Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Identifikace problémů při implementaci GDPR

Diplomová práce

Autor: Bc. Šárka Kaiserová
Studijní obor: Informační management

Vedoucí práce: doc. Ing. Vladimír, Bureš, Ph.D., MBA

Hradec Králové Únor 2020

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.02.2020 Bc. Šárka Kaiserová

Poděkování:

Ráda bych na tomto místě poděkovala svému vedoucím práce Doc. Ing. Vladimíru Burešovi, PhD., MBA, za jeho cenné rady a odbornou podporu při řešení problematiky. Poděkování patří všem lidem, kteří se podíleli na překladech dotazníků, ale také přátelům, kteří mi pomohli získat kontakty na vhodné respondenty. V neposlední řadě bych chtěla poděkovat respondentům, kteří zodpověděli dotazník, a mé rodině, která mě po dobu studia podporovala.

Anotace

Diplomová práce zkoumá oblast legislativy GDPR, která vstoupila v platnost 25. května 2018. Pomocí dotazníkového šetření mapuje situaci ve firmách v 8 zemích Evropské unie, kterých se zúčastnilo 307 respondentů. Cílem této práce je ověřit tři hypotézy: (1) GDPR je pro podnikatelské subjekty nesrozumitelné; (2) Většina oslovených podnikatelských subjektů se dopouští pochybení; (3) GDPR přineslo firmám uvědomění si hrozeb a rizik související se zpracováním dat. Diplomová práce přináší zajímavé údaje nejen o dodržování nové legislativy, ale také o vnímání GDPR samotnými respondenty.

Klíčová slova

GDPR * Dodržování GDPR * Řízení rizik * Obecná nařízení ochrana osobních údajů * Implementace * Kybernetické útoky * Ochrana dat * Osobní data

Annotation - Title: Identification of issues during the GDPR implementation

The master thesis investigates the area of the European Union´s General Data Protection Regulation (GDPR), which came into force on May 25, 2018. In the form of a questionnaire survey, it maps the situation in the enterprises in 8 countries of the European Union attended by 307 respondents. The main objective of this thesis is to verify three hypotheses: (1) GDPR is incomprehensible for business entities; (2) Most of the addressed companies do or did the mistakes in the GDPR area; (3) GDPR showed the companies of the threats and risks associated with data processing. The master thesis brings interesting data not only on compliance with the new legislation but also on the perception of GDPR by the respondents themselves.

Keywords

GDPR * GDPR Compliance * Risk Management * General Data Protections Regulations * Implementatiton * Cyber Attacks * Data Protection * Personal Data

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Kvantitativní a kvalitativní data označovaná také jako tvrdá a měkká data, jsou cenný artikl, jsou všudy přítomná a každou vteřinou jejich objem roste. Vznikají tak gigantické databáze, které jsou vlastněny státy, velkými korporacemi a organizacemi [Bologniny, 2017, s. 173]. Člověk už není jediným impulzem pro jejich vznik. Například rozvoj umělých neuronových sítí, jejichž vzorem byla právě lidská nervová soustava, přinesl novou možnost, jak získat nová data, nalézt nové propojení. Shromážděná data slouží pro analýzy nebo predikce a jsou tak důležitým nástrojem dnešní doby. Příkladem mohou být servery třetích stran, které sledují, shromažďují, analyzují chování uživatelů s cílem optimalizace webu či segmentaci spotřebitele a jejich raketový rozvoj [Sorensen, 2019 s. 3]. Data nemusí být pouze využívána jako zdroj informací, mohou být přetvářena na falešné zprávy a je velmi těžké, často až nemožné, odhalit pravdu [Cohen, 2019, s. 82]. Cílem může být klamání voliče či spotřebitele. Příležitosti, které data představují, musí být v rovnováze s ochranou těchto dat [Bologniny, 2017, s. 171]. Nutnost ochrany dat je celosvětově vnímána jako nejvyšší priorita. S růstem množství dat se zároveň zvyšuje pravděpodobnost pokusů o narušení kybernetické bezpečnosti, a to legálním i nelegálním způsobem. Kybernetické útoky mohou být rozděleny dle typu útoku nebo dle cíle útoku. Každoročně je veřejnost po celém světě informována příslušnými organizacemi o hrozbách kyberprostoru. V ČR upozorňuje na nové hrozby Národní centrum kybernetické bezpečnosti [NCKB]. Ročně prezentuje na svých webových stánkách desítku nových hrozeb, např. Meltdown (chyba v moderních procesorech) v lednu 2018, pishingové útoky na akademickou sféru v září 2018 nebo vyděračské e-maily v dubnu 2019 [NCKB].

Nutnost ochrany dat si uvědomují nejen právnické osoby, ale také již fyzické osoby. Právnické osoby podstupují cvičení, kdy probíhá simulace kybernetického útoku s cílem zvýšit odolnost společnosti a připravit ji na krizové situace [NÚKIB, a, 2019]. Fyzické osoby ještě v nedávné minulosti vkládali dobrovolně svá data na různé webové stránky, dnes již většina velmi obezřetně zvažuje poskytnutí svých osobních dat, neboť nebezpečí zneužití je příliš vysoké a tuto skutečnost si již uvědomuje snad

každý. Předání osobních údajů může být vědomé i nevědomé. V roce 2019 obletělo celý svět varování před technickými a programovými prostředky čínské společnosti HUAWEI, která byla spojena s potencionální špionáží a zneužitím osobních dat. V červnu roku 2019 varoval před touto hrozbou také Úřad pro kybernetickou a informační bezpečnost v ČR [NÚKIB, b, 2019].

Ochranu soukromí fyzických osob považují demokratické státy za jedno ze základních práv občana. V České republice je právo na ochranu soukromí zakotveno v ústavě jako *„právo na nedotknutelnost osoby a jejího soukromí“* (čl. 7, odst 1), *„právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života*“ (čl. 10 odst. 2), *„právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“* (čl. 10 odst. 3) [PSP, 2019].

V České republice platí ochrana osobních údajů od roku 1992 [ÚOOU, a, 2019]. A přesto právní rámec General Data Protection Regulation (dále jen GDPR), který se zrodil pod taktovkou Evropské unie (dále jen EU) pro ochranu osobních údajů fyzických subjektů na území států EU, byl v ČR v roce 2018 velkým zásahem do firemních procesů, ale také skvělou podnikatelskou příležitostí pro poradenské firmy, které využily neznalosti právnických osob a nejasností v české legislativě. Média i marketingové kampaně často šířily nepřesné nebo dokonce mylné informace [ÚOOU, a, 2019]. Podnikatelské subjekty se obávaly vysokých sankcí. Pokuty plynou z nedodržení ochrany osobních údajů a jsou stanoveny ve výši 20 mil. EUR nebo až 4 % ročního celkového příjmu [GDPR.eu, 2019]. Subjekty proto využívaly služeb poradenských firem, které často představovaly nemalé náklady. O rok později tato bublina splaskla a nasnadě je tedy otázka, jak se s GDPR vyrovnaly podnikatelské subjekty. Dokázaly správně implementovat GDPR v praxi?

2 Cíl práce

Cílem práce je zmapovat obecné povědomí o GDRP a jeho implementaci u vzorkovaných právnických subjektů v praxi. Nedílnou součástí je také identifikace pochybení, která jsou v rozporu s GDPR a kterých se oslovené právnické subjekty vědomě či nevědomě dopustily či stále ještě dopouštějí.

Cíl práce lze rozdělit do několika dílčích cílů:

- Definovat zkoumané oblasti zpracování dat;
- Vybrat země EU, ve kterých budou právnické subjekty osloveny;
- Zmapovat situaci u vzorkovaných právnických subjektů;
- Vyhodnotit zjištěné výsledky globálně, na úrovni zkoumaných zemí EU;
- Vyhodnotit zjištěné výsledky na úrovni vzorkovaných států;
- Detailněji analyzovat provázanost dat u odpovědí, kde bude patrná zajímavá nebo výrazná diferenciace dat;
- Analyzovat subjektivní pohled respondentů na přínosy GDPR;
- Navrhnout potřebné změny pro nejzávažnější a nejčastěji se vyskytující pochybení.

Na základě uvedených hlavních a dílčích cílů byly stanoveny tyto hypotézy:

- GDPR je pro podnikatelské subjekty nesrozumitelné;
- Většina oslovených podnikatelských subjektů se dopouští pochybení;
- GDPR přineslo firmám uvědomění si hrozeb a rizik související se zpracováním dat.

3 Metodika zpracování

Primárním zdrojem teoretických informací byly webové stránky:

- Úřadu pro ochranu osobních údajů ČR - https://www.uoou.cz/
- GDPR EU - https://gdpr.eu

Uvedené internetové zdroje představují nejen teoretický zdroj informací, ale prezentují také dotazy právnických subjektů a aktuality z oblasti GDPR. Zdroje lze beze sporu považovat za relevantní, neboť Úřad pro ochranu osobních údajů ČR *„je dozorovým úřadem, podle článku 52 GDPR nezávislým a podle § 50 zákona o zpracování osobních údajů ústředním správním úřadem. Podle § 54 odst. 2 zákona o zpracování osobních údajů zejména“* [ÚOOU, a, 2019] a GDPR EU je oficiální knihovnou zaštítěnou EU na platformě programu pro výzkum a inovace Horizont 2020, jejímž jedním z úkolů je pomoci právnickým subjektům být v souladu s GDPR. Dále byly využity odborné články z databází vědeckých příspěvků, v kterých je možné nalézt toto téma v relativně velkém rozsahu. Po prvotním prozkoumání aktuálnosti informací v článcích jednotlivých let byl výběr zúžen na období 2017 – 2019. Využity byly databáze:

- SCIENCE DIRECT
- WEB OF SCIENCE
- SPRINGER
- SAGE
- SCOPUS
- SAGE Journals

Hledání vhodných zdrojů je prezentováno diagramem PRISMA, který je uveden v příloze č. 1. Nejvíce odborných článků bylo nalezeno v databázi SCOPUS a SPRINGER. Hledanými pojmy, kromě hesla GDPR, byly: osobní údaje, anonymizace dat, identity data management, kybernetické útoky, biometrické údaje apod. Tyto zdroje byly doplněny informacemi z platné legislativy. Opomenut nebyl ani Národní úřad kybernetické bezpečnosti., který přinesl aktuální informace z oblasti kybernetických útoků. Naopak byly vyřazeny texty s omezeným přístupem, články

z oblasti psychologie, medicíny či detailní softwarové příručky a články zabývající se algoritmy. Pro prvotní prozkoumání bylo vybráno 471 článků, z kterých bylo použito 63 zdrojových souborů. Pro odstranění duplicit byl použit software Duplicate Cleaner, který, s poměrně velkou přesností, odhalil zdvojené texty. Software disponuje algoritmem, který umožňuje vyhledávání duplicit dle názvu, velikosti, podobného obsahu. Případné další duplicity a podobnost textu pomohl odhalit software Mendeley, který byl použit pro samotnou práci s odbornými texty. Software Mendeley plní funkcionalitu osobní elektronické knihovny, je volně přístupný, zpříjemňuje a velmi usnadňuje práci se zdroji v podobě komentování textů, osobních poznámek, citace, rychlého prohledávání. Pro citace nabízí software Mendeley nástroj „Mendeley Cite“, který je kompatibilní s aplikací Microsoft Office 365 a je otevřen paralelně s aplikací MS Word a plugin je automaticky vkládá do dokumentu [Mendeley, 2019]. Knihovna je dostupná také např. z mobilního telefonu, což umožňuje kontinuální práci nezávislou na PC.

3.1 Dotazníkové šetření

Pro praktickou část bylo zvoleno dotazníkové šetření založené na on-line platformě SURVIO a probíhalo 9 týdnů, v období od 20.11.2019 do 26.01.2020. Cílovou skupinou jsou právnické osoby, které působí ve vybraných zemích EU: Česká republika, Slovensko, Velká Británie, Francie, Bulharsko, Polsko, Španělsko, Německo. Otázky jsou pro všechny respondenty dotazníkového šetření stejné. Z důvodu jednoznačnosti, srozumitelnosti a překonání jazykových bariér byl dotazník přeložen do oficiálních jazyků používaných ve vybraných zemích:

- Angličtina – cílová země Velká Británie
- Francouzština – cílová země Francie
- Bulharština – cílová země Bulharsko
- Polština – cílová země Polsko
- Španělština – cílová země Španělsko
- Němčina – cílová země Německo

Dotazníky byly přeloženy osobami s jazykovými znalostmi na min. stupni C1. Primárním jazykem je český jazyk, který byl použit jako sedmá jazyková varianta

dotazníků pro šetření v České republice a na Slovensku. Ze zemí EU byly vybrány právě tyto země, protože autorka práce zná Čechy žijící v těchto zemích, kteří doporučili potencionální respondenty a zároveň pomohli doladit překlad či formulaci otázky a zachytit drobné nuance tak, aby se překlad maximálně přiblížil jazykovému vyjadřování respondentů, a byl tedy správně obsahově, ale také formálně.

U dotazníku byla zvolena anonymní elektronická forma, aby vzorkovaní neměli zábrany sdělovat informace o firmě, kde působí [Škaloudová, 2011]. Elektronická forma dotazníku je nejjednodušší a nejlevnější způsob, jak získat požadované odpovědi a, vzhledem k rozsahu zkoumané lokality, také jedinou schůdnou formou [Škaloudová, 2011]. Zároveň nabízí variabilitu zvoleného zařízení, prostřednictvím kterého může dotazovaný odpovídat. Respondenti byli kontaktováni výhradně elektronicky prostřednictvím e-mailu, kde byl uveden odkaz na dotazník. Někteří respondenti požadovali zaslání odkazu v rámci aplikace WhatsApp, proto byla využita jako další komunikační nástroj. Každému respondentovi byla zaslaná pouze příslušná jazyková verze. Pro výzkum nebyly použity sociální sítě, kde je šíření dotazníků nekontrolovatelné. Z důvodu přehledu, o počtu oslovených respondentů a počtu získaných zodpovězených dotazníků, byly dotazníky zasílány výhradně autorkou práce. Počet vzorkovaných by měl být minimálně 30 osob z každé země, aby nedošlo ke statistické chybě druhého druhu [Škaloudová, 2011]. Vzhledem k časové i finanční náročnosti zpracování jednotlivých dotazníků, bylo cílem dotazníkového šetření získat více respondentů. Výběr byl proveden náhodně, a tato skutečnost tak odráží reprezentativu každé země, a tedy celkově charakteristiku základního souboru [Škaloudová, 2011].

Převážná část otázek dotazníku je konstruována jako polytomické otázky s uzavřenou odpovědí a s možností vybrat jednu nebo více odpovědí, což je uvedeno v instrukcích každé otázky [Škaloudová, 2011]. Kromě kvalitativního vyjádření jsou použity i numerické škály, kdy je od respondenta požadována odpověď formou zařazení do adekvátní skupiny, dle stanovené stupnice, tedy kvantitativní forma odpovědi [Škaloudová, 2011]. Otevřené otázky byly z dotazníku úmyslně vynechány, neboť nestandardizované odpovědi je, z důvodu jazykových bariér,

obtížné správně vyhodnotit a byla by nezbytná participace překladatelů, která představuje výrazné prodloužení výzkumu. Z tohoto důvodu bylo použito pouze několik polouzavřených otázek, kdy je respondent vyzván k vyplnění zejména názvu používaného software, aplikace nebo poskytovatel služby, pokud nemůže zvolit jednu z nabízených variant. Konstrukce otázek je formulována jednoduše, jednoznačně a neutrálně s ohledem na možné jazykové bariéry a erudovanost tazatelů [Škaloudová, 2011]. Otázky jsou vytvořeny tak, aby jasně definovaly právnickou osobu, tedy její velikost, dle počtu zaměstnanců (mikro podnik, malý, střední a velký podnik), typ (státní podnik, soukromý podnik, příspěvková organizace), sektor (veřejná správa, zdravotnictví, školství, pojišťovnictví a finance, průmysl, stavebnictví, e-shop a je uvedena také možnost „jiné, uveďte“). Další otázky jsou zaměřeny na samotného respondenta a zjišťují, na jaké úrovni respondent pracuje (zaměstnanec, střední management a top management) a v jakém oddělení (HR oddělení, IT oddělení, účetní oddělení, logistika, marketing, vedení firmy a ostatní).

Další otázky se již zabývají samotnou problematikou GDPR a vycházejí z doporučení a často kladených otázek ze strany právnických osob ÚOOU a také z výsledků šetření z května 2019, které bylo realizováno na 716 malý firmách v rámci EU, a je prezentováno na webových stránkách GDPR.EU [GDPR.EU, 2019].

Dotazník obsahuje 40 otázek, aby bylo dosaženo přiměřené časové náročnosti a ochoty respondenta dokončit dotazník. Maximální doporučená časová náročnost pro zdravého dospělého jedince je 40–45 min, po této době přichází únava a nesoustředěnost [Škaloudová, 2011]. Časová náročnost dotazníku v pilotážním šetření ukázala, že vyplnění dotazníku probíhalo v rozmezí 10–15 min. Smyslem pilotáže bylo zejména zjištění a následně odstranění nedostatků dotazníku. Při pilotáži se odhalují nedostatky dotazníku a velký důraz je kladen na jednoznačnost a srozumitelnost [Škaloudová, 2011]. Pilotáž byla rozdělena do dvou základních fází. První fází bylo testování dotazníku v ČR, kdy bylo osloveno 10 osob z rozdílných pozic a odlišných oborů. Cílem bylo ověřit, že dotazník je srozumitelný nejen pro zaměstnance z IT oddělení, ale také pro zaměstnance účetního či personálního oddělení.

Na základě šetření, které probíhalo 1 týden, byl dotazník upraven. U dvou otázek byla změněna formulace otázky, u jedné otázky doplněna nová varianta odpovědi. Po uvedené korekci, byl dotazník zadán k překladu do všech jazykových mutací, který probíhal v horizontu několika týdnů, maximální délka překladu trvala 3 týdny. Následovala konzultace jednotlivých překladů s kontaktními osobami (Čechy žijících v příslušné zemi). Komunikace probíhala převážně telefonicky, což se ukázalo jako rychlý a efektivní způsob. Nejnáročnější a nejpracnější byl překlad do bulharštiny, kde specifikace jazyka vyžadovala často jinou formulaci otázky než u ostatních jazyků tak, aby jí rodilý Bulhar správně porozuměl. Samotná korekce bulharského dotazníku probíhala na straně kontaktní osoby v Bulharsku z důvodu používání azbuky, důvody oprav byly opět komunikovány telefonicky. U ostatních jazykových mutací probíhala korekce na straně autorky práce, na základě připomínek kontaktních osob. Po této korekci následovalo oslovení několika respondentů, v každé zemi bylo osloveno 3–5 respondentů. Pilotní testování prokázalo, že další úprava dotazníku již není nutná. Celková časová náročnost obou fází pilotáže byla 7 týdnů. Dotazník byl zaslán 2456 respondentům, e-mailovou formou bylo osloveno 2236 vzorkovaných, prostřednictvím aplikace WhatsApp 220 vzorkovaných.

Aby byl výsledek diplomové práce co možná nejvíce objektivní a prezentoval aktuální stav implementace GDPR u podnikatelských subjektů EU, je v neposlední řadě také úkolem dotazníkového šetření získat co největší množství vzorkovaných. Diplomová práce je založena na teoretických informacích podložených literární rešerší a prakticky ověřena empirickým výzkumem.

3.2 Statistické vyhodnocení dat

Pro statistické vyhodnocení dat byl využit analytický software TIBCO Data Science – SW STATISTICA (dále jen SW STATISTICA), a to trial verze. Používání software je po registraci zdarma po dobu 30 dnů, pro uživatele je jistě příjemné i to, že je v českém jazyce, ačkoliv se jedná o zahraniční software. Základní ovládání programu je intuitivní, ale součástí programu je odkaz na tutoriál na internetové serveru Youtube, kde je představena základní i mírně pokročilá funkcionalita software.

Dodavatel software uvádí, že program nabízí 17 tis. funkcí [Tibco Software, 2020]. Data pro analýzu lze snadno importovat do programu a následně je v něm i upravit. Samotné vyhodnocení dat může mít podobu tabulky statistických hodnot nebo podobu grafu. Výsledky lze ukládat jako jednotlivé sobory, nebo si výstupy sumarizovat do protokolu. Vše je přehledně uspořádané ve stromové struktuře, která je primárně stále zobrazena v levé části pracovní plochy. SW STATISTICA byl využit především pro statistické vyhodnocení dvou bloků otázek. První blok otázek byl zaměřen na to, zda respondenti správně označí všechny osobní údaje, které GDPR definuje jako osobní data. Druhý blok otázek vyhodnocuje, jak moc ovlivnilo GDPR samotného respondenta: z pohledu zvýšení administrativy, pocitu kontroly apod. Na druhém bloku byly aplikovány výpočty základních statistických parametrů. Dále byly, ze SW STATISTICA, generovány krabicové grafy a histogramy. Pro jednoduché vyhodnocení byla také využita aplikace MS Excel, která nabízí zajímavější vizualizaci koláčových grafů a snadnější práci s textovými hodnotami výzkumu, které naopak SW STATISTICA často nenačetl správně a odkazoval na klasickou kontingenční tabulku, která je také součástí SW STATISTICA.

Každá země vykazuje jiný počet respondentů, proto byla data trichotomických otázek a výběrových otázek převedena na procentuální vyjádření poměrem četnosti výskytu dat a počtem dotazníků dané země, nebo průměrnou známkou příslušné země, pokud se jednalo o škálové otázky.

Data v kapitole 6.1 byla uspořádána nejprve do přehledné tabulky hodnot jednotlivých otázek podle zemí. Výsledné hodnoty byly za každou otázku seřazeny sestupně, tedy od nejlepšího výsledku po nejhorší. V dalším kroku byl výsledek nahrazen pořadovým číslem, jednička značí nejlepší výsledek. Sejným hodnotám bylo uděleno totožné pořadové číslo, pokud tedy tři země dosáhly 100 %, všem třem zemím bylo uděleno číslo jedna. Následně bylo stanoveno průměrné pořadové číslo každé země, kde opět nejnižší průměrné číslo představovalo nejlepší výsledek, a země byly seřazeny od nejlepšího výsledku po nejhorší. Z důvodu přesnosti bylo použito zaokrouhlení na dvě desetinná místa.

