmy a jejich seznámenost s povinnostmi Nařízení. Konečná otázka opět rozdělila respondenty na dvě skupiny. Na 77 % firem z této skupiny se již přípravou na Nařízení zabývat začalo, a respondenti mohli tedy pokračovat na část poslední. Zbytek dotazovaných nám již pouze uvedl, z jakých důvodů se přípravou dosud nezabývali. Zde převažovala časová vytíženost firem. V poslední části jsme se pak dozvěděli, jak moc jsou či nejsou firmy připraveny. Zde se za pomocí škály ohodnotilo celých 46 % firem jako nepřipravených. V konečném součtu všech dotázaných firem nám pak vyšlo, že procentuální podíl připravených firem tvoří pouze 28,42 %, což byl opravdu překvapující výsledek.

Vzhledem k výsledkům šetření jsem také sepsal stručné doporučení, kterým by se mohly dotyčné firmy inspirovat, jakmile se začnou přípravou zabývat. Při hodnocení vlivu Nařízení na situaci v České republice jsme dospěli k závěru, že situace možná nebude až tak kritická, protože Nařízení znamená velké změny především pro střední a velké podniky a jak vyplynulo také z šetření, ty se řadily z větší části mezi firmy již připravené. Velký počet nepřipravených firem jsme pozorovali spíše mezi mikro a malými podniky. Pro většinu z nich by ale zavedení Nařízení nemělo znamenat až tak velkou změnu, jelikož se zákon o ochraně osobních údajů, který byl do teď v platnosti, řadil mezi ty přísnější ve srovnání se zákony ostatních členských států EU.

Seznam obrázků

Seznam použitých zkratek

EU	Evropská unie
EUR	Euro
HR	Human resources, v překladu lidské zdroje
IT	Informační technologie
Nařízení	General Data Protection Regulation
Pověřenec	Pověřenec pro ochranu osobních údajů

Seznam použité literatury

Monografické publikace a elektronické monografie

Eger, L., & Egerová, D. (2014). *Základy metodologie výzkumu: pro studenty ekonomických oborů*. V Plzni: ZČU.

Evropský parlament a Rada Evropské unie. (1995). *Směrnice Evropského parlamentu a Rady 95/46/ES*. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31995L0046&from=CS

Evropský parlament a Rada Evropské unie. (2002). *Směrnice Evropského parlamentu a Rady 2002/58/ES*. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS

Evropský parlament a Rada Evropské unie. (2016). *Nařízení evropského parlamentu a rady (eu) 2016/679*. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=en

Janečková, E., & Bartík, V. (2016). *Ochrana osobních údajů v pracovním právu: (otázky a odpovědi)*. Praha: Wolters Kluwer Česká republika.

Latham, & Watkins. (2017). *GDPR Compliance Checklist*. Dostupné z: https://www.globalprivacyblog.com/files/2017/05/GDPR-Compliance-Checklist-003.pdf

Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., & Tomíšek, J. (2017). *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer.

Parlament České republiky. (2009). *Sbírka zákonů* (Částka 11). Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5405

Parlament České republiky. (2010). *Sbírka zákonů* (Částka 95). Dostupné z: http://www.mvcr.cz/soubor/sbirka-zakonu-dokumenty-sb095-10-pdf.aspx

Redakce Sagit. (2017). *Ochrana osobních údajů: zákon o ochraně osobních údajů a další právní předpisy. GDPR – obecné nařízení Evropského parlamentu a rady (EU) 2016/679, o ochraně osobních údajů: redakční uzávěrka 28.8.2017*. Ostrava: Sagit.

Internetové zdroje

www.oou.cz (2014). *Ochrana osobních údajů.* Cit. 24.2.2018, dostupné z: http://www.oou.cz/

www.uoou.cz (2017a). *Úřad pro ochranu osobních údajů.* Cit. 1.2.2018, dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

www.uoou.cz (2017b). *Úřad pro ochranu osobních údajů.* Cit. 1.2.2018, dostupné z: https://www.uoou.cz/zakladni-prirucka/ds-4744/archiv=0&p1=3938

www.uoou.cz (2017c). *Úřad pro ochranu osobních údajů.* Cit. 11.3.2018, dostupné z: https://www.uoou.cz/1-obecne-na-izeni/d-27266

cs.wikipedia.org (2018). *Wikipedie.* Cit. 16.3.2018, dostupné z: https://cs.wikipedia.org/wiki/Osobn%C3%AD_%C3%BAdaj

www.zakonyprolidi.cz (2017). *101/2000 Sb. Zákon o ochraně osobních údajů*. Cit. 24.2.2018, dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

Seznam příloh

Přílohy

Příloha A: Dotazník

Připravenost firem na General Data Protection Regulation

Dobrý den,

věnujte prosím několik minut svého času vyplnění následujícího dotazníku, který slouží jako průzkum připravenosti firem v ČR na General Data Protection Regulation(dále jen „GDPR").

GDPR, neboli obecné nařízení o ochraně osobních údajů je nová směrnice Evropské Unie, která vstupuje v platnost 25. května 2018 a dotkne se každého, kdo shromažďuje nebo zpracovává osobní údaje Evropanů.