4 Teoretická východiska práce

4.1 Literární rešerše

Ochrana osobních údajů prezentovaná často anglickou zkratkou GDPR znamená General Data Protection Regulation a představuje Obecné nařízení o ochraně osobních údajů v evropském prostoru, *„které od 25. 5. 2018 přesně stanovuje pravidla pro zpracování osobních údajů a práva subjektů údajů (subjektem údajů jsou fyzické osoby)"* [ÚOOU, a, 2019]. Nařízení nemá zajistit pouze ochranu pro subjekty údajů, snaží se také vybalancovat křehkou rovnováhu mezi ochranou údajů a jiný předpisy jako je např. právo hospodářské soutěže, ochrana spotřebitele či duševní vlastnictví [De Hert, 2017, s. 193]. V současné době se jedná o nejprogresivnější průlomový systém, který zavádí kontrolní mechanismy a regulace v tak velkém rozsahu [Digital Technologies, 2019 s. 1] a je považován za nejdůležitější novinku v rámci obecného nařízení EU o ochraně osobních údajů [De Hert, 2017, s. 193]. Nařízení se týká všech právnících osob, které podnikají na území EU, nebo nakládají s osobními daty fyzických osob EU bez ohledu na to, kde se sídlo firmy nachází [O'BRIEN, 2016, s. 81]. GDPR umožňuje členským státům jistou volnost v oblasti automatizovaného rozhodování, konkrétně v čl. 22 odst. 2 a čl. 22 odst. 3 jsou uvedena vhodná opatření pro automatizované rozhodování, která by měla být členskými státy aplikována [MALGIERI, 2019, s. 6]. V národních zákonech implementujících GDPR byly identifikovány 4 odlišné přístupy k automatizovanému rozhodování [MALGIERI, 2019, s. 6]:

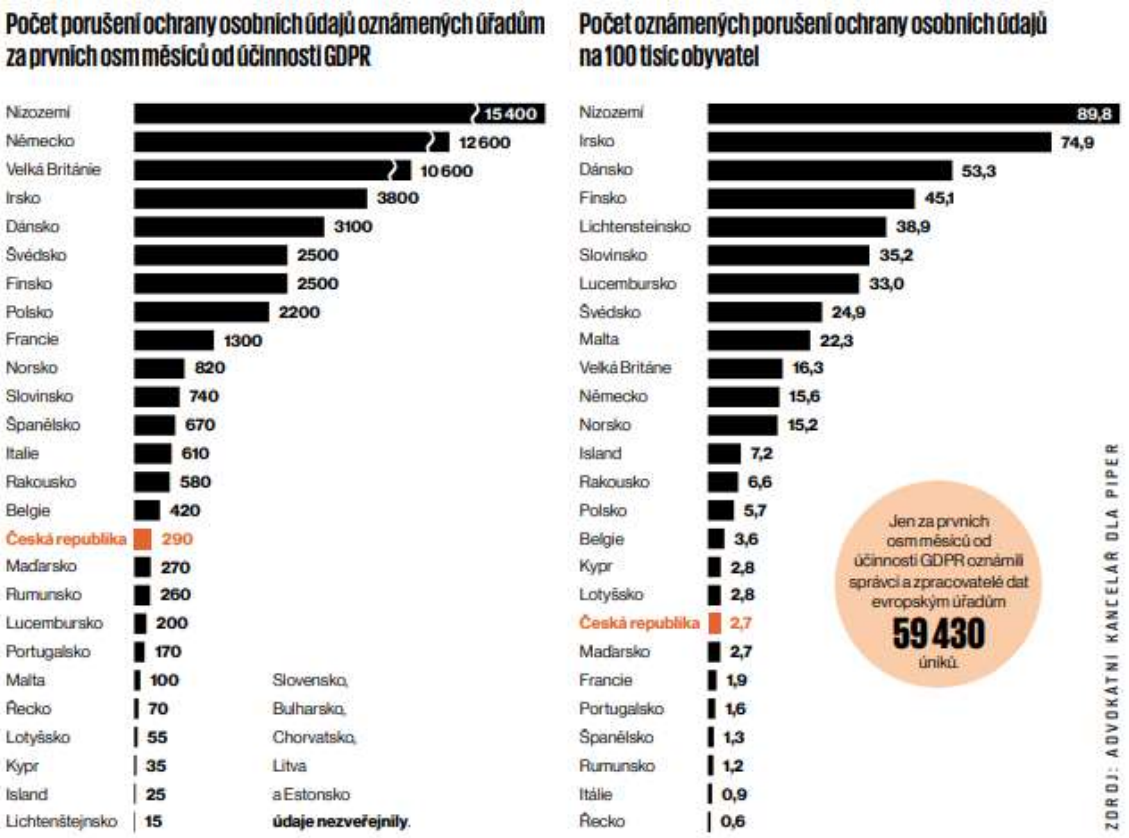
a) **Negativní přístup** – členský stát nepovoluje žádný konkrétní případ povoleného automatizovaného rozhodování a je aplikován většinou zemí (např. Itálie, Rumunsko, Švédsko, Dánsko, Polsko, Finsko, Kypr, Řecko, Česká republika, Estonsko, Litva);
b) **Neutrální přístup** – členský stát implementoval čl. 22, ovšem neuvedl žádné konkrétní opatření k ochraně práv a svobod a legitimních zájmů subjektů, o jejichž data se jedná (např. Německo, částečně Rakousko a Belgie);
c) **Procedurální přístup** – členský stát poskytuje záruky dle čl. 2, které jsou založeny zejména na konkrétních postupech, které mají správci údajů

provádět a dodržovat, např. oznámení o zkoumání dat (např. Irsko, Velká Británie, částečně Slovinsko);

d) **Proaktivní přístup** – členský stát navrhuje nové konkrétní záruky v souladu s čl. 2 (např. Francie, Maďarsko).

Pro českou legislativu znamenalo Obecné nařízení o ochraně osobních údajů nahrazení zákona 101/2000 Sb., o ochraně osobních údajů [ÚOOU, a, 2019]. Navzdory sankcím dokazují průzkumy, že společnosti nejsou v souladu s GDPR. Dle společnosti Forrester Research 80 % společností v Evropě a Severní Americe nebylo k 25. 5. 2018 v souladu s GDPR [Duncan 2018, s. 9]. V roce 2019 průzkum provedený EU upozornil na skutečnost, že více než polovina ze 716 oslovených malých firem, nedisponuje znalostmi o používání správných nástrojů a nedodržuje klíčová pravidla GDPR [GDPR.eu, b, 2019]. Společnost CISCO prezentovala v únoru 2019 výsledky průzkumu, který ukázal, že 59 % podniků splňuje požadavky GDPR, 29 % očekává zajištění během roku a 3 % nejsou schopny dostát GDPR požadavkům vůbec [Bičíková, 2019]. Jako nejpřipravenější země, se dle průzkumu CISCO, jeví Španělsko, naopak nejméně připravené země jsou: Japonsko, Rusko a Turecko [Bičíková, 2019]. K obdobným závěrům dospěla i společnost KPMG zabývající se poradenskou činností, která prezentovala na konferenci o GDPR výsledek průzkumu, který byl proveden na 52 českých významných společnostech a odhalila 76 prohřešků [ÚOOU, b, 2019, s. 12]. Mezi nejčastější detekované chyby patří chybně vymezený rozsah údajů, které firmy zpracovávají, chybějící definice účelu zpracování dat, ale také způsob získávání souhlasu od fyzických osob [ÚOOU, b, 2019, s. 12]. Dalším identifikovaným prohřeškem je sledování o návštěvnících webu a používání cookies. Firmy neupozorňují na používání cookies nebo nemají souhlas se zpracováním cookies [ÚOOU, b, 2019, s. 12]. Nejméně prohřešků bylo zjištěno u institucí typu: banky a pojišťovny, nejvíce naopak u sportovních organizací [ÚOOU, b, 2019, s. 12]. V prvních 8 měsících po zavedení GDPR bylo evropským úřadům nahlášeno celkem 59 430 případů porušení ochrany osobních údajů. Nejvíce případů, celkem 15 400 bylo nahlášeno v Nizozemí, nejméně naopak na Islandu a v Estonsku, pouze 25 případů [ÚOOU, b, 2019, s. 10]. Pořadí jednotlivých států je uvedeno na obrázku č. 1. Česká republika se umístila ve druhé polovině

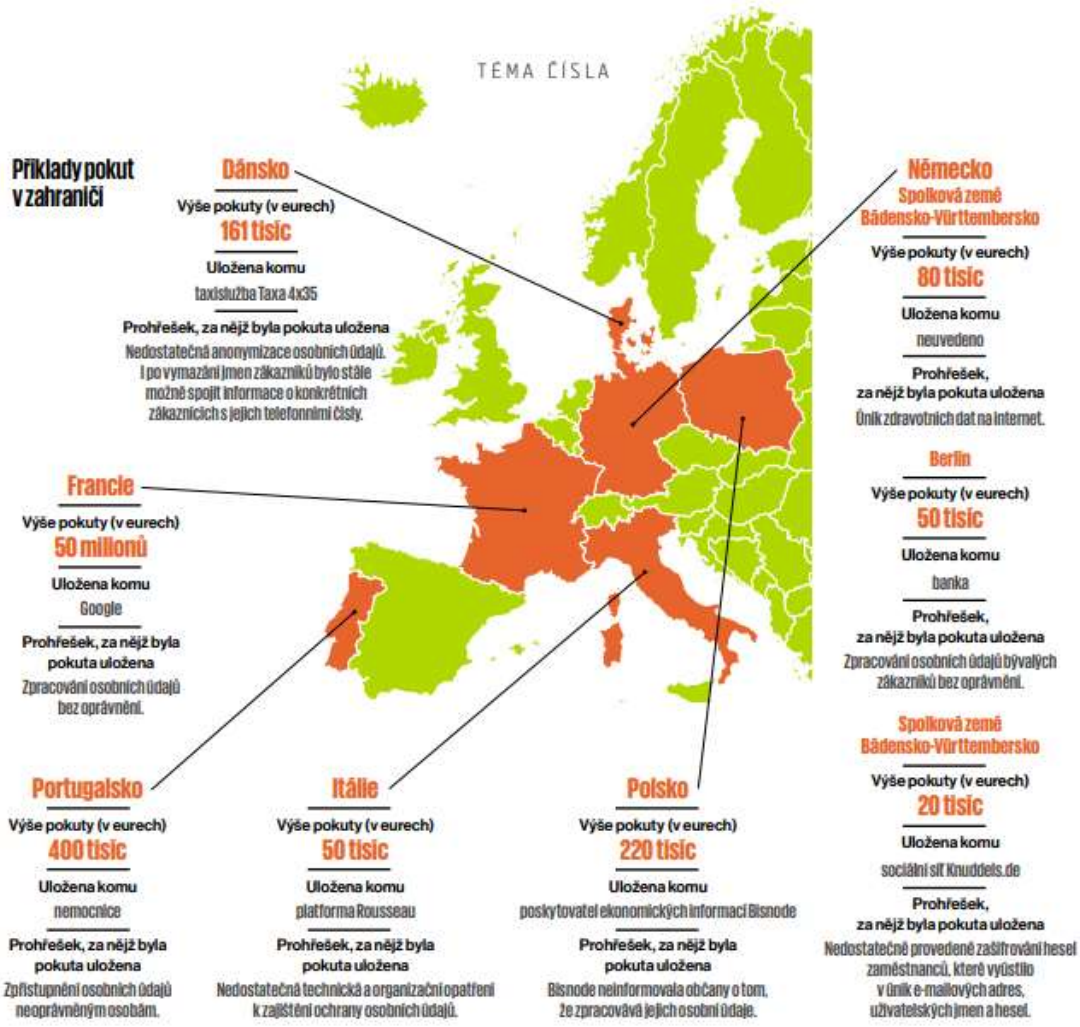
prezentovaného žebříčku s celkem 290 případy, tj. 2,7 případu na 100 tis. obyvatel [ÚOOU, b, 2019, s. 10].



Obrázek 1: Počet porušení ochrany osobních údajů
Zdroj: ÚOOU, 2019, s.10

EU prezentuje Nařízení Evropského parlamentu a Rady (EU) 2016/679 jako nejpřísnější zákon o ochraně osobních údajů na světě, za jehož porušení budou udělovány vysoké sankce [GDPR.eu, a, 2019]. Kontrolní úřady udělily již několik desítek pokut, jak ukazuje obrázek č. 2. Udělené sankce se pohybovaly v České republice od 5 tis. CZK do 250 tis. CZK [ÚOOU, b, 2019, s. 10]. Naopak v zahraničí jsou udělovány mnohonásobně vyšší pokuty. Doposud nejvyšší pokuta byla udělena společnosti Facebook 113 mld. CZK za porušení ochrany soukromí od Americké Federální komise pro obchod (FTC) [ČTK a iDNES, 2019]. Další rekordní pokuta byla udělena francouzským úřadem CNIL americké společnosti GOOGLE za špatné podávání informací uživatelům o tom, jak jsou používána jejich data, výše pokuty činila 50 mil. € [ÚOOU, b, 2019, s. 11]. V Portugalsku obdržela nemocnice ve městě

Barreiro pokutu 400 tis. € za poskytování údajů o pacientech neoprávněným osobám [ÚOOU, b, 2019, s. 11]. Dánské taxislužbě byla udělena pokuta 160 tis. € za to, že neprovedla anonymizaci nebo odstranění dat svých zákazníků [GDPR.eu, c, 2019].



Obrázek 2: Příklady pokut v zahraničí
Zdroj: ČTK a iDNES

Důležité je také na tomto místě zmínit „paradox soukromí“. Na jedné straně jsou právnické osoby nuceny provést opatření pro ochranu osobních údajů fyzických osob a zároveň tyto fyzické osoby dobrovolně sdílejí svá data a udělují bezhlavě souhlas, aniž by si podmínky řádně přečetly [Botta, 2019, s. 5]. Důvod je jednoduchý, neochota číst obsáhlé texty. Dle průzkumu Evropské komise z roku 2015 bylo zjištěno, že podmínky pročítá pouhých 18 %, 31 % je nečte vůbec a 49 % pouze

částečně [Botta, 2019, s. 6]. Bez ohledu na tuto skutečnost musí firmy dostát povinnostem plynoucím z nařízení o GDPR. Úprava či zavedení nových firemních procesů či audit stávajícího stavu, je pro firmy vždy palčivým úkolem, který vyžaduje čas, znalosti a finance. Pro firmy je základním stavebním kamenem vstupní audit, který ukáže, jaká data, jakým způsobem a v jakém rozsahu zpracovává (Brodin, 2019, s. 3). Do technologií a poradenských služeb investovaly malé podniky 1 000 – 50 000 EUR, a přesto si nejsou jisté, zda jsou v souladu s GDPR (GDPR.eu, b, 2019). Odhalit případné nedostatky může pomoci kontrolní seznam, který je k dispozici na webových stránkách GDPR.eu (GDPR.eu, c, 2019). Seznam je rozdělen do čtyř základních bloků, z nichž každý obsahuje několik dílčích konkrétních bodů, definující bližší parametry. **Základní bloky** [GDPR.eu, d, 2019]**:**

1) Dodržení zákonného rámce a transparentnosti;
2) Bezpečnost dat;
3) Odpovědnost a správa;
4) Právo na soukromí.

Zároveň jsou také doporučeny služby založené na end-to-end šifrování nebo jiné funkce zabezpečení ochrany osobních údajů, pro které je kolébkou vzniku často Švýcarsko, tedy neutrální území, mimo rámec EU [GDPR.eu, e, 2019]. Někteří poskytovatelé navíc nabízejí také speciální funkce pro splnění GDPR, jako je např. Matomo´s anonymizace [GDPR.eu, e, 2019]. Doporučení poskytovatelé pro jednotlivé služby jsou následující.

E-mailová komunikace

Doporučení poskytovatelé: **ProtonMail, Hushmail, Tutanota, Mailfance** [GDPR.eu, e, 2019]. Uvedené webmaily jsou označovány jako nejbezpečnějšími e-mailovými službami, používají end-to-end šifrování (dále jen E2EE). Poskytovatel e-mailové služby **ProtonMail** sídlí ve Švýcarsku, používá HTTPS spojení a automatické šifrování OpenPGP [ProtonMail]. Služba **Hushmail** byla uvedena do provozu v roce 1999 jako jedna z prvních šifrovaných služeb [Hushmail, 1999]. E-mailová služba **Tutanota** je známá především tím, že je plně otevřeným zdrojem s aplikacemi pro iPhone a Android, používá šifrování 2FA, zemí původu je Německo

[Tutanota]. V roce 2017 vydali na svých stránkách výzvu pro opuštění Google [Tutanota]. Služba **Mailfance** používá E2EE, servery této společnosti jsou uloženy v Belgii. Používány jsou standardy Sender Polici Framework (SPF) a Domain Keys Identified Mail (DKIM), umožňuje serveru odesílatele zahrnout do zprávy digitální podpis, který může přijímající server ověřit [Maifence.com, 2019].

VPN

Doporučení poskytovatelé: **ProtonVPN, AirVPN** [GDPR.eu, e, 2019]. Poskytovatel služby **ProtonVPN** sídlí ve Švýcarsku, podporován je pouze protokol OpenVPN, výměna klíčů probíhá přes 2048 bitové RSA a šifrovaná jsou přes AES-256, ověření integrity probíhá přes HMAC-SHA256 [ProtonVPN, 2019]. Služba **AirVPN** má své kořeny v Itálii, podporuje pouze protokol OpenVPN, nemá specializované aplikace pro iOS nebo Android [AirVPN].

Analýzy

Doporučení poskytovatelé: **Open Web Analytics, Matomo** [GDPR.eu, e, 2019]. **Open Web Analytics** slouží pro analýzu používání webových stránek, je založen na Javascriptu PHP nebo REST, s podporou obsahu jako je WordPress [Matomo, 2019]. Software **Matomo** se prezentuje jako přesnější nástroj, než je Google Analytics [Matomo, 2019].

Předávání zpráv

Doporučení poskytovatelé: **Signal, WhatsApp, Threema** [GDPR.eu, e, 2019]. Aplikace Signal je považovaná za nejbezpečnější aplikaci pro zasílání zpráv. Komunikace mezi koncovými uživateli je šifrovaná a podporuje aplikace pro iOS, Android a Desktop [GDPR.eu, e, 2019]. Aplikace **WhatsApp** byla irským úřadem deklarována jako dostatečně bezpečným nástrojem po zasílání zpráv, který je v souladu s GDPR [GDPR.eu, e, 2019]. Aplikace **Threema** je z uvedených třech služeb jedinou, která pro založení účtu nevyžaduje telefonní číslo [Threema, 2019]. Opět se jedná o služby zaštítěnou švýcarskými zákony [GDPR.eu, e, 2019].

Cloudová uložiště

Doporučení poskytovatelé: **Tresorit, Sync.com, Boxcryptor** [GDPR.eu, e, 2019]. Poskytované služby a zabezpečení jsou velmi obdobná, u cloudu **Tresorit** lze vyzdvihnout, že je používán více než 10 tis. organizacemi a umožňuje nastavení omezení přístupu s datem expirace platnosti přístupu [GDPR.eu, e, 2019]

Nástroj pro teamovou spolupráci

Doporučení poskytovatelé: **Wire** [GDPR.eu, e, 2019]. I tento nástroj je z produkce švýcarské firmy a nabízí široké spektrum služeb od chatů, videokonferencí až po sdílení souborů [GDPR.eu, e, 2019]. Vše je zabezpečeno E2EE.

Nástroj pro tvorbu poznámek

Doporučení poskytovatelé: **Standard Notes, Joplin** [GDPR.eu, e, 2019]. Bezplatná aplikace pro vytváření úkolů a poznámek ve formátu Markdown [Joplin, 2019]. Poznámky lze synchronizovat s různými cloudovými službami včetně Nextcloud, Dropbox, OneDrive, WebDAV a pracuje na platformě Windows, Linux, MacOS, Android, OS [Joplin, 2019].

Ačkoliv je regulační nařízení rozepsáno v 81 článcích na 100 stranách [PSP, 2019] a státní úřady podporují správnou aplikaci GDPR příklady z praxe, vzorovými dokumenty a návody [ÚOOU, a, 2019] jeho výklad je pro firmy stále nesrozumitelný [Brodin, 2019, s. 8].

4.2 Důležité pojmy GDPR

Podstatou GDPR je možnost fyzické osoby samostatně se rozhodnout, komu a za jakým účelem poskytnout svá osobní data. Funkce souhlasu lze vyjádřit slovy: *„svobodně dána a informována“* [Botta, 2019, s. 4], ale také má *„právo být zapomenut“* [Burri a Schär., 2016, s. 490]. Tohoto práva fyzické osoby příliš nevyužívají, např. dle vyjádření společnosti Coca-Cola mají ve své databázi statisíce klientů a doposud požádali o vymazání dat pouze 4 klienti [ÚOOU, b, 2019, s. 14]. Na druhé misce vah je právnická osoba, neboli subjekt, na který GDPR klade odpovědnost související s ochranou, zpracováním a již zmíněným výmazem (skartováním) osobních údajů.

Aktéry v GDPR jsou **fyzické osoby**, tj. právní pojem definující člověka z masa a kostí, označované též jako subjekt údajů a **právnické osoby** neboli subjekty, které zpracovávají údaje fyzických osob. Subjekty jsou též nazývány správci osobních údajů, které mohou pověřit zpracováním údajů třetí osobu, tzv. **zpracovatele osobních údajů**. **Osobním údajem** se pak rozumí informace o fyzické osobě, která ji jednoznačně identifikuje [ÚOOU, a, 2019]. Osobním údajem mohou být nejen data typu: datum narození, bydliště, rodné číslo, ale také biometrický údaj (otisk prstu, otisk krevního řečiště), videozáznam, fotografie. Zvláštní skupinu tvoří tzv. zvlášť citlivé údaje, kam se řadí náboženské vyznání, sexuální orientace a zdravotní stav. **Zpracování osobních dat** představuje operaci, nebo soubor operací s daty (třídění, ukládání, tisk, výmaz, šíření), ale také zničení dat [ÚOOU, a, 2019]. Zpracování osobních dat může provádět správce, nebo může správce požádat jiný subjekt o zpracování údajů, tzv. **zpracovatele**. Zpracování údajů mezi správcem a zpracovatelem musí být podloženo písemnou smlouvou, dle článku 28 odst. 3 Obecného nařízení, ve které bude definován předmět, doba trvání zpracování, povaha a účel zpracování, typ zpracovávaných osobních údajů, kategorie subjektů údajů, povinnosti a práva správce, okolnosti zpracování [ÚOOU, a, 2019]. Všechny veřejné subjekty a orgány veřejné moci mají povinnost zřídit pozici pověřence. Hlavním úkolem **pověřence** je poskytování informací, poradenská činnost, monitoring činností, zpracování záznamů o činnostech zpracování a spolupráce s ÚOOU [ÚOOU, a, 2019].

4.3 Zásady a právní důvody zpracování

Zásady a právní důvody zpracování jsou definovány takto [ÚOOU, a, 2019]:

- *„Zákonnost, korektnost, transparentnost – správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně a korektně“;*
- *„Omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely“;*
- *„Minimalizace údajů – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány“;*
- *„Přesnost – osobní údaje musí být přesné“;*

- *„Omezení uložení – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány";*
- *„Integrita a důvěrnost – technické a organizační zabezpečení osobních údajů".*

Důležité je zde zdůraznit, že obecné nařízení nedoléhá na fyzické osoby využívající data výhradně pro osobní a domácí činnost, např. tvorba rodinného rodokmenu [ÚOOU, a, 2019]. Dále se netýkají orgánů zajišťující stíhání či odhalování trestních činů, nebo veřejnou ochranu či bezpečnost [ÚOOU, a, 2019].

Firmy s více než 250 zaměstnanci mají povinnost vést **záznam o činnostech zpracování**, které popisují obecné záznamy o zpracování dat a prokazují, že je firma v souladu s GDPR. V záznamech o činnostech je přesně definován: účel zpracování (proč data subjekt zpracovává), popis kategorií subjektů (čí data subjekt zpracovává – dodavatelé, odběratelé apod.), popis kategorií osobních údajů (jméno a příjmení, bydliště, e-mail apod.), lhůty pro výmaz, informace o předání třetím stranám a technická a organizační opatření pro ochranu dat [ÚOOU, a, 2019]. Skutečnost, že je firma v souladu s GDPR, dokládá také pověřenec pro ochranu osobních údajů, kodexy či osvědčení. **Osvědčení o souladu zpracování** může vydat pouze Český institut pro akreditaci prověřeným subjektům a dokládá, že subjekt zpracovává data v souladu s GDPR [ÚOOU, a, 2019]. **Kodexy** představují pokyny pro daný sektor, např. bankovnictví, zdravotnictví, je vypracováván zástupcem daného sektoru a musí být schválen ÚOOU, který po jeho prostudování dokument připomínkuje a vyzve k odstranění nedostatků, v opačném případě dokument schválí a kodex je platným vodítkem v oblasti zpracování dat pro všechny subjekty sektoru [ÚOOU, a, 2019]. V některých případech je správce povinen provést **posouzení vlivu na ochranu osobních údajů** [ÚOOU, a, 2019]. Vyžadováno je především [ÚOOU, a, 2019]:

- *„U systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky;*

- *U rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech;*
- *U rozsáhlého systematického monitorování veřejně přístupných prostorů.“*

Naopak byla zrušena **oznamovací povinnost** o zamýšleném zpracováním dat [ÚOOU, a, 2019].

4.4 Zabezpečení dat

Data lze rozdělit do dvou základních kategorií: **tištěná data** a **elektronická data. Tištěná data** jsou obvykle ukládána do šanonů či archivačních boxů a následně do archivu, spisovny, skříně či šuplíku. **Elektronická data** mohou být uložena takřka kdekoliv: na serverech, cloudových uložištích, v notebooku, mobilních telefonech atd. Ať už mají data tištěnou či elektronickou podobu, musí být chráněna tak, aby byl přístup umožněn pouze oprávněným osobám a jejich manipulace s daty byla pod kontrolou. Firmy mají často ve svých směrnicích tzv. proces **politiky čistého stolu**. Tato metodika ukládá zaměstnanci povinnost, uklidit všechny citlivé a důvěrné dokumenty (tištěné i elektronické) na stanovené bezpečné místo před opuštěním svého pracovního místa na delší dobu. Toto pravidlo se vztahuje také na **tisk a skartaci** dokumentů. Dokumenty se musí bez prodlení odebrat z tiskárny, navíc bývá samotný tisk chráněn heslem. **Důvěrné a citlivé dokumenty** nemohou být pouze vhozeny do koše či roztrhány, ale musí být řádně skartovány. Dodržování procesu „politiky čistého stolu“ je kontrolováno, a v případě zjištění prohřešku proti tomuto pravidlu, může být se zaměstnancem zahájeno disciplinární řízení. Zatímco tištěná data zabezpečí klíč, kterým může být i biometrický údaj (otisk prstu, sítnice, krevního řečiště apod.), zajištění elektronických dat vyžaduje sofistikovanější nástroj. U zmíněných biometrických data je navíc velmi důležité, aby tyto údaje jednotlivce nebyly vzájemně propojitelné napříč různými provozovateli biometrických služeb [NAUTSCH, s. 58, 2019].

4.4.1 Identity Data Management (IDM)

IDM je metoda, která se používá pro jednoznačnou identifikaci uživatele [Alsayed, 2019]. IDM přestavuje bezpečnostní prvek a zároveň technologické řešení, které

umožní firmám automatizovat, centralizovat a zabezpečit správu přístupů a práv v IT systémech, proto se IDM stal v poslední dekádě nejdůležitější výzvou pro každou organizaci [Kunz, et. al, 2019]. Maximalizovat bezpečnost a minimalizovat únik citlivých a důležitých údajů je důležitý úkol každé organizaci a je na něj kladen velký důraz. Bez IDM si nelze představit ani cloudové prostředí, kterého využívá stále větší množství firem z důvodu rentability a flexibility, a i zde je požadované a bezesporu nutné mít řízení přístupů pod kontrolou [Kunz, et. al, 2019]. Základní mechanismus IDM je **RBAC** = Role-Based Access Control, který představuje kontrolu uživatelů a jejich přístupů. Tento mechanismus zajišťuje uživateli získání role, tj. konkrétního oprávnění v systému, např. založení e-mailového účtu, přístup do ERP systému. Složitost a počet úkolů, které IDM musí řešit v moderních společnostech, neustále roste, což vede ke zdokonalování stávajících nástrojů. Nástupce RBAC je ABAC a nabízí dostatečnou flexibilitu k překonání několika problémů s řízením přístupu [Kunz, et.al, 2019]. Díky variabilitě nastavení může IDM spravovat všechny účty, kterými organizace disponuje:

- **Zaměstnanci** – identita začíná nástupem zaměstnance do organizace, a naopak končí ukončením pracovního poměru;
- **Externisti** – mezi externisty patří např. zákazníci, dodavatelé, využívají přístup prostřednictvím VPN, často používají certifikáty;
- **Technické a servisní účty** – administrátorské účty, účty aplikací, obvykle nezanikají po odchodu vlastníka účtu.

Zajištění bezpečnosti je tím složitější, čím větší je organizace a roztříštěnost systému. Aspekt bezpečnosti je zohledněn již vývojáři, např. v algebraickém modelu, který umožňuje kombinovat politiku bezpečnosti a analyzovat jejich vliv na předem definované omezení [Khair, et.al., 2016]. V literárních zdrojích je k dispozici několik metod pro analýzu a řízení přístupu [Khair, et.al., 2016]. Princip a funkčnost algebraického modelu byla popsaná např. K.E.Sabri a H.Hiary v *článku „Algebraický model manuální kontroly bezpečnosti“* [Khair et.al. 2016]. Nutno podotknout, že omezujícím nástrojem IDM jsou náklady. Proto tento nástroj používají zejména velké a střední firmy. Důvodem je nejen velké množství uživatelů a informačních

systémů, ale také nutnost častých změn. IDM využívá např. ČEZ, Equa bank, Česká televize, Česká pošta [AMI, 2014].

4.4.2 Šifrování

Kryptografie veřejných klíčů je používána více než 40 let [Jasobson, 2015, s. 25]. **Šifrování end-to-end** (dále E2EE) představuje zabezpečení komunikace, které zajistí zamezení přístupu k datům během jejich přenosu třetí straně. Data jsou šifrována u svého zdroje, následně bezpečně, spolehlivě a bez jakéhokoliv úsilí přenesena adresátovi. Zprávu nelze dešifrovat dříve, než dosáhne svého cíle. Přenášená data nelze číst nebo s nimi manipulovat, přístup není umožněn ani poskytovateli internetových či aplikačních služeb. E2EE používá např. tyto aplikace a služby: WhatsApp, NextCloud, Wire, ProtonMail, MS Microsoft Outlook. **Nejčastěji je šifrování používáno pro** [Jacobson, 2015, s.26]**:**

- Elektronickou poštu (e-mail);
- Okamžité zprávy (IM);
- Výměna souborů;
- Voice over IP (VoIP).

Ačkoliv je šifrování bezesporu účinný nástroj pro ochranu dat, z pohledu GDPR není šifrování povinné, a dokonce není určen standard či typ osobních údajů, které mají být šifrováním chráněny. Šifrování je tak pouze bezpečnostním prvkem, *„který i v některých případech může správci zlepšit jeho postavení v případě úniků těchto údajů, jelikož v takovém případě se na něj nemusí (v závislosti na případu, neznamená to, že pokaždé) vztahovat povinnost ohlašovat případ porušení zabezpečení osobních údajů dozorovému úřadu, resp. jej oznamovat subjektu údajů. Vždy je však nutné míru rizika posoudit, a to i v případě, že byla použita pseudonymizace či dostatečně silné šifrování a zdali nedošlo i ke kompromitaci šifrovacího klíče. Pseudonymizaci či šifrování osobních údajů je nutné použít pouze v odůvodněných případech, kdy tyto prostředky mají opodstatnění (viz článek 32 obecného nařízení)“* [ÚOOU, a, 2019].

4.4.3 Anonymizace a pseudoanonymizace

Anonymizace a pseudoanonymizace slouží k odstranění/skrytí identity fyzické osoby [Bologniny, 2017, s. 171]. Ovšem díky Big Datům, je stále častější otázkou, zda je anonymizace a pseudoanonymizace skutečně reálná nebo se již jedná pouze o snahu ochránit získaná data. Pojem **Big Data** je často chybně vnímán zejména jako „velký soubor“, ve skutečnosti ovšem není klíčovou vlastností jeho velikost, ale schopnost prohledávat a integrovat velké soubory dat a hledat souvislosti, predikovat chování a aktivity [Andrew, 2019, s. 2]. Big Data jsou tvořena třemi hlavními zdroji [Andrew, 2019, s. 2]:

- **Ekonomické transakce** (smlouvy, registrace u institucí, úmrtí, manželství);
- **Webové stránky** (elektronické obchodování, sociální média);
- **Fyzický pohyb lidí** – shromažďování informací pomocí kamer, satelitů.

Big data mohou být používána k ovládání jednotlivce i trhu [Andrew, 2019, s. 3]. **Anonymizace osobních údajů** představuje proces odstranění takových údajů, které umožní, ať už přímo, nebo nepřímo, identifkovat danou osobu. Jedná se o nevratný proces, což znamená, že osobu nelze zpětně identifikovat. Anonymizace osobních údajů osvobozuje zpracovatele od přísných GDPR opatření, s daty může volněji nakládat [ÚOOU, 2019] Pro zajištění anonymity dat je nutné, aby správce pravidelně přehodnocoval vrstvy anonymizace dat a používaných scénářů [Bologniny, 2017, s. 176]. Anonymizace osobních údajů se používá v případě, kdy dochází k velkému zpracování dat a osobní údaje osoby nejsou pro výzkum a zpracování dat klíčové [Heurix, 2017, s. 1].

Pseudoanonymizace osobních údajů nepatří do katergorie anonymizace dat [Bologniny, 2017, s. 177]. Pseudoanonymizace je pouze bezpečnostní opatření, které zabraňuje přímému propojení mezi datovým souborem a identitou daného subjektu [Bologniny, 2017, s. 177], např. jména a adresy jsou uloženy odděleně. Při sběru a práci s daty tak není jasná identifikace. Pseudoanonymizace je vratný proces. Na základě klíče lze data zpětně spojit a identifikovat osobu. Proto je nezbytné eliminovat možnost vnějších útoků a provést řadu preventivních opatření [Bologniny, 2017, s. 173]. Jedním z nich je ukládat klíče odděleně od dat, což

znemožní zpětnou identifikaci [Bologniny, 2017, s. 173]. Je to poprvé kdy evropské normy definovaly pojem „pseudoanonymizace“ a to právě v GDPR [Bologniny, 2017, s. 174]. Pseudoanonymizace osobních údajů se používá např. při použití údajů v lékařských výzkumech o pacientech.

4.4.4 Firewall

Firewall zajišťuje zabezpečení počítačové sítě více než 25 let, a to v podobě hardwareové i softwareové [H-Square, 2019]. Instalace zvýší zabezpečení síťové infrastruktury a zároveň je primárním vstupem, přes který probíhá všechna komunikace. Na základě nastavených bezpečnostních pravidel a politik, které monitoruje síťový provoz a umožní komunikaci pouze důvěryhodným sítím. Pro nedůvěryhodné zdroje je naopak bariérou. Firewally se vyvíjely jako reflexe na rostoucí hrozby. Od jednoduchého filtrování paketů a stavové kontroly jsou novodobé firewally schopny kontrolovat a filtrovat informace napříč všemi vrstvami a včas identifikovat útoky, které se snaží firewall obejít např. zneužitím protokolu (CISCO). Firewall nové generace označovaný NGFW od společnosti Palo Alto Networks se vyznačuje několika unikátními vlastnostmi [H-Square, 2019]:

- *„**Klasifikace provozu na základě identifikace aplikace** nikoliv portu, na kterém je provozována“;*
- ***„Identifikace uživatele jménem**, nikoliv jen IP adresou“;*
- ***„Blokování hrozeb v reálném čase“;***
- ***„Identifikace, řízení a nahlížení** (dekrypce) do šifrovaného provozu a aplikací (SSL a SSH)“;*
- ***„Technologie Single-Pass Architecture** pro souběžné zpracování více paralelních úloh kombinovaná s multi-gigabitovou propustností“;*
- ***„Virtualizace** umožňuje v rámci jednoho fyzického boxu provozovat více virtuálních firewallů. Každý virtuální systém je plně funkčním firewallem se samostatnou správou“;*
- *„Palo Alto Networks Next-Generation Firewally nabízejí jedinečný přehled a kontrolu aplikací, uživatelů a obsahu pomocí tří patentovaných identifikačních technologií: **App-ID**, **User-ID** a **Content-ID**, což zajišťuje*

bezpečné používání aplikací, a zároveň výrazně snížení celkových nákladů na bezpečnost“.

Firewall je běžně používaný ochranný prvek, jehož cena se odvíjí od kvality firewallu či souvisejících služeb, které poskytovatel nabízí.

4.4.5 Zálohování a archivace dat

Zálohování i archivace dat by měla být procesní součástí každé firmy. **Zálohování dat** představuje pojistku pro případ ztráty, poškození, odcizení dat, provádí se dle pevného časového harmonogramu, obvykle částečné zálohy na denní bázi a minimálně jednou měsíčně plné zálohy.

Archivace dat znamená odložení dat, která nejsou potřebná, např. archivace faktur předchozích období. Zálohují a archivují se nejen konkrétní data, ale také celé programy, a tak není jednoduché mít k dispozici dostatečný prostor. Data se mohou zálohovat na přenosná média, zálohovací server, ale stále oblíbenějším se stávají datová uložiště a zálohování je outsourcováno. Poskytovatelé, kromě klasického backup (zálohování), nabízejí svým zákazníkům využívajícím cloud zálohování formou snapshot, tedy aktuální kopií celého systému k určitému datu. Při výběru dat je nejdůležitějším prvkem **rychlost obnovy dat**, tedy stav 1:1, kdy zákazník může začít opět normálně fungovat. Zálohování dat, stejně tak jako aktualizace operačního systému a aplikačních programů může být obtížná u zaměstnanců, kteří se pravidelně nepřipojují do vnitropodnikové sítě. Příkladem mohou být obchodní zástupci.

Aktualizace operačních systémů a aplikačních programů je vyžadovaná z důvodu nové funkcionality, odstranění chyb, zajištění vyšší kybernetické bezpečnosti. Aktualizace je obvykle nastavená automaticky, ale protože vyžaduje uzavření programů, restart počítače apod. uživatelé ji, bohužel, opakovaně odmítají, ačkoliv je pro ně důležitá, obzvlášť u antivirových programů. Jak bylo výše uvedeno, technologických nástrojů pro ochranu dat je, bez ohledu na GDPR, několik a dávají firmám do rukou účinné zbraně, jak svá data chránit a firmy je používaly před

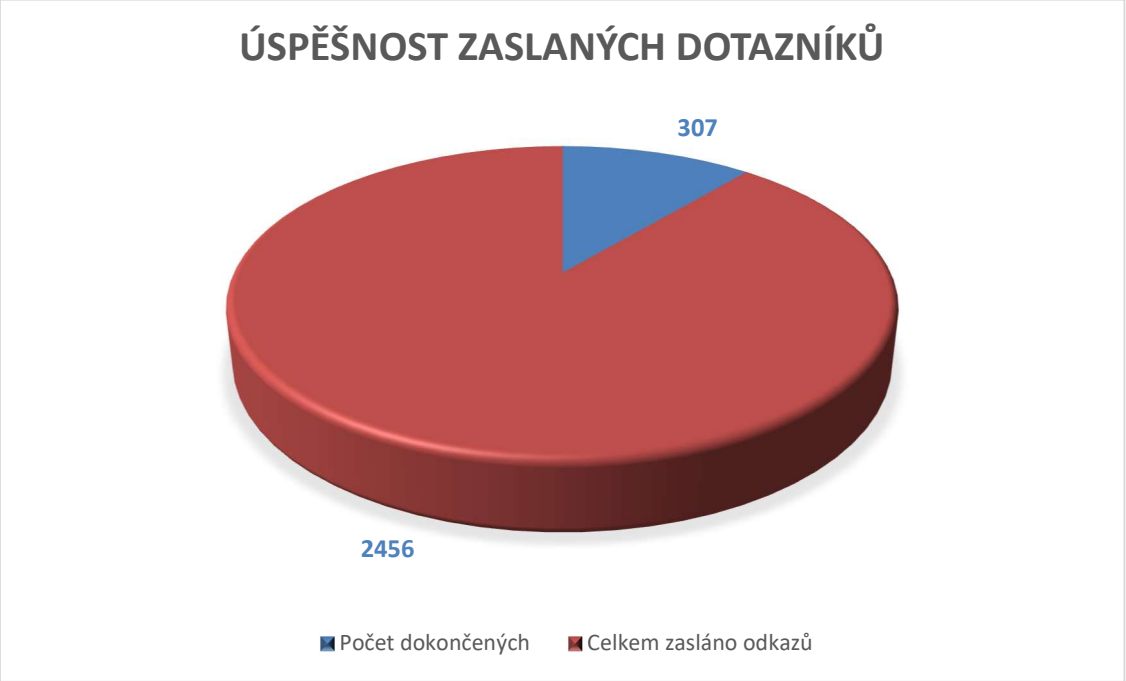
vznikem GDPR. Pojďme si tedy na závěr znovu připomenout, co se očekávalo od GDPR [Burri a Schär, 2016, s. 490]:

1) ***„Silnější ochrana poskytovaná uživatelům a jejich údajům;***
2) ***Zvýšené odpovědnosti subjektů kontrolujících a zpracovávajících údaje;***
3) ***Pevnější pochopení nařízení z hlediska jeho územního dosahu“***.

5 Praktická část

5.1 Dotazníkové řešení

V dotazníkovém šetření bylo dosaženo úspěšnosti 13 %. Z 2456 oslovených dokončilo dotazník celkem 307 respondentů, jak graficky znázorňuje obrázek č. 3.

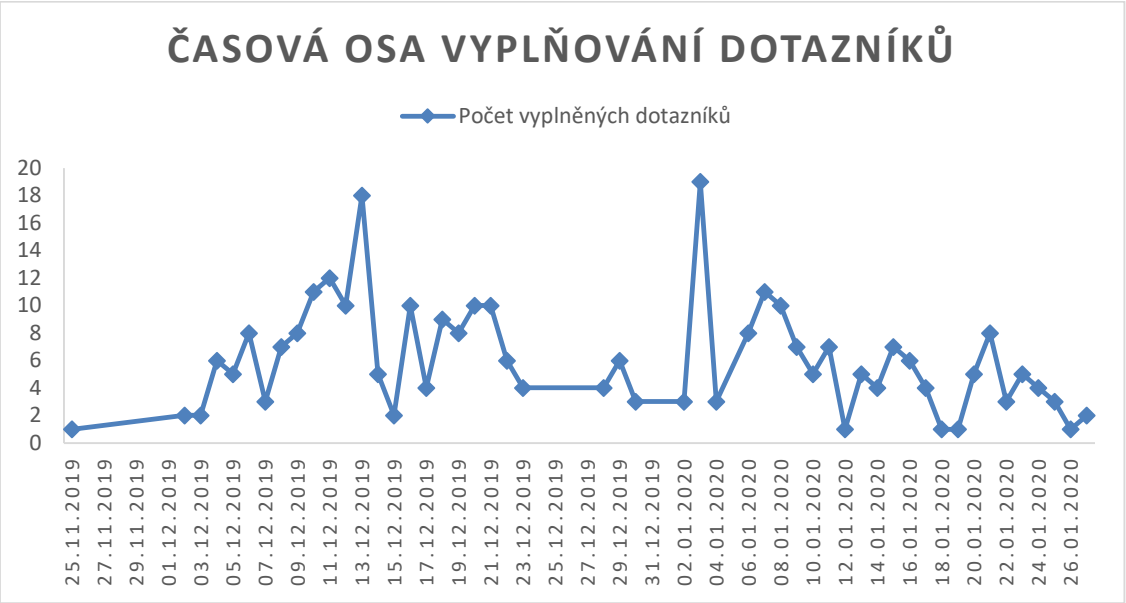


Obrázek 3: Úspěšnost zaslaných dotazníků

Zdroj: Vlastní zpracování

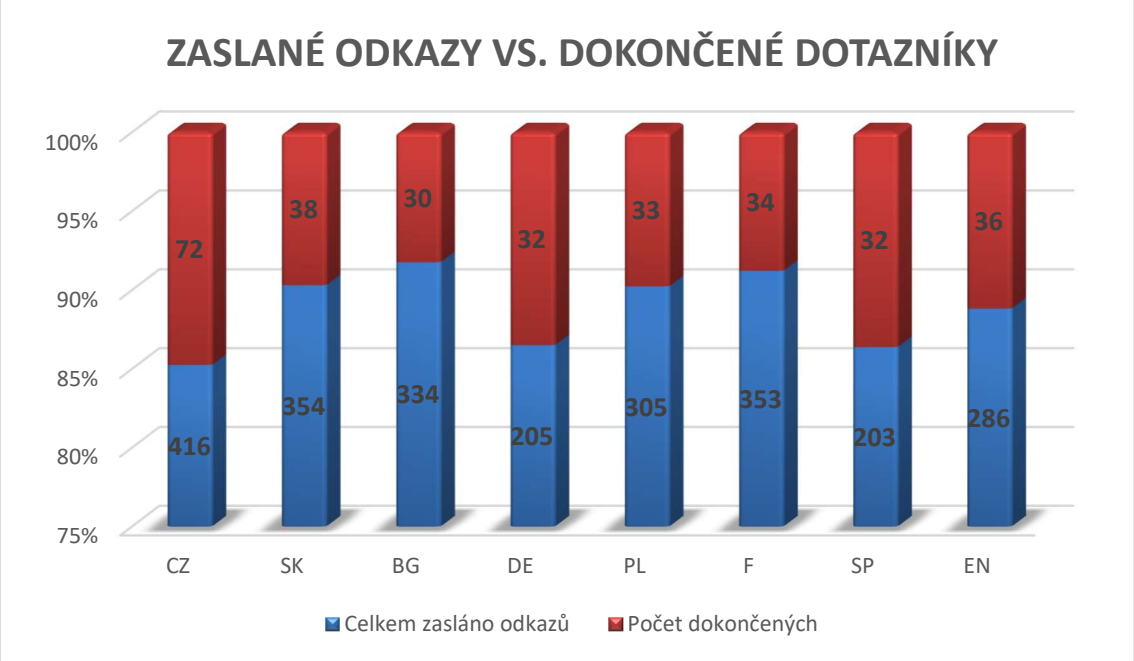
Časová osa na obrázku č. 4 prezentuje vyplňování dotazníků v jednotlivých dnech. V období vánočních svátku byl počet odpovědí minimální, naopak maxima dosahuje křivka dne 13.12.2019 a na počátku ledna 2020, ačkoli odkazy byly potencionálním respondentům rozesílány v pravidelném režimu cca 45 dotazníků denně kromě období Vánoc, tedy od 24. do 29.12.2019. Velké výkyvy mohou být způsobeny koncem roku, kdy většina firem má více aktivit, např. vyhodnocování obratů , tlak na dosažení plánu, účetní závěrka, inventarizace majetku a zásob, archivace dokumentů a v neposlední řadě i vánoční večírky, akce se zákazníky a dovolené či uzavření společnosti z důvodu vánoční odstávky, která mnohdy trvala až do 10.01.2020, např. v Polsku a v Německu. Dotazníky byly rozesílány respondentům jednotlivě, s konkrétním oslovením osoby, aby bylo dosaženo navázání kontaktu

s danou osobou, a přesto bylo dosaženo poměrně nízké úspěšnosti, jak je prezentováno grafem dokončených dotazníků na obrázku č. 5.