Dotazník je součástí bakalářské práce, která je vypracovávána na stejné téma na Fakultě ekonomické ZČU v Plzni. Dotazování je anonymní.

Předem děkuji za spolupráci.

Tadeáš Janda

janda.tadeas@gmail.com

*Povinné pole

1. Jaká je velikost Vaší firmy/firmy, ve které pracujete? *

- ◯ Mikro podnik (méně než 10 zaměstnanců)
- ◯ Malý podnik (méně než 50 zaměstnanců)
- ◯ Střední podnik (méně než 250 zaměstnanců)
- ◯ Velký podnik (více než 250 zaměstnanců)

2. V jakém sektoru Vaše firma podniká? *

- ◯ Primární sektor (prvovýroba) - získání produktů a surovin z přírody a obdělávání půdy (těžba, lesnictví, zemědělství, rybářství)
- ◯ Sekundární sektor (druhovýroba) - zpracování produktů z prvovýroby a výroba hmotných statků - průmysl
- ◯ Terciární sektor (služby) - doprava, zdravotnictví, obchod, školství, kultura a komunální služby
- ◯ Kvartérní sektor (znalostní sektor) - věda, výzkum, vysokoškolské vzdělávání, poradenství
- ◯ Kvintérní sektor (nejpokročilejší technologie) - high-tech (informační technologie, biotechnologie, nanotechnologie)

3. V jaké konkrétní oblasti podniká Vaše firma?

Vyberte prosím z příslušného sektoru (na základě předchozí otázky) konkrétní oblast podnikání Vaší firmy.

3.1. Primární sektor

Vyberte

3.2. Sekundární sektor

Vyberte

3.3. Terciární sektor

Vyberte

3.4. Kvartérní sektor

Vyberte

3.5. Kvintérní sektor

Vyberte

4. Které z níže uvedených osobních údajů Vaše firma zpracovává? *

- [ ] Adresní a identifikační údaje (jméno, příjmení, datum a místo narození, rodinný stav, rodné číslo, státní příslušnost, adresa trvalého bydliště, telefon)
- [ ] Citlivé údaje (údaje vypovídající o národnostním, rasovém nebo etnickém původu, členství v odborových organizacích, odsouzení za trestný čin, sexuálním životě, genetickém údaji, politických postojích, náboženství a filosofickém přesvědčení, zdravotním stavu nebo biometrickém údaji)
- [ ] Popisné údaje (vzdělání, znalost cizích jazyků, odborné znalosti a dovednosti, počet dětí, obrazový záznam z kamerového systému, vojenská služba, předchozí zaměstnání, zdravotní pojišťovna, mzda, číslo cestovního dokladu, bankovní spojení apod.)
- [ ] Údaje o jiné osobě (adresní a identifikační údaje člena rodiny, manžel/manželka, dítě apod.)

5. Setkala se někdy Vaše firma s únikem osobních údajů? *

- ○ Ano
- ○ Ne

6. Setkali jste se již ve Vaší firmě s pojmem GDPR? *

- ○ Ano
- ○ Ne

DALŠÍ

*Povinné pole

Míra seznámenosti s GDPR

7. V jakých informačních zdrojích jste se ve firmě s pojmem GDPR již setkali? *

- [ ] Směrnice Evropské unie o GDPR
- [ ] Úřad pro ochranu osobních údajů
- [ ] Webové stránky zaměřené na GDPR
- [ ] Sociální sítě (Facebook, Twitter, YouTube, LinkedIn, atd..)
- [ ] Internetové zprávy / deníky
- [ ] Televize
- [ ] Tisk
- [ ] Jiné: _____