Obrázek 4: Časová osa vyplňování dotazníků

Zdroj: Vlastní zpracování

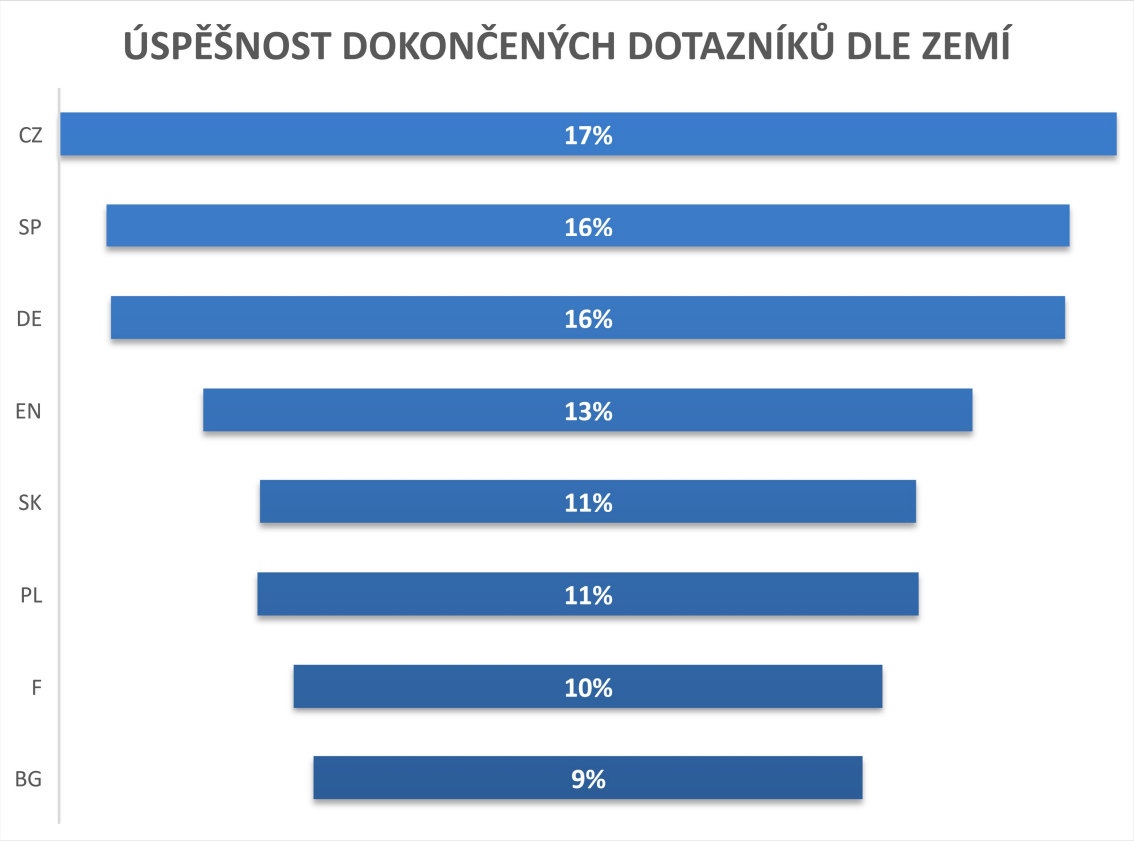


Obrázek 5: Zaslané odkazy vs. dokončené dotazníky

Zdroj: Vlastní zpracování

V každé zemi bylo osloveno 205 až 416 respondentů, z nichž průměrně 70 % tvořily zprostředkované kontakty od kontaktních osob (Čechů žijících v příslušné zemi).

Zbylé kontakty byly vyhledány na internetových stránkách, s cílem oslovit také státní instituce typu: nemocnice, školství a státní úřady, které ve skupině zprostředkovaných kontaktů chyběly, aby spektrum oslovených firem zasáhlo co možná nejširší možnou oblast. Z pohledu jednotlivých zemí byla nejvyšší úspěšnost v České republice (17 %), na druhém místě je Španělsko (16 %) a Německo (16 %) na třetím místě je Velká Británie (13 %), dále Slovensko (11 %) a Polsko (11 %), na předposledním místě je Francie (10 %) a nejnižší úspěšnosti bylo dosaženo u Bulharska (9 %).



Obrázek 6: Úspěšnost dokončených dotazníků dle zemí
Zdroj: Vlastní zpracování

V průběhu dotazníkového šetření byla zjištěna velká variabilita osob, respektive pracovních pozic, které byly dostatečně erudované v oblasti GDPR, a tedy schopné odpovědět na zadané otázky. V některých firmách byla správa GDPR v kompetenci IT oddělení, v jiných firmách tuto oblast zastřešovalo finanční oddělení případně HR oddělení, outsourcována nebo roztříštěna mezi několik osob.

Obrázek 7: Dokončené dotazníky
Zdroj: Vlastní zpracování

Ačkoliv byl osloven respondent, který měl v dané oblasti nejvíce informací, jeho znalosti převážně nepokryly odpovědi na všechny otázky. Respondent z finančního oddělení měl obvykle přehled o výši nákladů vynaložených na GDPR, naopak mu byla cizí oblast týkající se IT problematiky. Pro tyto případy zvolili respondenti odpověď "nevím" a netipovali pouze vhodnou odpověď, což zabránilo zkreslení dotazníkového šetření. Výše uvedená fakta potvrzuje samotný výsledek dotazníkového šetření, kdy respondent neznal odpověď na otázku, např. u výše nákladů investovaných do GDPR. Dalším ukazatelem potvrzujícím prezentované tvrzení je poměr počtu zobrazených dotazníků a počtu dokončených, tedy zodpovězených dotazníků. Pokud se zaměříme na otevřené dotazníky, celých 49 % dotazníků bylo pouze zobrazeno, což představuje 296 potencionálních respondentů a 51 % oslovených dotazník dokončilo, tj. 307 vzorkovaných.

Průměrný čas, který respondenti strávili vyplňováním dotazníku, činí 17:06 min, nejrychleji byl dotazník vyplněn za 4:37 min a nejdéle za 15h 15 min. Průměrná hodnota je ovšem výrazně ovlivněna třemi hodnotami, deklarující vyplňování dotazníku po dobu delší než 1 hodina. Jedna z hodnot ukazuje, že vyplňování

dotazníku trvalo 15 h a 15 min, druhá hodnota 1 h a 12 min, třetí hodnota 1 h a 11 min. Pokud vyloučíme uvedené tři extrémní hodnoty, které mohly být způsobeny pozastavením zpracování dotazníku respondentem, opuštění zařízení (počítače, tabletu apod.), průměrná hodnota strávená vyplněním dotazníku činí 13 min. Z pohledu četností je 230 dotazníku vyplněno v intervalu 8 min až 15 min.

Pomocí chí-kvadrátu bylo zjištěno, že dotazníkové šetření nejvíce ovlivnili respondenti z České republiky, dále ze Slovenska a Velké Británie.

Tabulka 1: Vliv států na výstup dotazníkového šetření

Stát	Četnosti	Očekávané četnosti	Testové kritérium
BG	30	30	0,00
CZ	72	30	58,80
DE	32	30	0,13
F	34	30	0,53
GB	36	30	1,20
PL	33	30	0,30
SK	38	30	2,13
SP	32	30	0,13
Celkem	**307**	**240**	**63,23**

Zdroj: Vlastní zpracování

Prostřednictvím dotazníkového šetření se podařilo získat dostatek odpovědí, napříč spektrem oblastí jednotlivých otázek a přineslo zajímavé výsledky, které jsou popsány dále.

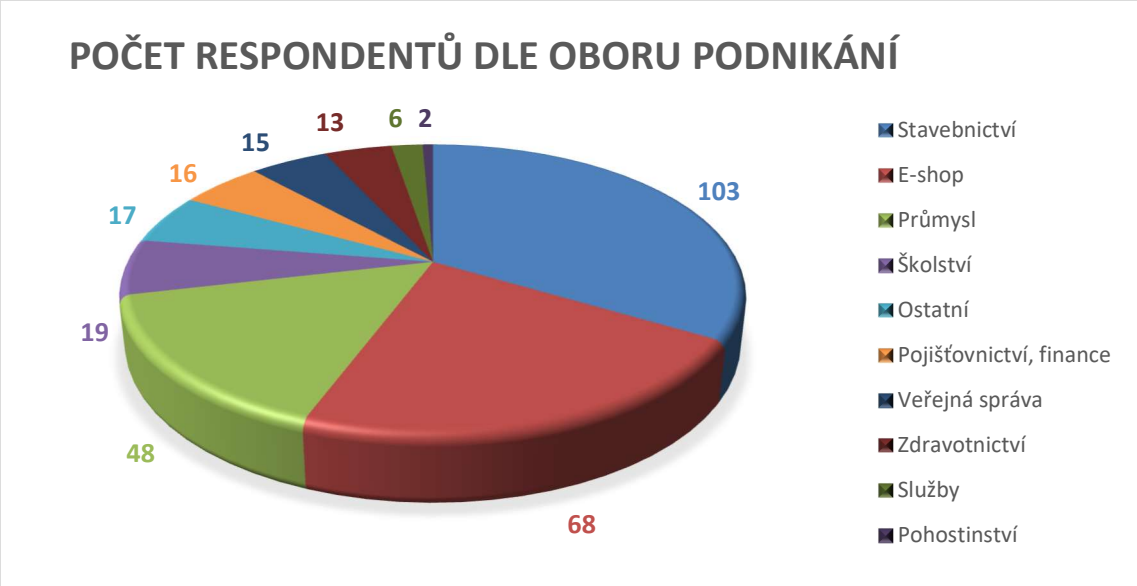
5.2 Vyhodnocení respondentů

Účastníky výzkumu byly firmy všech velikostí od mirko firem po velké podniky. Při zaslání dotazníků samozřejmě nebylo jasné, kdo z oslovených dotazník vyplní a garancí získání požadovaného počtu respondentů mohlo být pouze množství zaslaných dotazníků firmám všech velikosti. Resumé výsledků ukazuje, že z celkového počtu 307 dotazníků je 114 z oblasti malých podniků (počet zaměstnanců 11–50) a 101 z oblasti středních podniků (počet zaměstnanců 51–250 zaměstnanců). Na pomyslném třetím místě s 58 respondenty jsou velké firmy (více než 250 zaměstnanců) a nejméně respondentů, celkem 34, je z oblasti mikro

podniků (méně než 10 zaměstnanců). Výše uvedená data přehledně prezentuje graf na obrázku č. 8.

Obrázek 8: Počet respondentů dle velikosti firmy
Zdroj: Vlastní zpracování

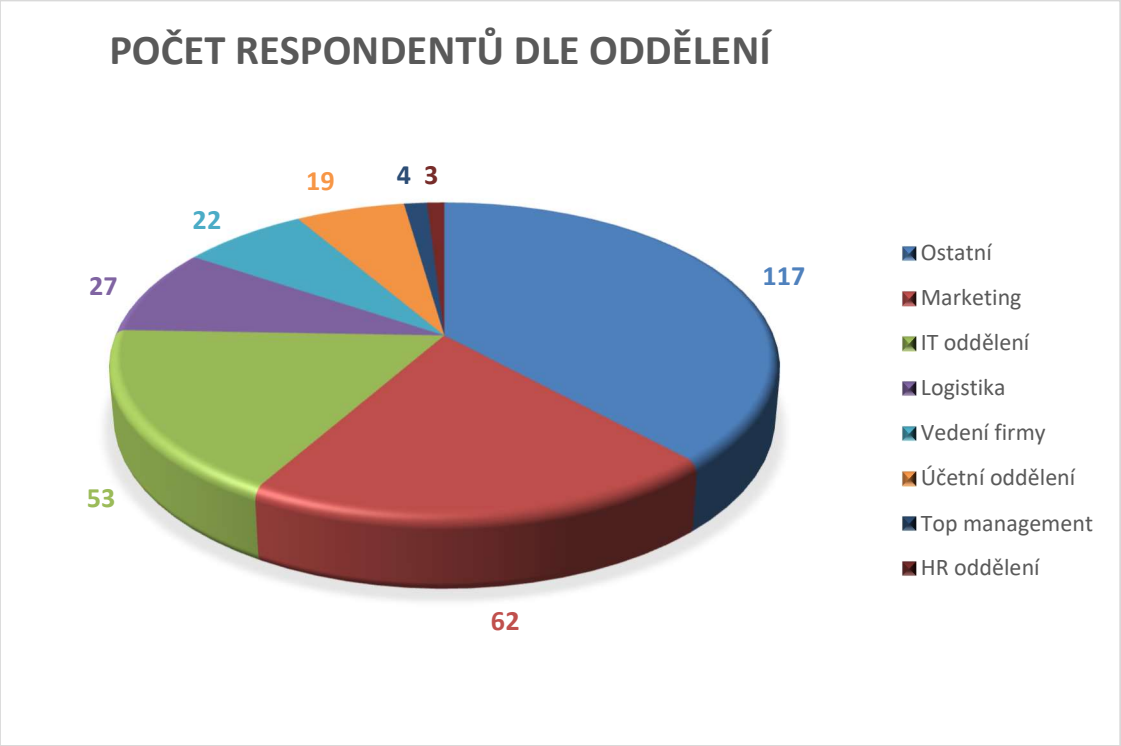
Nejvíce vzorkovaných firem je z oblasti stavebnictví (103), na druhém místě je e-shop (68) a na třetím místě průmysl (48), dále je zastoupeno školství (19), pojišťovnictví a finance (16), veřejná správa (15), zdravotnictví (13), služby (6), pohostinství (2).



Obrázek 9: Počet respondentů dle oboru podnikání
Zdroj: Vlastní zpracování

Obory, které byly zastoupeny pouze jedním respondentem, jsou zahrnuty ve skupině „ostatní“ (17). V uvedené poslední skupině jsou např. respondenti z oblasti: armády, advokacie, kultury apod.

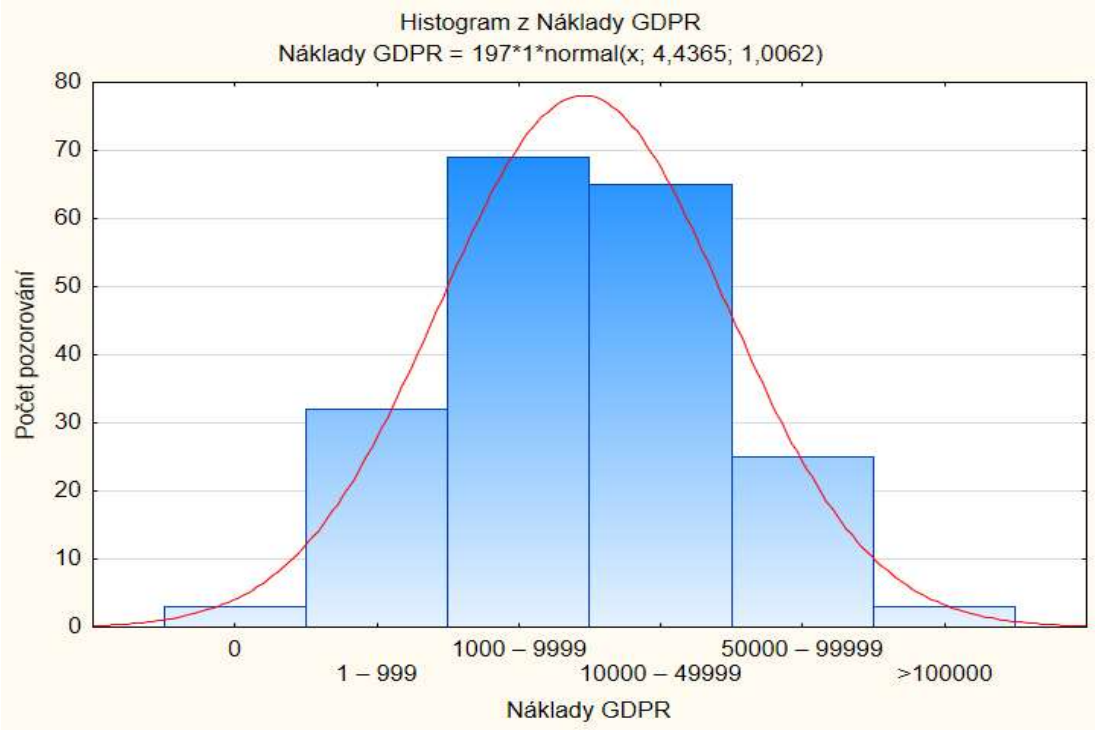
Rozložení počtu respondentů dle oddělení, ve kterém pracují, je prezentován grafem č. 10. Ve skupině ostatní (117) jsou nejvíce zastoupeny firmy z oboru stavebnictví (65), průmysl (15), školství (11). Zejména ve stavebnictví a školství jsou specifické pozice, které nebyly v dotazníkovém šetření definovány, dalším důvodem jsou osoby pracující na živnostenský list, např. makléř, firemní právník apod.



Obrázek 10: Počet respondentů dle oddělení
Zdroj: Vlastní zpracování

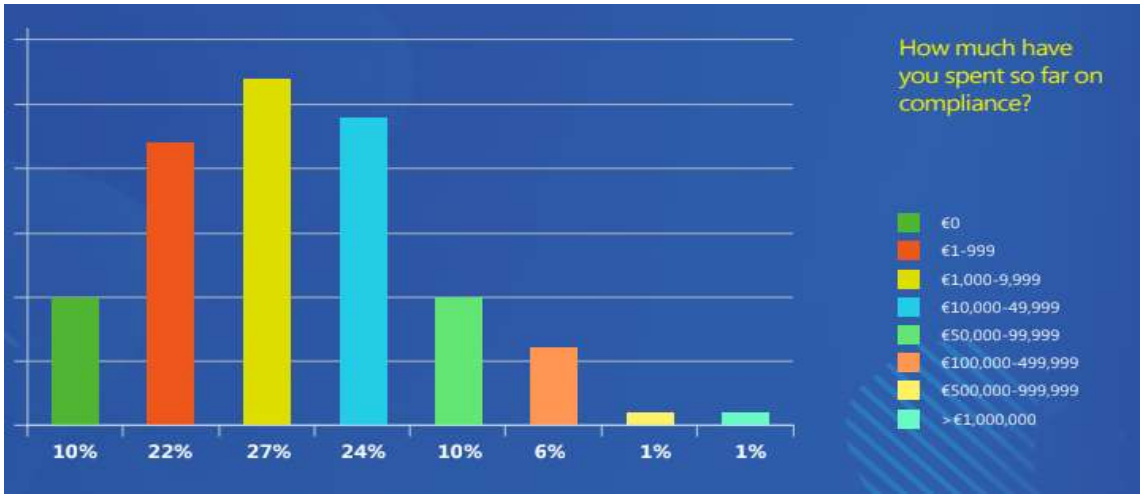
Třetina respondentů uvedla, že neví, jaké náklady firma vynaložila na GDPR. Nevyšší četnost vykazují dva intervaly nákladů 1 000 – 9 999 € (69), kde nejvyšší četnosti vykazují e-shopy (23), firmy z oboru stavebnictví (21) a z průmyslu (11). Druhý interval 10 000 – 49 999 € (65) má nejvyšší četnost v oboru stavebnictví (35). Na dalším místě je interval 1 – 999 € (32), nejvyšší četnost je vykazována u e-shopů (14). Náklady ve výši 50 000 – 99 999 € (25) vykázaly nejčastěji firmy z oblasti stavebnictví (17) a více než 100 000 € (3) deklarovaly firmy z oblasti průmyslu. Tři

respondenti uvedli, že firma vynaložila na GDPR nulové náklady, všichni tři vzorkovaní patří do skupiny mikro firem, tedy s počtem zaměstnanců nižším než 10, obory podnikání jsou odlišné: e-shop, školství, právnické služby. Výše nákladů je graficky znázorněna histogramem č. 11, kde uvedené zmiňované skupiny (1 000 – 999 a 10 000 – 49 999) vykazují absolutní četnosti téměř 70 vzorkovaných pro každou z nich, z celkového počtu 197. Z vyhodnocení byli vyloučeni vzorkovaní, jejichž odpověď byla „nevím“ (110). Rozložení pravděpodobností znázorňuje červená křivka, která představuje Gaussovo rozdělení, kde globální maximum je v bodě 9999.



Obrázek 11: Náklady GDPR
Zdroj: Vlastní zpracování v programu SW STATISTICA

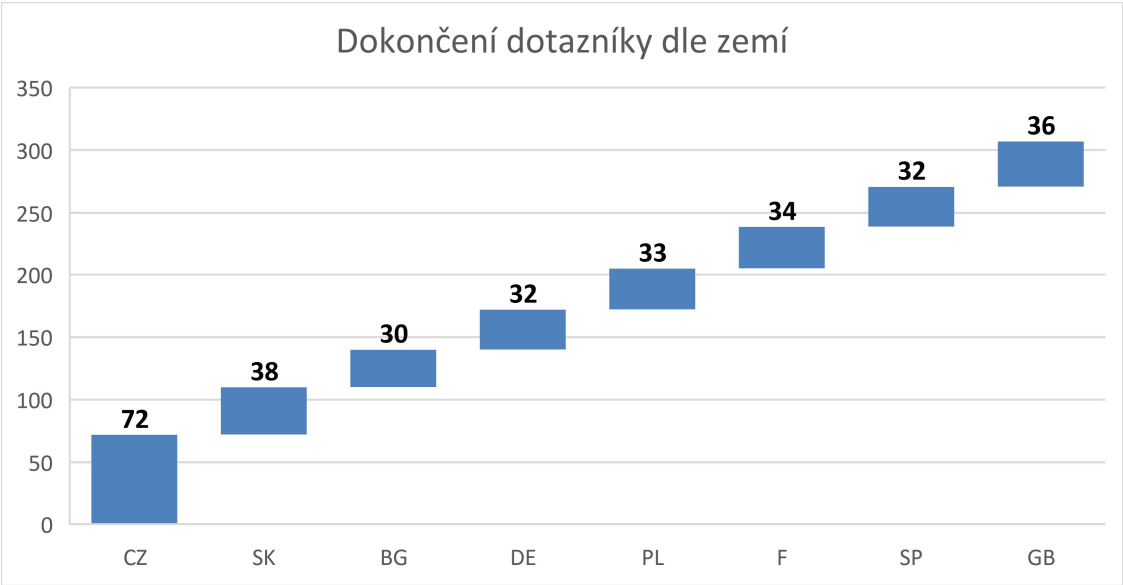
Zjištěné hodnoty navazují na GDPR.EU Small Business Survay z května 2019 (dále jen GDPR Survay). Výsledky tohoto výzkumu prezentují, že nejvíce firmy investovaly ve skupině 1 000 – 999 € (27 %) [GDPR.eu, 2019], dotazníkové šetření diplomové práce (dále DŠDP) vykazuje 35 %. Na druhém místě byla skupina 10 000 – 49 999 € (24 %) [GDPR.eu, 2019], DŠDP prezentuje 33 %.



Obrázek 12: GDPR Survay: Výše nákladů investovaných do GDPR
Zdroj: GDPR.eu, 2019

5.3 Vyhodnocení GDPR dle zemí

Pro dotazníkové šetření bylo zvoleno 8 zemí EU: Česká republika, Polsko, Španělsko, Francie, Bulharsko, Slovensko, Německo a Velká Británie, která v červenci 2019, kdy vznikaly první podklady diplomové práce, byla ještě jejím členem. Po dlouhých a vleklých sporech na britském politickém poli, dotáhl výstup Velké Británie z EU, ke zdárnému konci, Boris Johnson. Dne 24.1.2020 byla oficiálně podepsána dohoda o ukončení členství Velké Británie v EU. Poslední dotazník z Velké Británie byl respondentem zodpovězen 23.1.2020, kdy byla země ještě oficiálním členem EU.



Obrázek 13: Dokončené dotazníky dle zemí
Zdroj: Vlastní zpracování

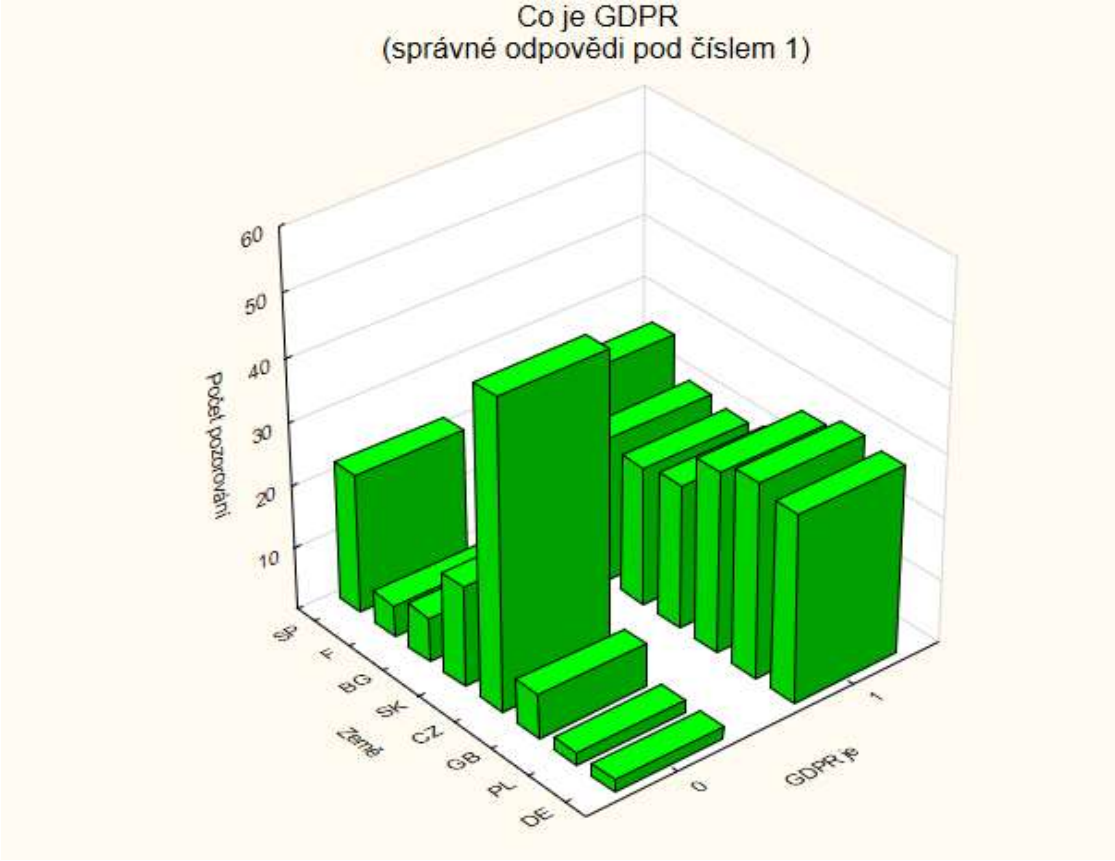
Graf číslo 13 indikuje, že z každé země bylo získáno minimálně 30 vzorkovaných, maximálně 72 vzorkovaných. Nejvíce respondentů se podařilo získat z České republiky (72), dále ze Slovenska (38), Velké Británie (36), Francie (34). Nejnižší počet je respondentů je vykazován za Španělsko (32), Polsko (33) a Německo (32). Minimální hranice bylo dosaženo v Bulharsku (30). Byla tak splněna další definovaná podmínka, která byla stanovena před zahájením dotazníkového šetření, a to získat minimálně 30 vzorkovaných z každé země.

5.3.1 Definice GDPR

Jednou ze základních otázek, na kterou respondenti odpovídali, byla zaměřena na definici GDPR. Vzorkovaní volili jednu ze 4 uzavřených odpovědí, které se lišily pouze ve specifikaci, koho chrání a kdo tento zákon musí dodržovat. Vzorkovaní nejčastěji chybně označovali, že GDPR chrání fyzické i právnické osoby nebo že zákon musí dodržovat subjekty, které mají sídlo společnosti na území EU. Faktem je, že GDPR vytváří tlak i na trhy mimo EU, dokonce již byl stanoven precedens nad použitím legislativy mimo území EU [Bendiek, 2019 s. 33]. Mezinárodní společnosti mnohem více ukládají data o svých evropských zákaznících v Evropě, aby byly v souladu s platnou legislativou [Bendiek, 2019 s. 33]. Touha společnosti po transparentnosti používání osobních údajů je vysoká, a ačkoliv je GDPR právním nařízením EU, významně zasahuje a ovlivňuje i státy mimo toto území [Laybats, 2018, s. 82].

Správná odpověď byla pouze jedna: Právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji, který musí dodržovat všechny firmy, manipulující s daty občanů EU, místo sídla firmy není podstatné. Správně otázku zodpovědělo celkem 197 respondentů (64,17 %). Dílčí úspěšnosti byly počítány jako poměr úspěšných odpovědí a celkového počtu dotazníků dané země. Nejvyšší procento úspěšnosti vykázaly tyto tři země: Polsko (93,94 %), Francie (85,29 %) a Velká Británie (80,56 %). Naopak nejnižší úspěšnost je u Španělska (31,25 %) a České republiky (31,94 %). Pro zjednodušení grafického výstupu jsou správné odpovědi označeny číslem 1 a chybné odpovědi číslem 0.

Navazující otázka zjišťovala, zda byli vzorkovaní proškoleni zaměstnavatelem v oblasti GDPR a četnost těchto školení. Uzavřené odpovědi dotazníku nabízely možnosti: (1) ne, (2) ano, jednou, (3) ano, opakovaně. Celkem nebylo proškoleno 29 respondentů (9,45 %). Nejvíce neproškolených vykázala Česká republika (18,6 %), Španělsko (15,63 %). Neproškolení zaměstnanci budou patřit mezi faktory ovlivňující úspěšnost odpovědi. Dalším významným faktorem bude forma školení, erudovanost školitele apod. Tyto otázky ovšem nebyly součástí dotazníkového šetření a nelze tak posoudit míru vlivu na správnost odpovědí.



Obrázek 14: Správné odpovědi dle zemí
Zdroj: Vlastní zpracování v programu SW STATISTICA

Nejvyšší úspěšnost vykazuje dvojice Německo a Velká Británie, kde byl také nejnižší počet neproškolených osob. Vzorkovaní mají poměrně dobré povědomí o tom, co vše jsou osobní údaje (64,17 %) a počet neproškolených osob je nízký (9,4 %).

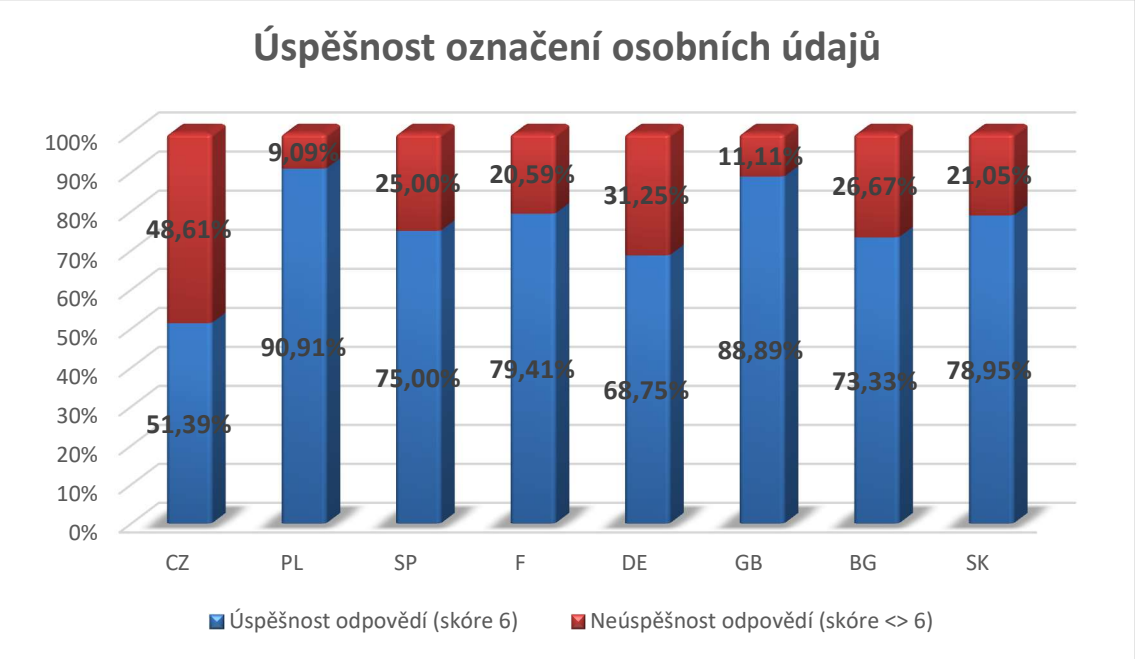
Tabulka 2: Úspěšnost odpovědí: Co je GDPR a četnost školení

Země	Úspěšnost	Absolutní četnost správných odpovědí	Počet dotazníků	Proškolen jednou	Proškolen opakovaně	Neproškolen	Neproškolen v %
CZ	31,94%	23	72	35	24	13	18,06%
PL	80,56%	31	33	22	11	0	0,00%
SP	31,25%	10	32	16	11	5	15,63%
F	93,75%	29	34	15	18	1	2,94%
DE	93,75%	30	32	7	24	1	3,13%
GB	85,29%	29	36	9	25	2	5,56%
BG	76,67%	23	30	18	10	2	6,67%
SK	57,89%	22	38	18	15	5	13,16%
Celkem	**64,17%**	**197**	**307**	**140**	**138**	**29**	9,45%

Zdroj: Vlastní zpracování

5.3.2 Osobní údaje

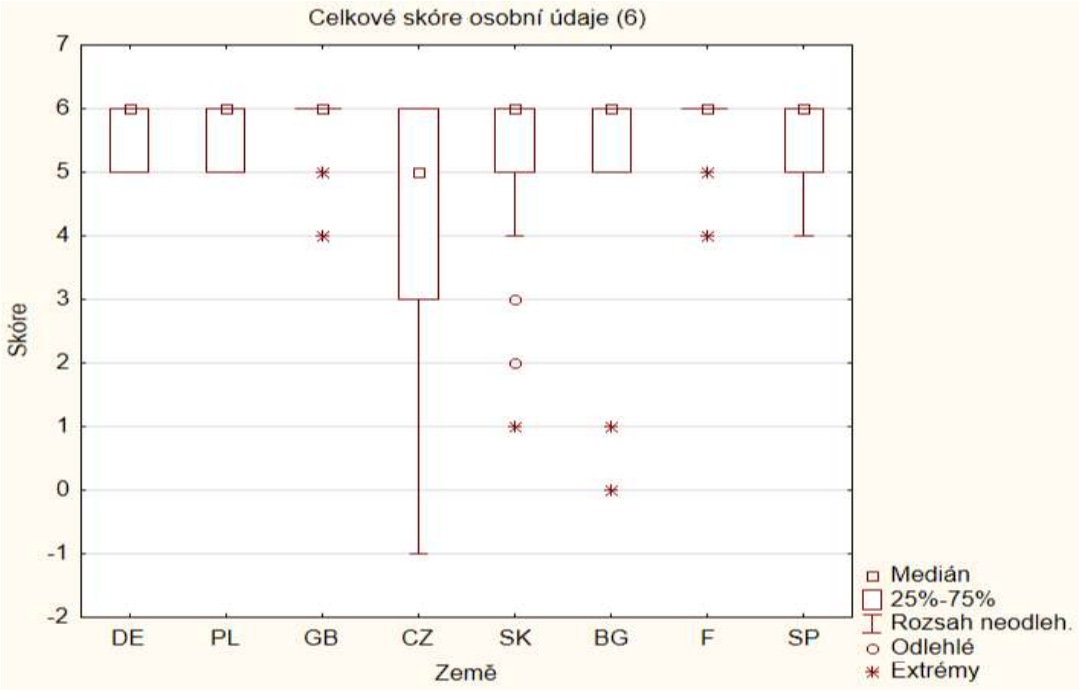
V této otázce měli vzorkovaní označit všechna uvedená data, která považovali za osobní údaje. Otázka byla vyhodnocena takto: za každý správně označený osobní údaj byl přiřazen jeden bod, naopak za chybně označený osobní údaj byl bod odečten. V případě, že osobní údaj nebyl označen, byla přiřazena nula. Celkovým součtem vzniklo skóre respondenta. Součet správných odpovědí je přesně 6.



Obrázek 15: Úspěšnost označení osobních údajů
Zdroj: Vlastní zpracování

Úspěšnost jednotlivých zemí je dána jako poměr absolutní čestnosti skóre 6 a celkovým počtem dotazníků dané země. Celková úspěšnost je 72,96 %. Nejpřesnější odpovědi, a tedy nejvyšší úspěšnost, vykazuje Polsko (90,91 %), Velká Británie (88,89 %) a Francie (79,41 %). Nejhůře vyhodnotili data respondenti České republiky (51,39 %) a Německa (68,75 %).

Grafické znázornění identifikace osobních údajů je prezentováno také krabicovým grafem níže. Výsledky České republiky se pohybují v kvartilovém rozpětí 25 % - 75 %. Hodnoty ostatních zemí se pohybují v prvním kvartilu, nebo se jedná pouze o odlehlé, nebo extrémní hodnoty. Nejčastěji respondenti chybně označovali jako osobní údaj: obrat firmy, služební telefonní číslo, identifikátory firmy (IČO, číslo účtu, adresa), výroční zprávu. Označení údajů týkajících se společnosti (IČO, výroční správa, obrat atd.) souvisí s chybným chápáním GDPR, kdy respondenti označili, že GDPR chrání fyzické i právnické osoby, jak je blíže uvedeno v článku 5.3.1.



Obrázek 16: Celkové skóre osobní údaje
Zdroj: Vlastní zpracování v programu SW STATISTICA

Výše uvedená data dokazují, že vzorkovaní dokážou identifikovat osobní data s celkovou úspěšností 72,96 %, což je vyšší hodnota než při definici GDPR v přechozím bodě, kde byla úspěšnost 64,17 %.

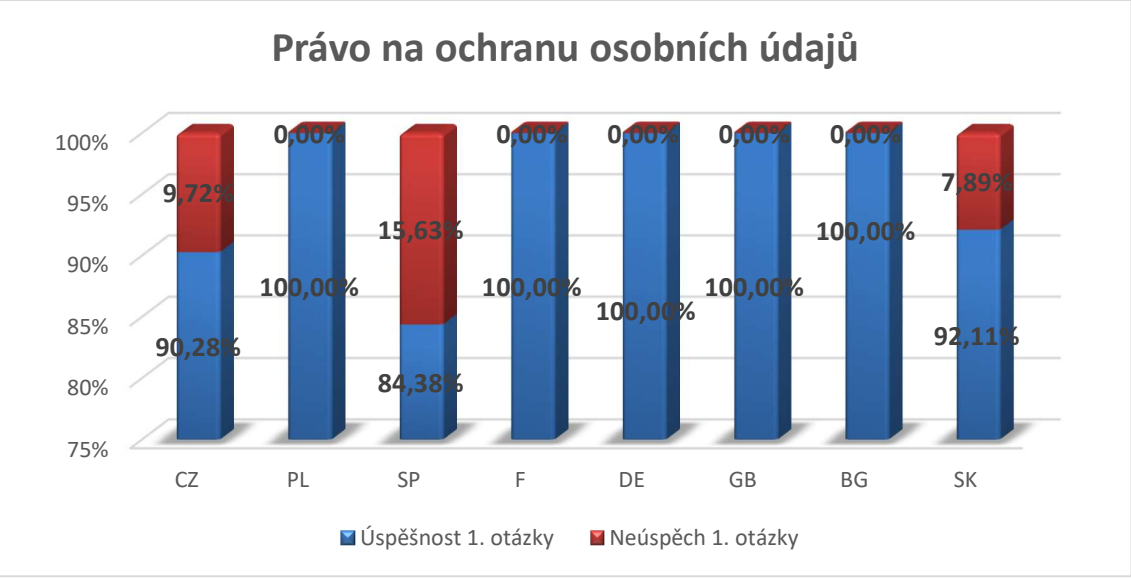
5.3.3 Práva GDPR

Úkolem respondenta bylo označit všechna práva, která GDPR zaručuje. Opět se jednalo o otázku s uzavřeným typem odpovědí. Odpovědi byly celkem 4 a každá z nich obsahovala definici jednoho ze základních práv, která GDPR zaručuje, tedy:

- Ochranu osobních údajů;
- Právo vyžádat si všechny údaje, které o poskytovateli údajů subjekt zpracovává;
- Právo na výmaz osobních údajů;
- Právo odmítnou zpracování údajů.

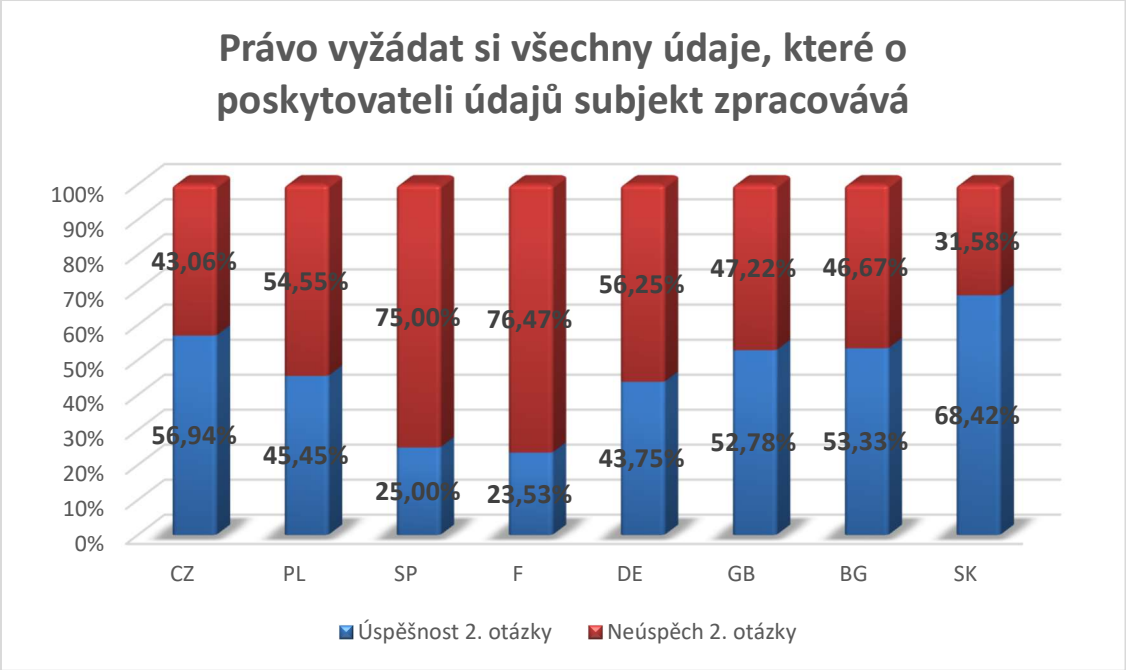
Vyhodnocení probíhalo obdobným způsobem jako v předchozím bodě. Za správnou odpověď byl respondentovi udělen jeden bod, za neoznačenou odpověď nula bodů. V této otázce nebyla v nabídce chybná odpověď. Skóre správně zodpovězených všech otázek je rovno 4 bodům.

Tato otázka odhalila vysokou neznalost vzorkovaných. Zatímco právo na ochranu osobních údajů bezchybně označili respondenti hned z 5 zemí a úspěšnost byla 95,11 %, u ostatních otázek byla chybovost výrazně vyšší. Níže uvedené grafy prezentují úspěšnost jednotlivých zemí. Celková úspěšnost první odpovědi je 95,11 %.



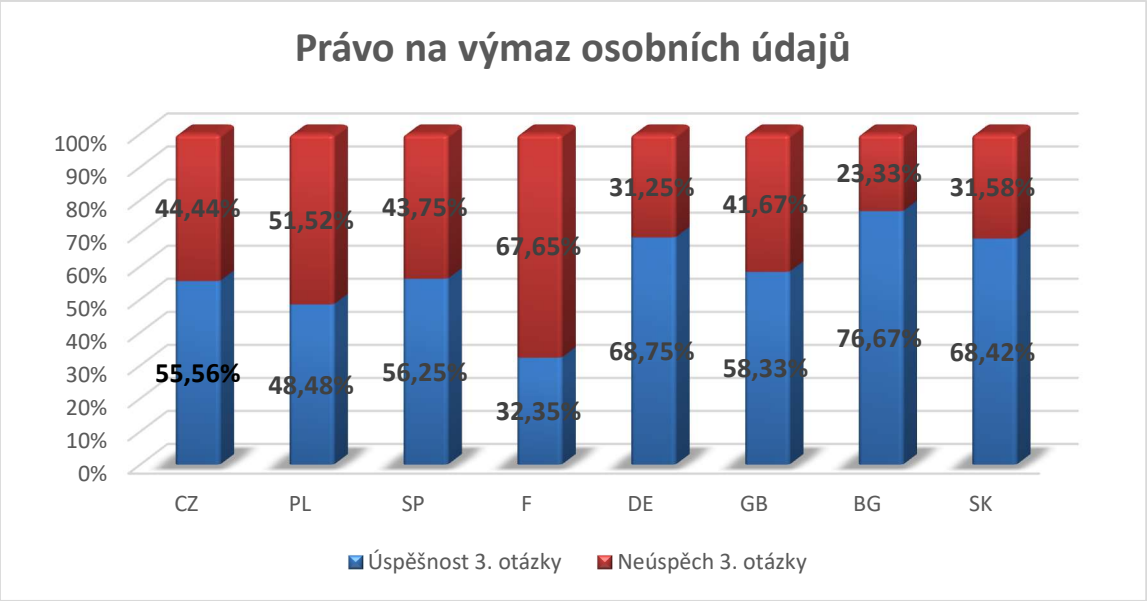
Obrázek 17: Úspěšnost otázky: Právo na ochranu osobních údajů
Zdroj: Vlastní zpracování

Bezchybné odpovědi vykázala: Francie, Německo, Velká Británie, Bulharsko a Polsko, naopak nejvyšší chybovost je u Španělska. Právo vyžádat si všechny údaje, které o poskytovateli údajů subjekt zpracovává, bylo druhou otázkou tohoto bloku. Správnou odpověď označilo pouhých 47,88 % a tato odpověď se tak řadí na poslední místo z uvedených 4 odpovědí. Mezi nejúspěšnější země patří Slovensko (68,42 %) a Česká republika (56,94 %). Naopak nejvíce chybných odpovědí vykazuje Francie (76,47 %) a Španělsko (75 %).