8. Jak dlouho je Vaše firma s tímto pojmem odhadem obeznámena? *

Vyberte

9. Ohodnoťte na stupnici 1 - 6, na kolik je Vaše firma seznámena s novými povinnostmi, které GDPR přináší.

9.1. Povinnost vést záznamy o činnostech zpracování. *

	1	2	3	4	5	6	
Zcela neseznámena	○	○	○	○	○	○	Zcela seznámena

9.2. Posouzení vlivu na ochranu osobních údajů. *

	1	2	3	4	5	6	
Zcela neseznámena	○	○	○	○	○	○	Zcela seznámena

9.3. Předchozí konzultace s dozorovým úřadem. *

	1	2	3	4	5	6	
Zcela neseznámena	○	○	○	○	○	○	Zcela seznámena

9.4. Ohlašování případu porušení zabezpečení osobních údajů dozorovému úřadu. *

	1	2	3	4	5	6	
Zcela neseznámena	○	○	○	○	○	○	Zcela seznámena

9.5. Oznamování případu porušení zabezpečení osobních údajů subjektu údajů. *

	1	2	3	4	5	6	
Zcela neseznámena	○	○	○	○	○	○	Zcela seznámena

9.6. Ustavení pověřence pro ochranu osobních údajů. *

	1	2	3	4	5	6	
Zcela neseznámena	○	○	○	○	○	○	Zcela seznámena

10. Začala se již Vaše firma zabývat otázkou přípravy na GDPR? *

- ○ Ano
- ○ Ne

ZPĚT DALŠÍ

*Povinné pole

Míra připravenosti na GDPR

11. Jak hodnotíte připravenost Vaší firmy na GDPR? *

	1	2	3	4	5	6	
Zcela nepřipravena	○	○	○	○	○	○	Zcela připravena

12. Na jaké pozici se ve Vaší firmě nachází osoba/osoby zodpovědná/zodpovědné za zpracování GDPR? *

Vaše odpověď

13. Které z následujících kroků jste museli/budete muset jako firma podstoupit ke splnění všech povinností GDPR? *

- [ ] Revize obchodních podmínek
- [ ] Upravení smluvních podmínek se zpracovatelem dat
- [ ] Posouzení vlivu na ochranu osobních údajů
- [ ] Konzultace zpracování osobních údajů s dozorovým úřadem
- [ ] Zavedení záznamů o činnostech zpracování
- [ ] Zavedení šifrování či pseudonymizace osobních údajů
- [ ] Jmenování pověřence pro ochranu osobních údajů
- [ ] Jiné:

14. Kolik času Vaší firmě odhadem zabral/zabere celý proces přípravy na GDPR? *

Vyberte

15. Jak hodnotíte dostupnost informací o GDPR? *

	1	2	3	4	5	6	
Velmi špatná	○	○	○	○	○	○	Velmi dobrá

16. Jak hodnotíte srozumitelnost dostupných informací o GDPR? *

	1	2	3	4	5	6	
Zcela nesrozumitelné	○	○	○	○	○	○	Zcela srozumitelné

ZPĚT ODESLAT

Nikdy přes Formuláře Google neposílejte hesla.

*Povinné pole

11. Z jakých důvodů se Vaše firma doposud nezabývala přípravou na GDPR? *

- [ ] Nedostatek informací k problematice GDPR
- [ ] Nedostatečná srozumitelnost informací k problematice GDPR
- [ ] Časová vytíženost firmy
- [ ] Jiné: _____

12. Jak hodnotíte dostupnost informací o GDPR? *

	1	2	3	4	5	6	
Velmi špatná	○	○	○	○	○	○	Velmi dobrá

13. Jak hodnotíte srozumitelnost dostupných informací o GDPR? *

	1	2	3	4	5	6	
Zcela nesrozumitelné	○	○	○	○	○	○	Zcela srozumitelné

ZPĚT ODESLAT

Nikdy přes Formuláře Google neposílejte hesla.

Konec dotazníku

Prosím potvrďte dotazník kliknutím na tlačítko "odeslat". Děkuji Vám za vyplnění dotazníku.

ZPĚT ODESLAT

Nikdy přes Formuláře Google neposílejte hesla.

Abstrakt

JANDA, Tadeáš. *General Data Protection Regulation*. Plzeň, 2018. 57 s. Bakalářská práce. Západočeská univerzita v Plzni. Fakulta ekonomická.

Klíčová slova: připravenost firem v ČR na GDPR, ochrana osobních údajů, směrnice Evropského parlamentu, General Data Protection Regulation, analýza

Cílem této bakalářské práce je zjistit připravenost vybrané skupiny na implementaci směrnice General Data Protection Regulation. První část práce pojednává o pojmech, zásadách a právech spojených právě s touto směrnicí. Druhá část pojednává o ostatních zákonech spojených s ochranou osobních údajů v České republice. Následuje demonstrace výsledků dotazníkového šetření, kterého se účastnilo 95 respondentů a uvedení významných aspektů, které mohou usnadnit přípravy potřebné pro plnění povinností směrnice. Samotné výsledky dotazníkového šetření dokazují, že je přes 70 % firem nepřipravených na implementaci směrnice. Po zhodnocení vlivu směrnice na situaci v České republice však vidíme, že střední a velké podniky jsou z větší části připraveny. Mikro a malé podniky jsou připraveny méně, ale přípravná opatření budou pravděpodobně méně rozsáhlá než u podniků větších, tudíž jim příprava zabere méně času.

Abstract

JANDA, Tadeáš. *General Data Protection Regulation*. Plzeň, 2018. 57 p. Bachelor Thesis. University of West Bohemia. Faculty of Economics.

Key words: degree of readiness for GDPR, data privacy, regulation of the European Parliament, General Data Protection Regulation, analysis

The aim of this bachelor thesis is to analyse the readiness of a selected group to implement the General Data Protection Regulation. The first part of the thesis deals with the concepts, principles and rights related to this regulation. The second part is about other laws related to the protection of personal data in the Czech Republic. This is followed by a demonstration of a results of the questionnaire survey which filled out 95 respondents, and a presentation of significant aspects that can facilitate the preparations needed to fulfil the obligations of the regulation. The very results of the survey show that over 70 % of companies are not fully prepared to implement the regulation. However, after assessing the impact of the regulation on the situation in the Czech Republic, we can see that medium and large-sized companies are largely prepared. Micro and small-sized companies are less prepared, but preparatory measures are likely to be less extensive than for the large companies, which means the preparation of the smaller-sized companies should take less time.