Obrázek 18: Úspěšnost otázky: Právo vyžádat si všechny údaje
Zdroj: Vlastní zpracování

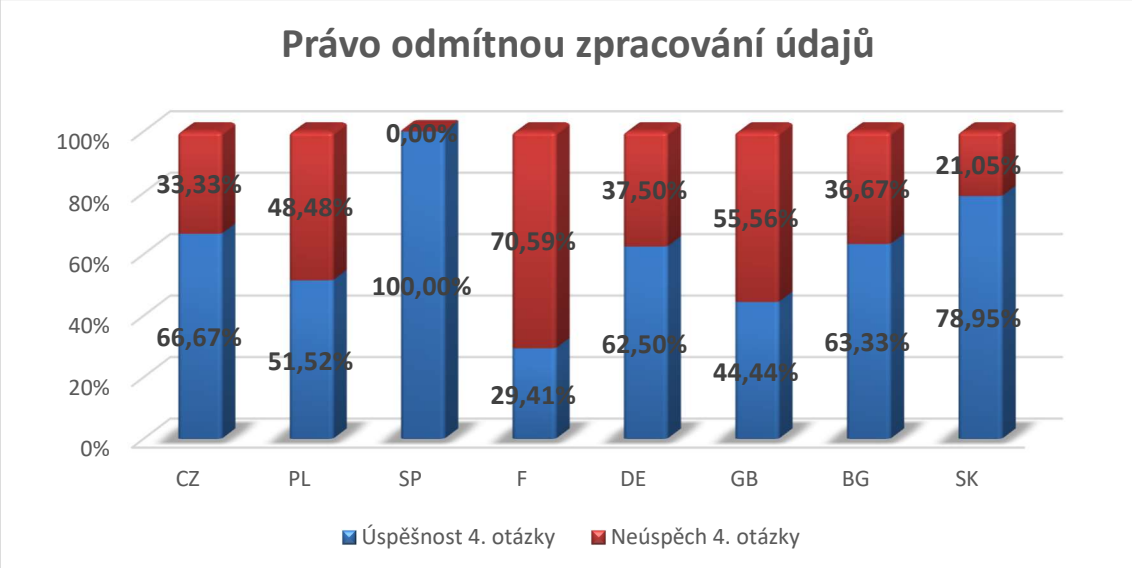
Výrazně lépe dopadla odpověď týkající se práva na výmaz osobních údajů, kde byla celková úspěšnost 57,65 % a zaujala třetí místo v tomto bloku odpovědí. Nejvyšší počtu správných odpovědí vykazuje Bulharsko (76,67 %), Německo (68,75 %), Slovensko (68,42 %) a Velká Británie (58,33 %). Respondenti mají GDPR spojeno tedy zejména s právem na ochranu osobních údajů a na jejich výmaz, naopak výrazně nižší povědomí mají o právu vyžádat si všechny údaje, které o nich subjekt zpracovává.



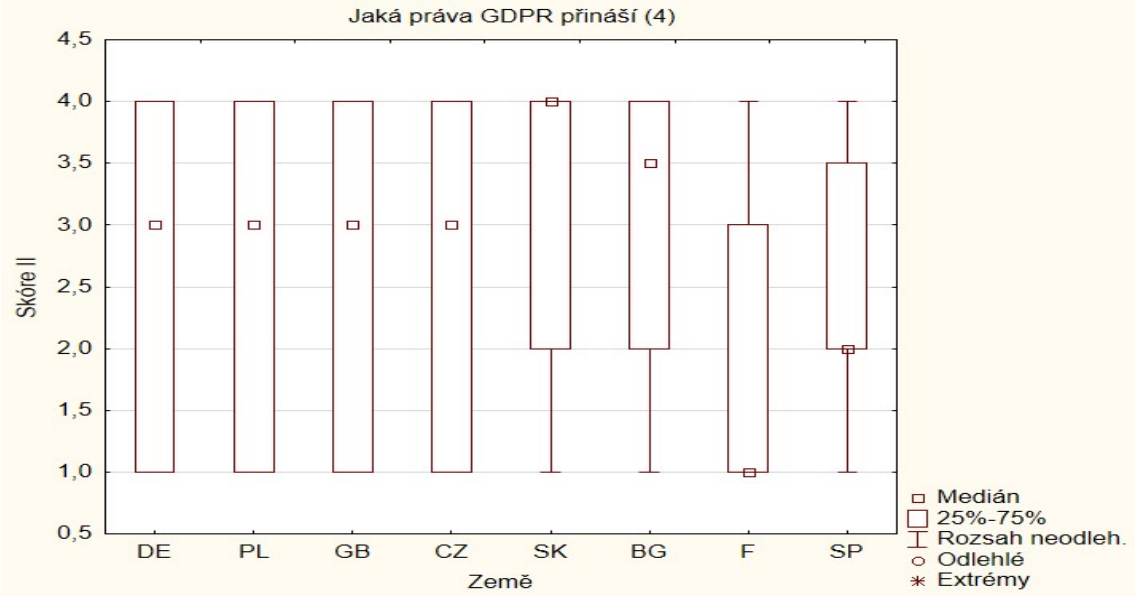
Obrázek 19: Úspěšnost otázky: Právo na výmaz osobních údajů
Zdroj: Vlastní zpracování

Respondenti jsou si tedy práva na výmaz osobních údajů vědomi, ale jak bylo zmíněno v bodu 4.2, využívají ho minimálně. Společnost Coca-Cola má ve své databázi statisíce klientů a doposud požádali o vymazání dat pouze 4 klienti [ÚOOU, b, 2019, s. 14].

Poslední odpověď se týkala práva odmítnout zpracování osobních údajů a patří na druhém místo z pohledu úspěšnosti odpovědí, která je 62,54 %.



Obrázek 20: Úspěšnost otázky: Právo odmítnou zpracování údajů
Zdroj: Vlastní zpracování



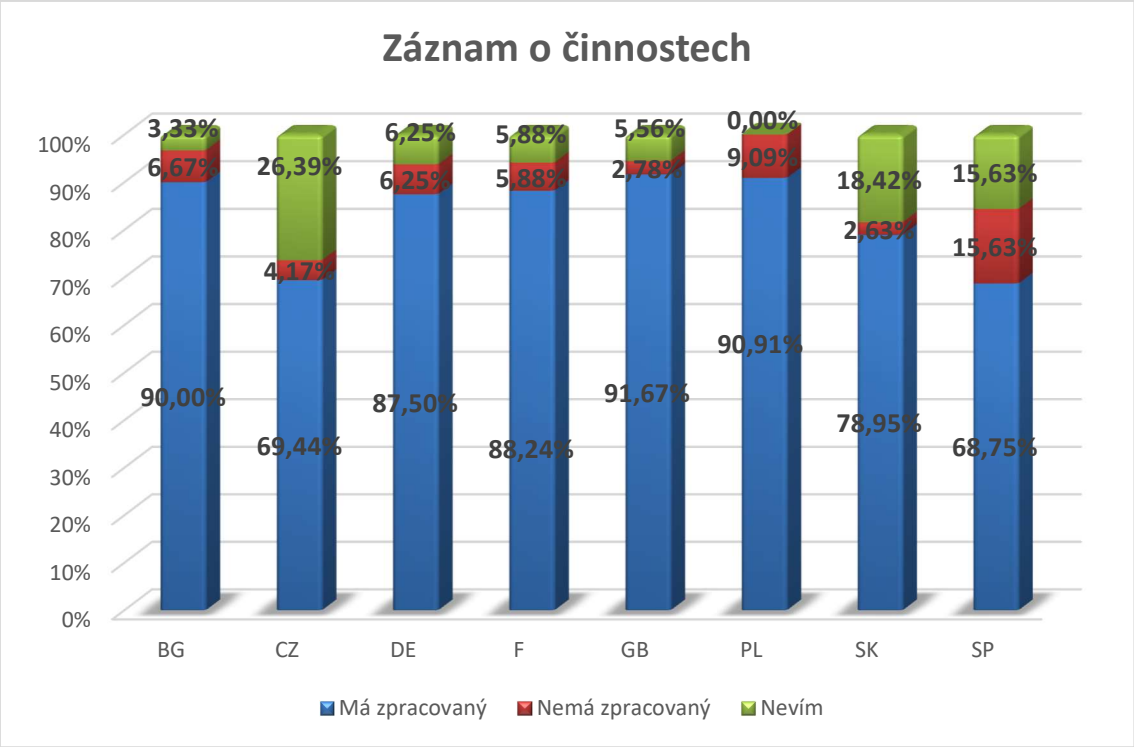
Obrázek 21: Jaká práva GDPR přináší
Zdroj: Vlastní zpracování v programu SW STATISTICA

Nejvíce správných odpovědí prezentuje Španělsko (100 %), Slovensko (78,95 %) a Česká republika (66,67 %). Nejvíce chybných odpovědí vykazuje Francie (70,59 %), Velká Británie (55,56 %) a Polsko (48,48 %). Celkové rozložení skóre získaného označením odpovědí je prezentováno krabicovým grafem č. 21.

GDPR mají vzorkovaní spojené především s právem na ochranu osobních údajů, kde úspěšnost odpovědí byla 95,11 %. Naopak si neuvědomují, že jim GDPR přináší také právo vyžádat si všechny údaje, které o fyzické osobě subjekt zpracovává (52,12 %).

5.3.4 Záznam o činnostech

Záznam o činnostech mají povinnost vést firmy s více než 250 zaměstnanci. Ačkoliv je většina respondentů z oblasti malých a středních firem, tedy s méně než 250 zaměstnanci, a GDPR jim proto neukládá povinnost zpracovat záznam o činnostech, převážná část vzorkovaných má záznam o činnostech firmy zpracovaný (81,4 %). Ani jedna ze vzorkovaných firem s více než 250 zaměstnanci (58) neuvedla, že by záznam o činnostech firmy neměla zpracovaný. 11 z nich ovšem uvedlo odpověď „nevím“.



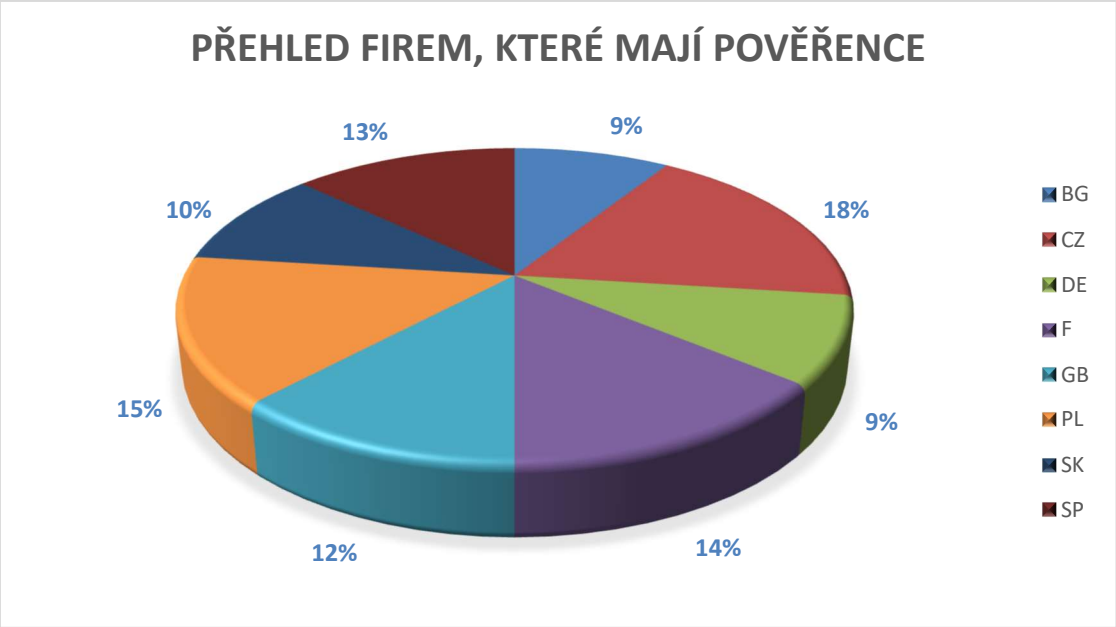
Obrázek 22: Záznam o činnostech
Zdroj: Vlastní zpracování

Zpracování záznamu o činnostech lze ovšem považovat za velmi vhodný nástroj, který společnosti pomůže odhalit hrozby a rizika, která v rámci manipulace s daty, vznikají a mohou tak včas zjednat nápravu, před vznikem problému.

Na základě výsledků respondentů lze usuzovat, že firmy, ve kterých vzorkovaní pracují, splňují zákonnou povinnost nad rámec svých povinností, tedy většina firem má zpracovaný záznam o činnostech firmy, ačkoliv by nemusela.

5.3.5 Pověřenec

GDPR ukládá povinnost všem veřejným subjektům a orgánům veřejné moci zřídit pozici pověřence. Hlavním úkolem **pověřence** je poskytování informací, poradenská činnost, monitoring činností, zpracování záznamů o činnostech a spolupráce s ÚOOU [ÚOOU, a, 2019]. Ve vzorkovaných je prokazatelně celkem 31 státních organizací, tedy ze skupiny samospráva či státní podnik. Celkem 4 vzorkovaní uvedli, že pověřence nemají.



Obrázek 23: Přehled firem, které mají pověřence
Zdroj: Vlastní zpracování

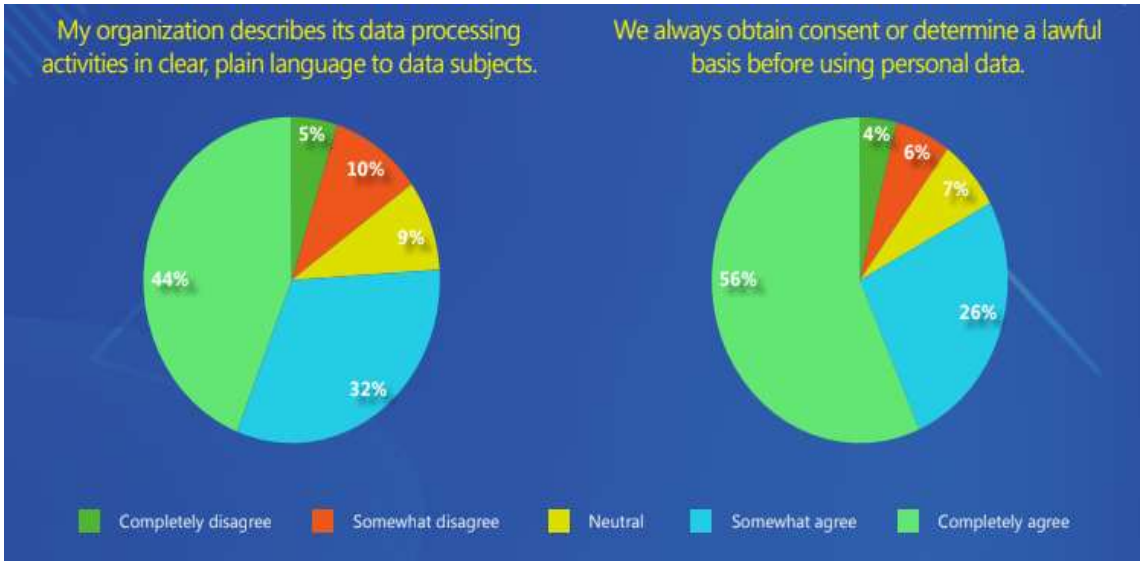
Mnohem zajímavější hodnota je celkový počet pověřenců, který činí 196, tedy téměř 64 % firem respondentů mají svého pověřence. Na rozdíl od záznamu o činnostech, který subjekty nic nestojí, pozice pověřence je spojena s nemalými náklady. V rámci marketingové bubliny o GDPR, např. v České republice, byl pověřenec symbolem souladu firmy s GDPR a obrany proti vysokým pokutám, které byly v médiích prezentovány. Celkem 22 firem, ze sektoru státních organizací, nemá uveden kontakt pověřence na webových stránkách ani na úřední desce a 3 z nich jsou státní organizace.

Ačkoliv mít pověřence ukládá legislativa GDPR pouze podnikům s více než 250 zaměstnanci, pozici pověřence zřídily či službu outsourcovaly i firmy, kterých se tato povinnost netýká a vynakládají tak náklady na jeho provoz.

5.3.6 Souhlas poskytovatele údajů

ÚOOU na svých stránkách uvádí, že GDPR rozpoutalo vlnu žádostí o souhlas se zpracováním údajů, kterými firmy zavalují občany, často zbytečně a dokazují tak nepochopení principů GDPR [ÚOOU, a, 2019]. Celkem 283 vzorkovaných (92 %) uvedlo, že před zpracováním osobních údajů mají, nebo částečně mají souhlas poskytovatele údajů, tedy fyzické osoby. 21 respondentů uvedlo odpověď „nevím“

a 3 respondenti uvedli, že s výrokem nesouhlasí, ačkoliv všichni tři vzorkovaní mají svého pověřence a je tak velký předpoklad, že je tento proces pod kontrolou a v souladu s legislativním nařízením. Další navazující otázka souvisí s profilováním uživatele a vyjádřením jeho souhlasu s užíváním cookies. Propojení dat umožňuje rychlé poskytnutí požadovaných služeb a nabízejí zákazníkovi srovnání webových stránek, produktů, např. v oblasti pojištění [Marano, 2019, s. 301]. Že se jedná o kontrolovanou oblast dokazuje např. francouzský regulátor ochrany údajů, Nationale de l'Informatique et des Libertés (CNIL), který uložil pokutu ve výši 50 milionů EUR za to, že společnost Google neposkytla uživatelům dostatečné informace a nezískala svůj souhlas při shromažďování informací k personalizaci reklam [Computer Fraud & Security, 2019]. Celkem 48 vzorkovaných potvrdilo používání cookies. Zároveň také většina z nich uvedla, že podnikli kroky v této oblasti, aby dostáli legislativě GDPR. Jako příklad uvedli např. obecné rozšíření informovanosti o používání cookies, informace o subjektech, s kterými data sdílí, zvětšení písma apod. Dotazníkové šetření prokázalo, že firmy dodržují tyto povinnosti, které jim GDPR ukládá, 43 z nich používá i anonymizaci a pseudoanonymizaci dat, což opět koresponduje s výsledkem GDPR Survay z května 2019, viz graf níže.

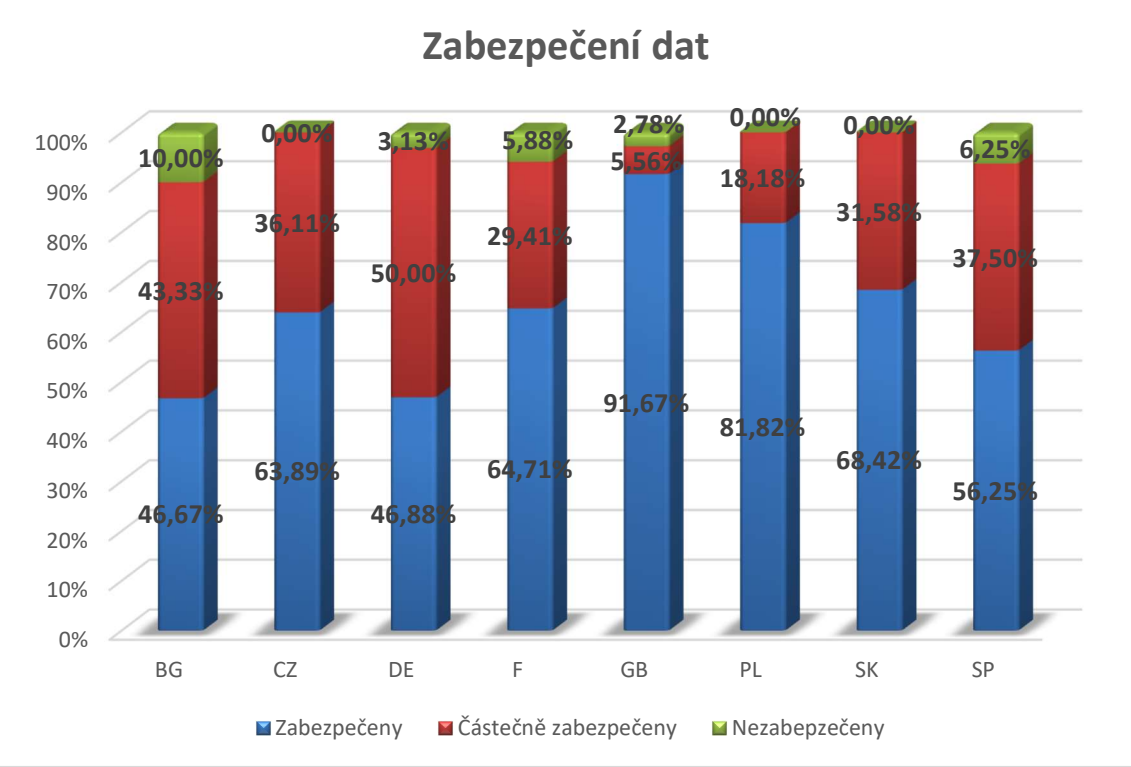


Obrázek 24: GDPR Survay: Zpracování osobních dat
Zdroj: GDPR.eu, 2019

5.3.7 Zabezpečení dat

Nesprávná ochrana osobních údajů, obzvlášť zvlášť citlivých údajů, může negativně ovlivnit nebo dokonce poškodit subjekty údajů [Ahmadian, 2018, s. 1467]. Posouzení vlivu na soukromí (PIA), které zahrnuje systematické hodnocení rizik, jehož cílem je identifikace hrozeb v oblasti soukromí, technické a organizační mechanismy k eliminaci hrozeb, jsou povinni provést správci [Ahmadian, 2018, s. 1467]. Se zabezpečením dat byli vzorkovaní konfrontování hned v rámci několika otázek. První blok otázek zjišťoval jejich názor na míru zabezpečení dat: jak jsou zabezpečena tisková data a elektronická data. Druhý blok zkoumal zabezpečení přístupu na mobilní telefon a počítač. Poslední blok otázek se zabývá šifrováním dat.

V prvním bloku otázek, který se týkal globálního zabezpečení dat, kde byla jako příklad uvedena: uzamčená skříň, serverovna, archiv, většina respondentů (79 %) uvedla, že jsou data zabezpečena, nebo alespoň částečně zabezpečena.



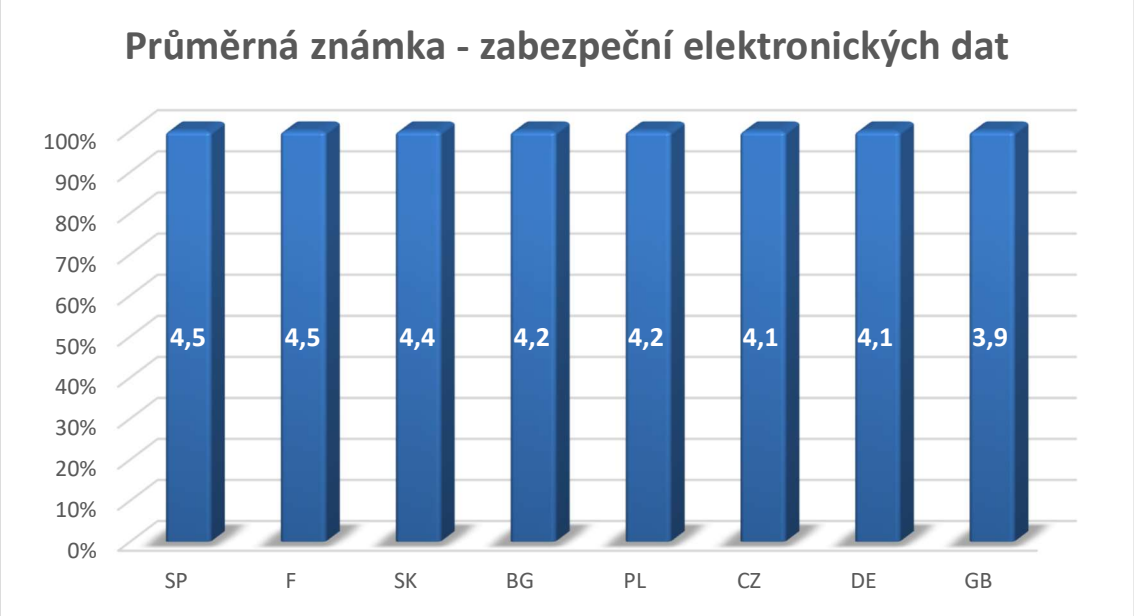
Obrázek 25: Zabezpečení dat
Zdroj: Vlastní zpracování

Celkem 9 respondentů naopak odpovědělo, že jsou data volně přístupná, což je, z pohledu GDPR, neakceptovatelné. Zástupci jsou z oblasti mikro firem (4), malých

firem (4) a z oblasti velkých firem (1), obor podnikání firem byl různý. Bližší rozlišení respondentů je prezentováno grafem č. 25. Nejvyšší pochybení je prezentováno u Bulharska (10 %). Naopak nejvyšší zabezpečení dat uvedli vzorkovaní z Velké Británie (91,67 %), Polska (81,82 %) a Slovenska (68,42 %). Míru částečného zabezpečení uvedlo nejvíce respondentů z Německa (50 %).

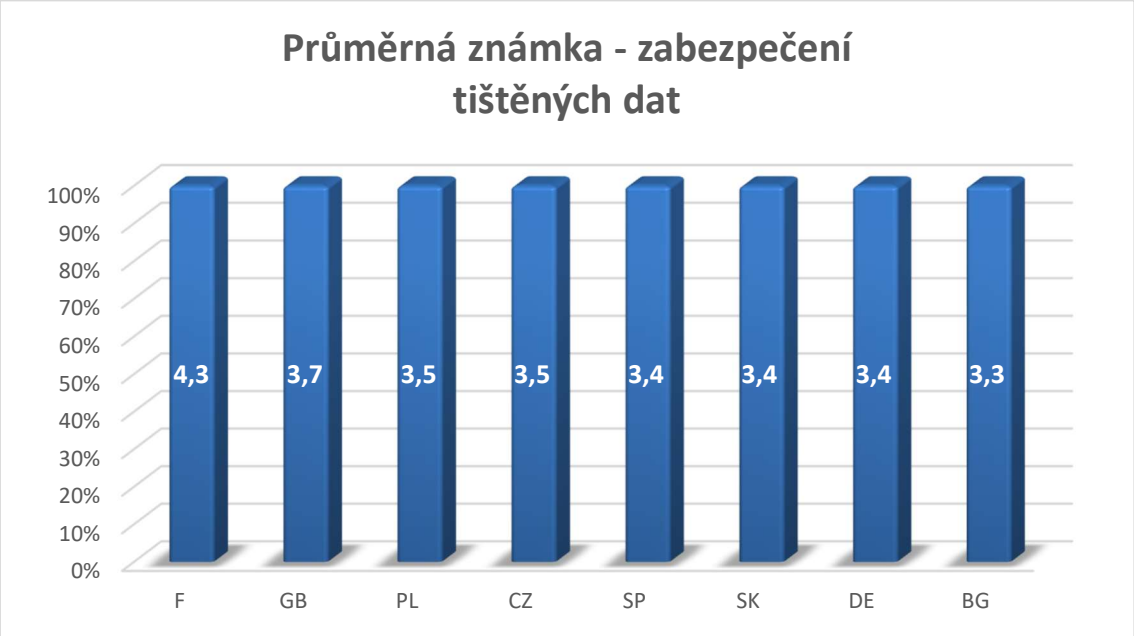
Na obecnou otázku zabezpečení dat navazovala otázka zaměřená na ochranu elektronických dat. Kromě samotné otázky bylo v zadání opět definováno také několik příkladů pro jasnější představivost respondenta: kontrolované přístupy, nahlížení na data, omezený přístup do serverovny, šifrování.

Odpověď nabízela škálu 1 až 5, při čemž 1 představuje nejnižší zabezpečení a 5 naopak nejvyšší zabezpečení elektronických dat. Celková průměrná známka byla 4,2. Průměrná známka byla zkoumána také z pohledu velikosti vzorkované firmy, ale průměrná známka měla obdobný trend pro jednotlivé společnosti, proto nebyla dále vyhodnocena. Z pohledu zemí dosáhla nejnižší průměrné známky Velká Británie (3,9) a na opačné straně je Španělsko (4,5) a Francie (4,5) s nejvyššími známkami. Průměrné známky definující zabezpečení elektronických dat dle respondentů jsou graficky znázorněny níže.



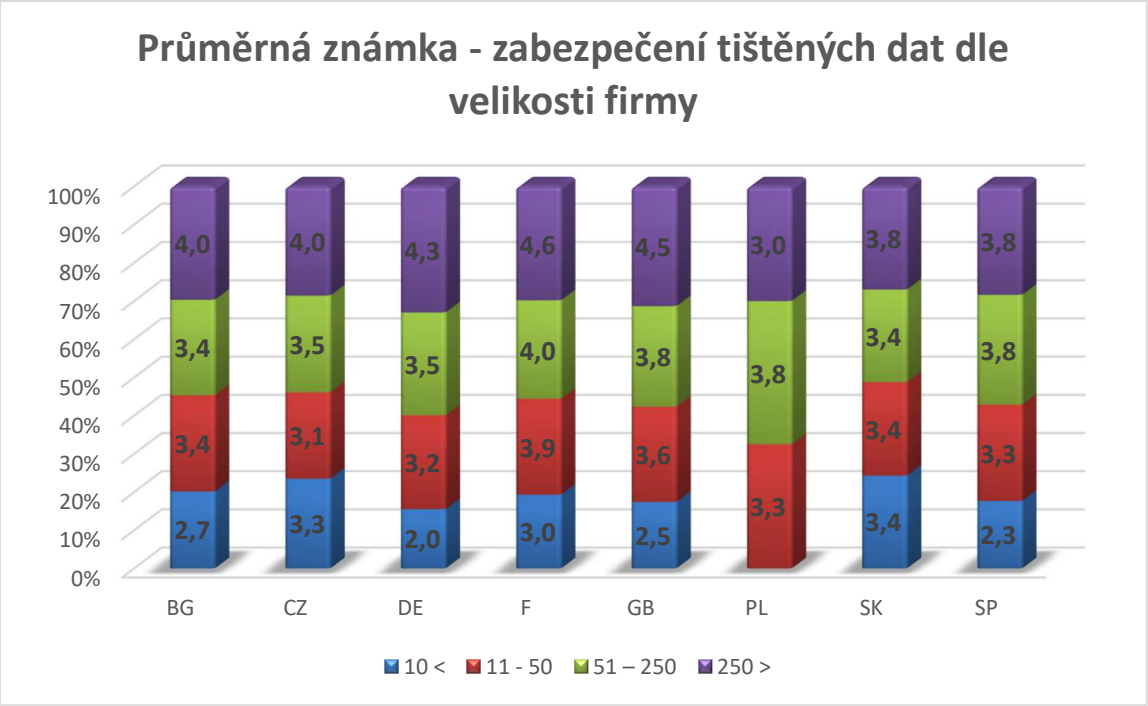
Obrázek 26: Průměrná známka zabezpečení elektronických dat
Zdroj: Vlastní zpracování

Další otázka se také zaměřila na bezpečnost dat, ale tentokrát tištěných, jako příklad byla uvedena: uzamčená skříň, zásuvka, politika čistého stolu. U tištěných dat je průměrná známka výrazně nižší neboli vzorkovaní vnímají zabezpečení tištěných dat na výrazně nižší úrovni. Zatímco průměrná známka definující zabezpečení elektronických dat byla 4,2, průměrná známka definující zabezpečení tištěných dat je 3,6, tedy o 1,4 bodu nižší výsledek. Z pohledu jednotlivých zemí vykazuje nejvyšší průměrnou známku Francie (4,3), což je o pouhých 0,2 méně, než tatáž země vykázala u zajištění elektronických dat. Na dalším místě je Velká Británie (3,7), s rozdílem -0,5 bodu proti zajištění elektronických dat, na další pozici je Česká republika a Polsko (3,5). U České republiky je rozdíl zajištění elektronických dat vs. tištěných dat -0,6 bodu a u Polska -0,7 bodu.



Obrázek 27: Průměrná známka zabezpečení tištěných dat
Zdroj: Vlastní zpracování

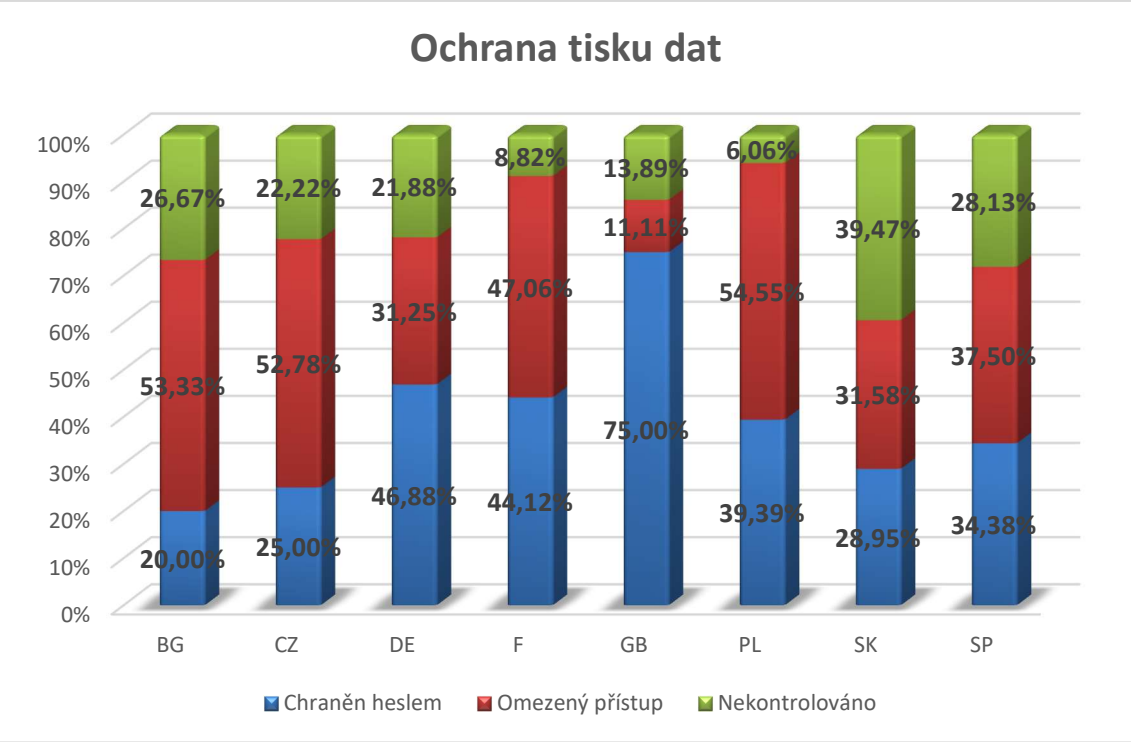
Zajímavý pohled také nabízí variabilita průměrných známek z pohledu velikosti firmy. Nejvyšší celkovou průměrnou známku 4,2 vykazují velké firmy (s více než 250 zaměstnanci), zatímco malé a střední firmy vykazují známku 3,5. Naopak známka mikro firem je 3,0. Níže uvedený graf prezentuje detailní hodnocení dle jednotlivých zemí v závislosti na velikosti firmy.



Obrázek 28: Průměrná známka zabezpečení tištěných dat dle velikosti firmy
Zdroj: Vlastní zpracování

Výstupem této otázky je zjištění, že respondenti vnímají vyšší zabezpečení u elektronických dat, než je tomu u tištěných dat. Tištěná data jsou méně chráněná, a tak citlivá na případný únik dat. Mikro firmy vnímají zabezpečení svých tištěných dat nejhůře. Z praktického hlediska to znamená, že velké firmy investují např. do uzamykatelných skříní, řízené archivace, zatímco mikro firmy nemají prostor nebo finance na zvýšení bezpečnosti tohoto segmentu dat.

S tištěnými daty úzce souvisí zabezpečení tisku, které mapovala následující otázka zabývající se tiskem dokumentů. Vzorkovaným byly nabízeny tři typy odpovědí: (1) tisk je chráněn heslem, (2) realizován na tiskárnu s omezeným přístupem, (3) tisk je nechráněný. Celkem 78,83 % vzorkovaných uvedlo, že tisk je chráněn heslem (37,79 %), nebo je tisk realizován na tiskárně s omezeným přístupem (41,04 %). Naopak nekontrolovaný tisk uvedlo 21,17 % respondentů. Nekontrolovaný tisk má nejvyšší zastoupení na Slovensku (39,47 %) a ve Španělsku (28,13 %). Naopak nejvíce chráněný tisk, tedy heslem, vykazuje Velká Británie (75 %).

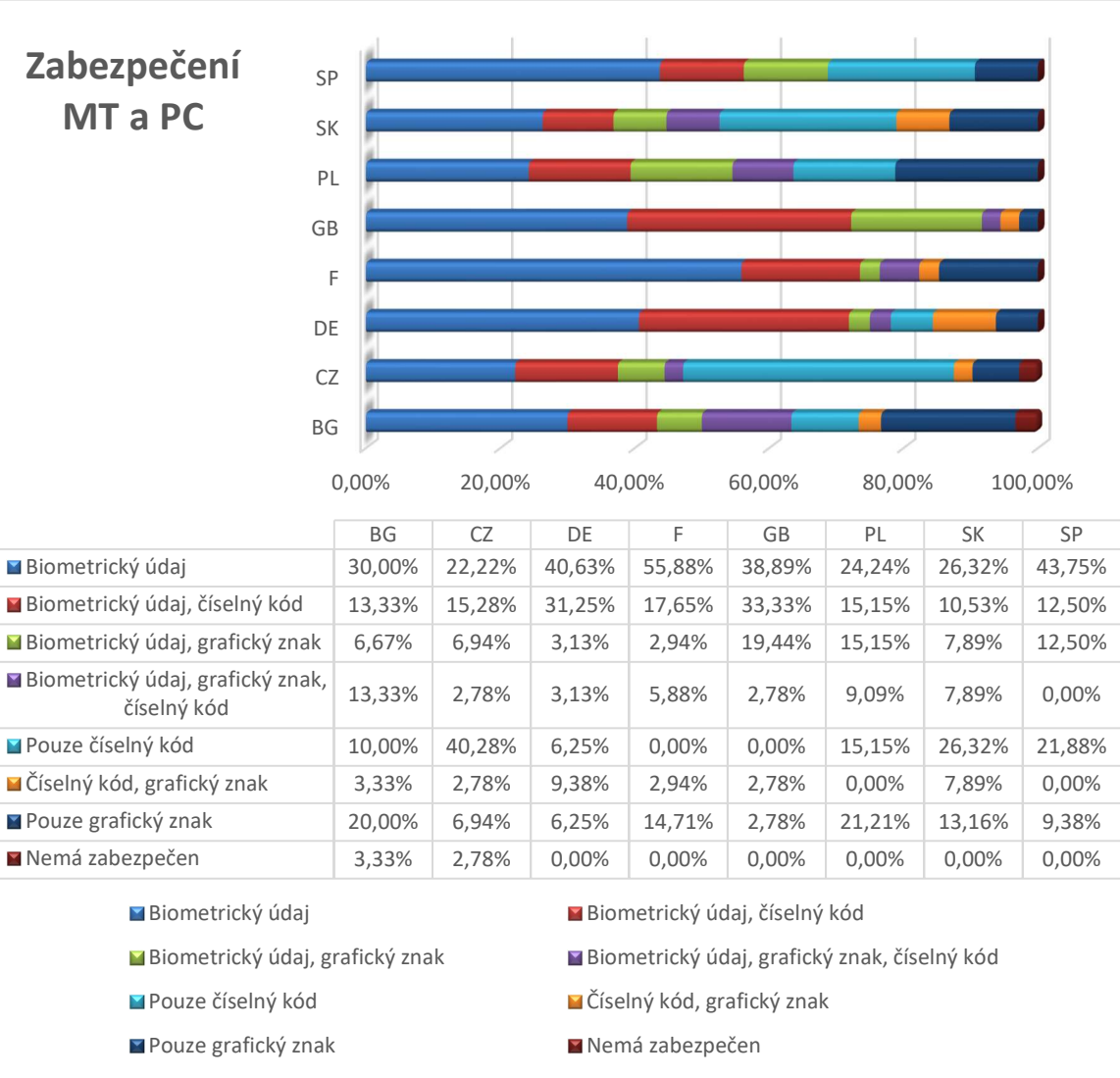


Obrázek 29: Ochrana tisku dat
Zdroj: Vlastní zpracování

Z pohledu velikosti firem tvoří stejný procentní podíl z celkového počtu nekontrolovaného tisku mikro firmy (36,92 %) a malé firmy (36,92 %), střední firmy jsou na druhém místě (21,54 %) a na třetím místě kupodivu i velké firmy (4,62 %). Nejvyšší podíl firem je ze sektoru podnikání e-shop (35,38 %).

Pod zabezpečením dat si lze představit širokou škálu více či méně účinných nástrojů. Dotazníkové šetření se zaměřilo alespoň na některé z nich. Vzorkovaní byli konfrontováni s otázkou, jak je zabezpečen jejich přístup na mobilní telefon a počítač. Pouze 3 respondenti uvedli, že přístup na jejich mobilní telefon ani počítač není zabezpečen, zbylí respondenti uvedli kombinaci různých bezpečnostních prvků, které byly v odpovědích definovány. Grafické znázornění dat je prezentováno grafem č, 30. Nejčastěji bývají data zabezpečena biometrickým údajem a číselným kódem, daleko méně je používán grafický znak. Biometrický údaj používá průměrně 25 respondentů z každé země, obvykle v kombinaci s číselným kódem, nebo grafickým znakem. V České republice je velmi významné používání pouze číselného kódu, ve Francii biometrický údaj. Uvedená data dokazují, že respondenti nepodceňují zabezpečení přístupu do mobilního telefonu a počítače a nejčetněji

využívají jedinečný kód v podobě biometrického údaje a biometrického údaje v kombinaci s číselným kódem, nebo s grafickým znakem.



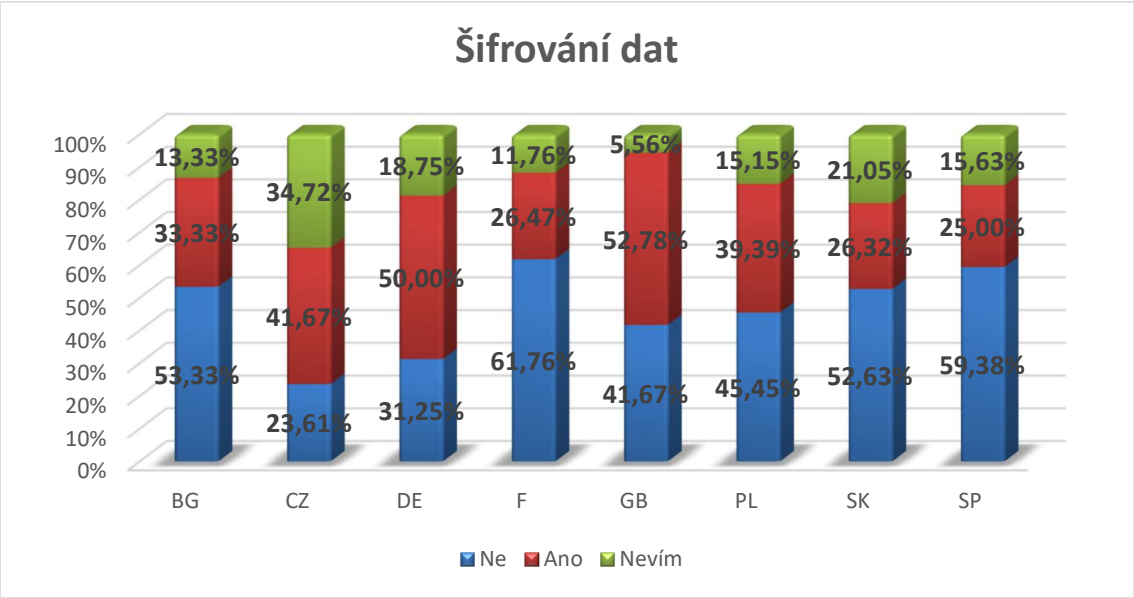
	BG	CZ	DE	F	GB	PL	SK	SP
Biometrický údaj	30,00%	22,22%	40,63%	55,88%	38,89%	24,24%	26,32%	43,75%
Biometrický údaj, číselný kód	13,33%	15,28%	31,25%	17,65%	33,33%	15,15%	10,53%	12,50%
Biometrický údaj, grafický znak	6,67%	6,94%	3,13%	2,94%	19,44%	15,15%	7,89%	12,50%
Biometrický údaj, grafický znak, číselný kód	13,33%	2,78%	3,13%	5,88%	2,78%	9,09%	7,89%	0,00%
Pouze číselný kód	10,00%	40,28%	6,25%	0,00%	0,00%	15,15%	26,32%	21,88%
Číselný kód, grafický znak	3,33%	2,78%	9,38%	2,94%	2,78%	0,00%	7,89%	0,00%
Pouze grafický znak	20,00%	6,94%	6,25%	14,71%	2,78%	21,21%	13,16%	9,38%
Nemá zabezpečen	3,33%	2,78%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%

Obrázek 30: Zabezpečení přístupu na mobilního telefon a počítač
Zdroj: Vlastní zpracování

5.3.8 Šifrování dat

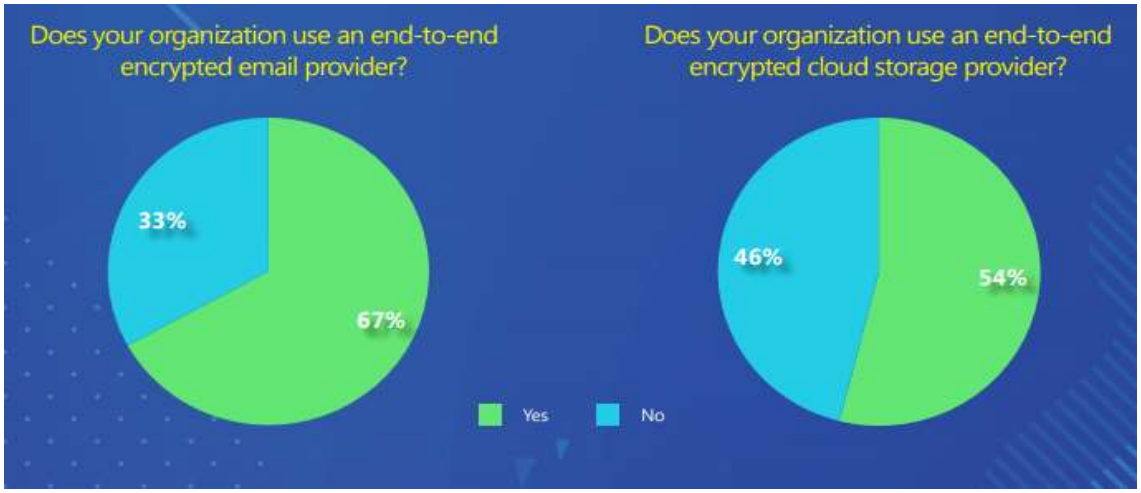
Kryptografie neboli šifrování nabízí další účinnou ochranu dat. Proto další blok otázek cílil právě na tuto oblast. Z celkového počtu vzorkovaných celkem 37,46 % potvrdilo, že jsou data v jejich počítači nebo mobilním telefonu jsou šifrovaná, 43,32 % uvedlo, že data šifrovaná nejsou a 19,22 % neznalo na tuto otázku odpověď. Premisa, že šifrování bude možné dále specifikovat dle velikosti firmy nebo oboru podnikání firmy, nebyla potvrzena. Rozložení respondentů je v rámci oblastí

rovnoměrné. Níže prezentovaná vizualizace dat prokazuje, že šifrování dat nejvíce využívá Velká Británie (52,78 %) a Německo (50 %).



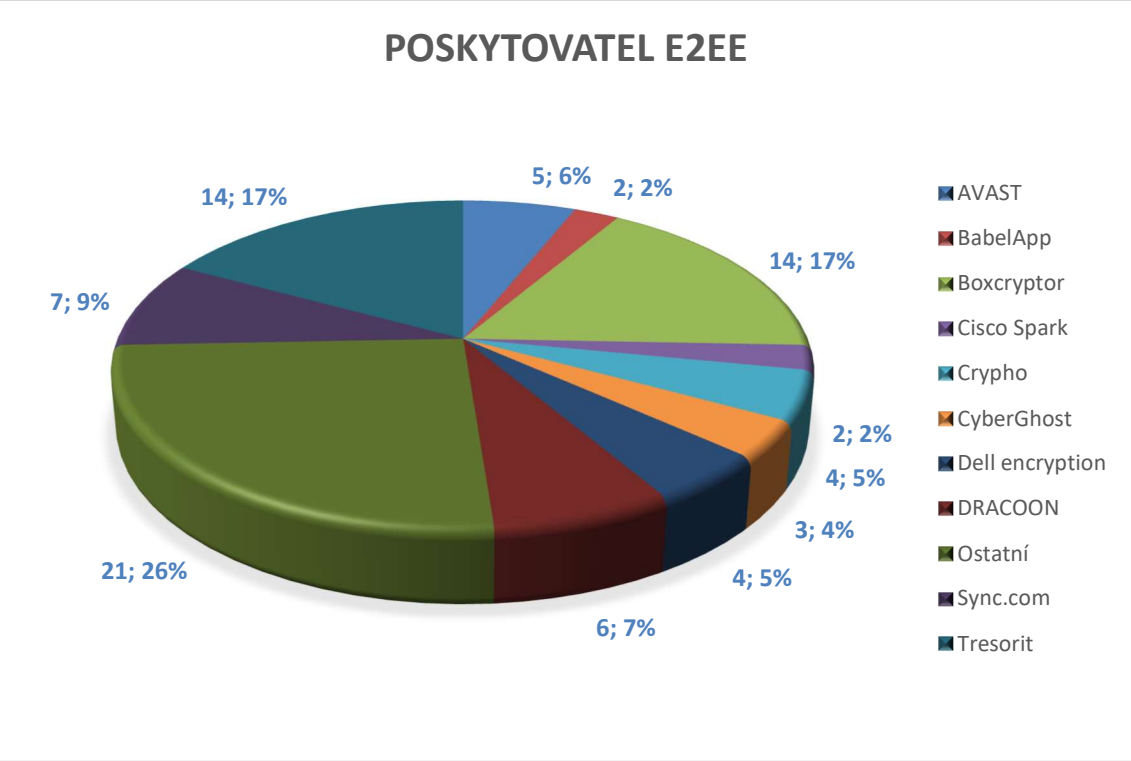
Obrázek 31: Šifrování dat
Zdroj: Vlastní zpracování

Navazující otázka zjišťovala, zda firma používá end–to–end šifrování (dále E2EE). Tuto skutečnost potvrdilo 103 respondentů, tedy 33,55 %, což je podstatně menší hodnota, než vykázal GDPR Survay, které uvádí hodnotu 67 % pro šifrování e-mailů, 54 % pro cloudová uložiště, např. Atento, E2E Global Lines, SkyGuard, Symantec atd. Celkem 17 respondentů uvedlo, že jméno poskytovatele neznají.



Obrázek 32: GDPR Survay: Použití E2EE v organizaci
Zdroj: GDPR.eu, 2019

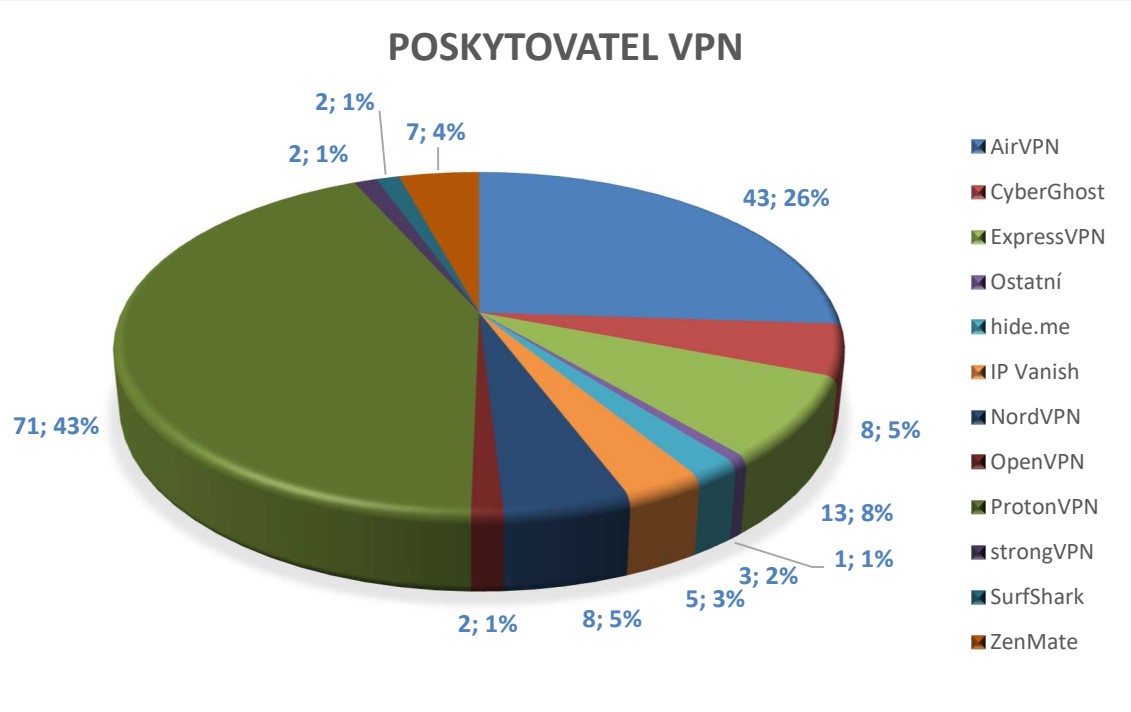
Vyhodnocení dle zemí je nevypovídající, roztříštěnost dat je příliš vysoká a četnost tak minimální. Úkolem respondentů bylo uvést jméno poskytovatele E2EE. Otázka nabízela konkrétní jména poskytovatelů, které uvádí ÚOOU jako spolehlivé a v případě, že v uvedené nabídce odpovědí nebylo jméno jejich poskytovatele uvedeno, mohli jej vepsat do otevřené odpovědi. Tresorit je cloudové uložiště definované ÚOOU jako bezpečné a je také druhou nejčastější odpovědí respondentů. Většina vzorkovaných ovšem využila volnou odpověď, která ukázala, že variabilita využívaných poskytovatelů, je vysoká. Nejčastěji uváděným poskytovatelem je Boxcryptor, zmíněný Tresorit, dále Dracoon, Crypho. Ve skupině „ostatní", jsou uvedeny jména poskytovatelů, které se v odpovědích objevily pouze jednou.



Obrázek 33: Poskytovatel E2EE
Zdroj: Vlastní zpracování

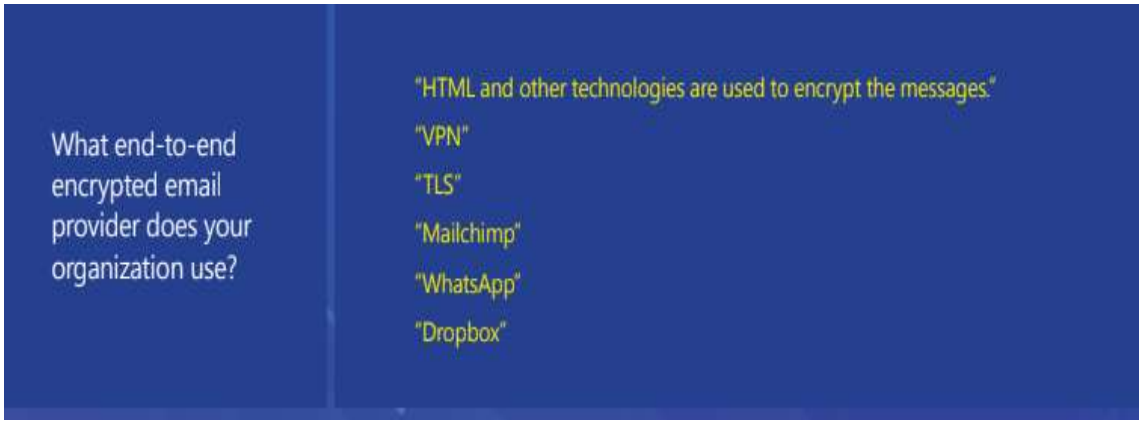
Zjišťovaným faktem byla také jména poskytovatelů VPN, e-mailové komunikace, teamové spolupráci a firemní komunikace. Odpovědi otázek opět reflektovaly doporučené bezpečné poskytovatele, které uvádí ÚOOU a nabízely i možnost otevřené odpovědi. Na otázku týkající se poskytovatele VPN odpovědělo pouze 105 respondentů, tedy třetina, ostatní uvedli, že VPN nepoužívají, nebo jméno

poskytovatele neznají, vyhodnocení dle zemí není vypovídající stejně, jako u předchozích dvou otázek. Nejčastěji uváděným poskytovatelem VPN je ProtonVPN (43 %), který ÚOOU řadí mezi spolehlivé poskytovatele [GDPR.eu, e, 2019], na druhém místě je Air VPN (26 %), také VPN řazena ÚOOU mezi bezpečné a na třetím místě Express VPN (13,8 %).



Obrázek 34: Poskytovatel VPN
Zdroj: Vlastní zpracování

Otázky z oblasti E2EE potvrzují premisu deklarovanou GDPR Survay, tedy že uživatelé nemají povědomí o poskytovatelích E2EE. Pokud budeme hovořit o konkrétních číslech GDPR Survay, dvě třetiny respondentů uvedli, že používají E2EE pro e-mailovou komunikaci, ale pouhých 9 % z nich dokázalo uvést jméno poskytovatele, který E2EE skutečně poskytuje [GDPR.eu, 2019]. Stejný výzkum se také dotazoval na poskytovatele cloudového uložiště používajícím E2EE. Přibližně polovina vzorkovaných potvrdila, že takového poskytovatele mají a jako příklad uvedla nejčastěji Google, iCloud, Microsoft, Amazon, ale zároveň opět uvedli i nesmyslné poskytovatele jako např. Reddit, což je poskytovatel sociální sítě v Irsku [GDPR.eu, 2019]. Neznalost vzorkovaných dokazuje obrázek níže, kde měli uvést jméno poskytovatele E2EE e-mailové komunikace [GDPR.eu, 2019].

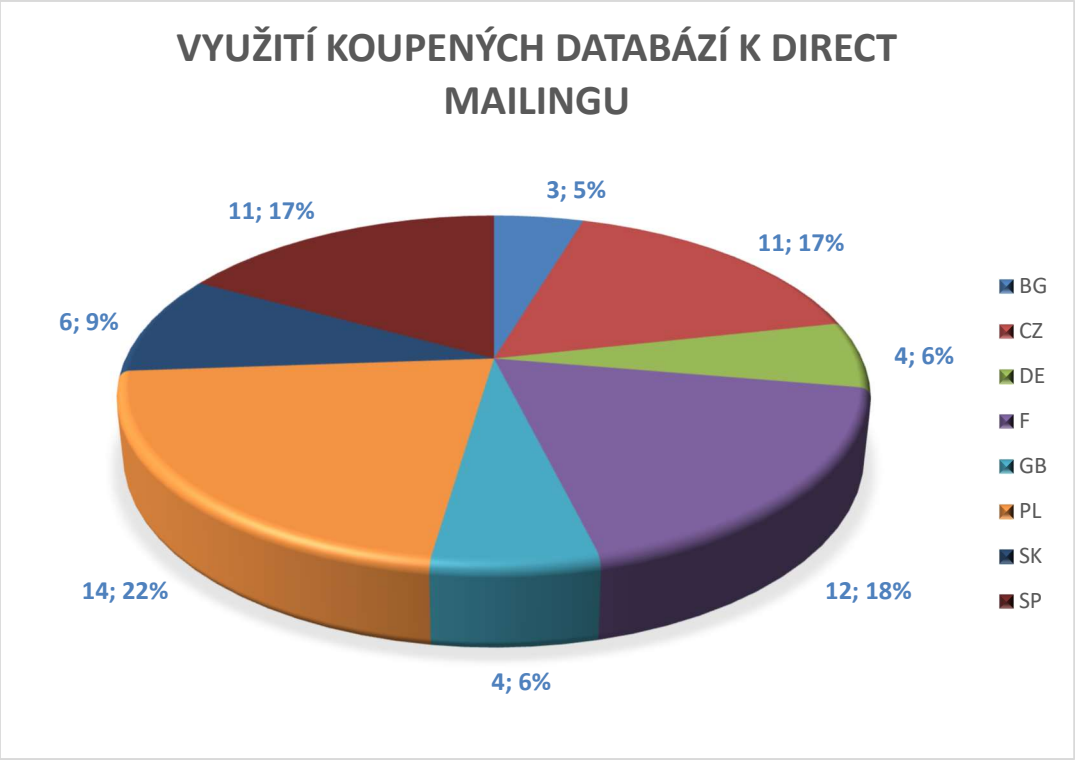


Obrázek 35: Poskytovatel E2EE pro e-mail
Zdroj: GDPR.eu, 2019

Respondenti dotazníkového šetření diplomové práce uvedli jako poskytovatele e-mailové služby Microsoft Outlook (171), Gmail (27), ProtonMail (27), Zoho Mail (11) a HushMail (10). Pod hranicí 10 respondentů je diverzifikace poskytovatelů vysoká, jako příklady lze uvést: 1&1, Mailfance, Thunderbird, T-Online, Yohoo! či Lotus. V souvislosti s e-mailovou komunikací je nutno také uvést, že celkem 19 respondentů uvedlo, že při hromadném zasílání e-mailů zákazníkům či dodavatelům jsou e-mailové adresy viditelné v adresáři e-mailu, což je pochybení proti pravidlům GDPR.

Závažnějším pochybením představuje využívání kontaktů ze zakoupených databází, jehož používání uvedlo 19 % respondentů. Jak na svých stránkách uvádí ÚOOU, je vysoce nepravděpodobné, že by kontakty nějaké databáze udělily takovýto konkrétní souhlas a obecný souhlas zahrnující více oblastí nelze použít [ÚOOU, a, 2019]. Jako příklad sankcionované firmy za toto pochybní může být Zaplo Finance s.r.o., které byla vyměřena pokuta ve výši 36 tis. Kč [ÚOOU, a, 2019]. Celkem 19 z nich také uvedlo, že v e-mailu není uveden odkaz pro odhlášení z rozesílky.

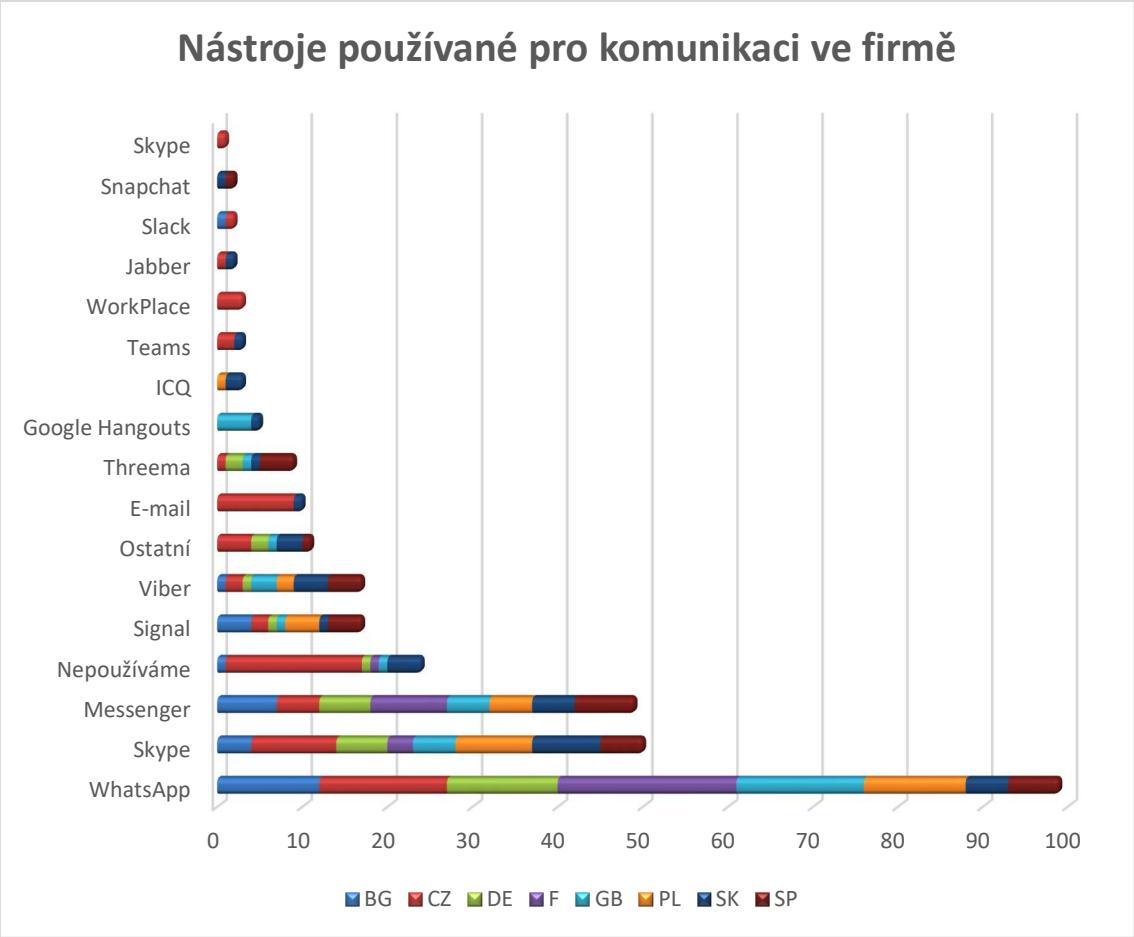
Používání kontaktů ze zakoupených databází, v kombinaci neuvedením odkazu na odhlášení z rozesílky, je velké pochybení proti legislativě GDPR. Této kombinace dosáhla nejvyšší četnosti Francie (12) a Bulharsko (3).



Obrázek 36: Využití koupených databází k direct mailingu
Zdroj: Vlastní zpracování

Vyšší erudovanosti v přehledu poskytovatelů se podařilo dosáhnout otázkou týkající se používaných nástrojů pro komunikaci ve firmě. Zde mají vzorkovaní poměrně jasno, ačkoliv 24 z nich uvedlo, že nepoužívají nástroje pro komunikaci ve firmě. Nejvíce používaným nástrojem je jednoznačně aplikace WhatsApp, dále Skype a Messenger. Nutno připomenout, že aplikace WhatsApp, Signal a Threema jsou ÚOOU uvedeny mezi bezpečnými poskytovateli [GDPR.eu, e, 2019]. V položce ostatní jsou zahrnuty komunikační nástroje s četností menší než 2, např. Free Conference, Mattermost, MS Teams, Toop Messenger.

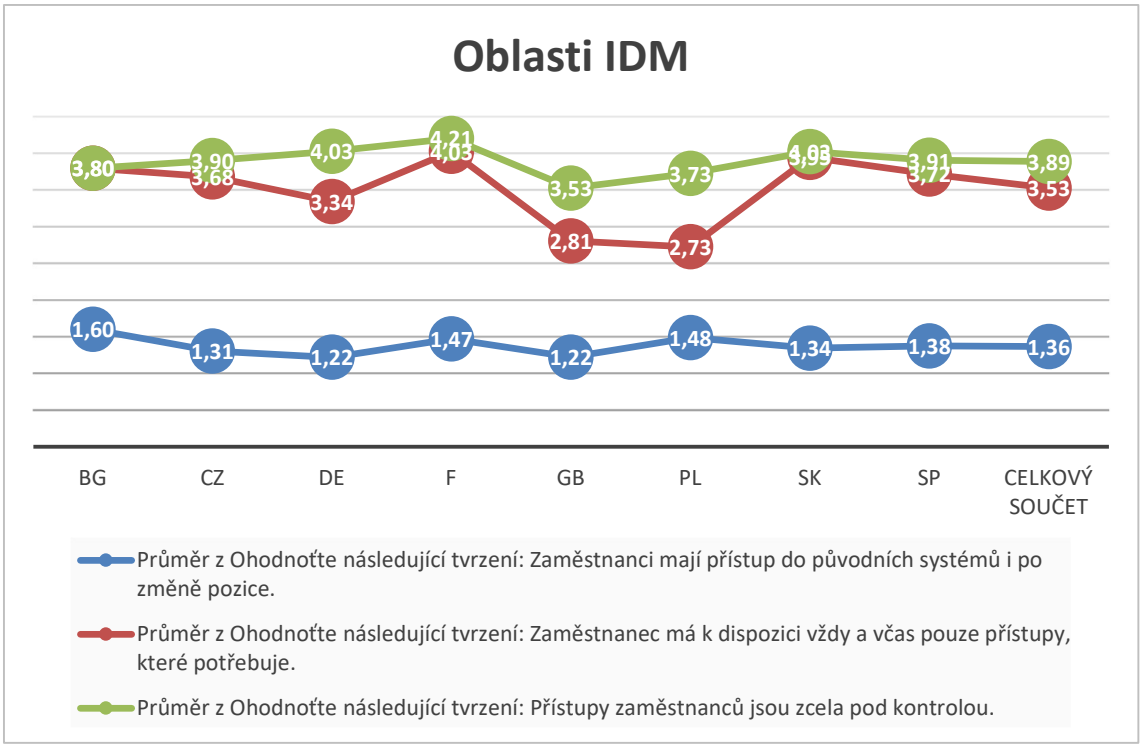
Nejvíce používaným nástrojem pro vzájemnou spolupráci, ať už z pohledu řízení projektu, komunikace, týmové spolupráce apod., je nástroj Trello, který používá 42 respondentů napříč zeměmi, dále Wire (40), Capterra (21) a Slack (17). 98 uživatelů uvedlo, že tyto nástroje nepoužívají a četnost u zbývajících je minimální, jako příklad lze uvést nástroje: Asana, Atlassian, Freelo, redPen, Teams, JIRA. Z uvedené skupiny nástrojů je Wire deklarován jako bezpečný [GDPR.eu, e, 2019].



Obrázek 37: Nástroje používané pro komunikaci ve firmě
Zdroj: Vlastní zpracování

5.3.9 Přístupy IDM

Podnikatelský subjekt musí ochránit data zákazníků nejen proti vnějším, ale také vnitřním vlivům. Zaměstnanci by měli mít vždy pouze přístup odpovídající jejich pracovním potřebám. Velkorysé udělování práv všem představuje vysokou hrozbu, a naopak velmi omezené přístupy často paralyzují chod firmy. Přístupy k datům a obecně do systémů, jsou problematikou velkých korporací, kde proces udělení přístupu od samotného podání požadavku, po přidělení přístupu, nebo naopak odebrání, je velmi zdlouhavý. Uživatelé tak na přístup čekají nebo ho mají ještě nějaký čas po změně pozice. Několik otázek bylo zaměřeno právě na tuto problematickou oblast. Respondent zvolil pro každou otázku odpověď odpovídající míře souhlasu či nesouhlasu, při čemž 1 značila odpověď „ne“ a 5 naopak hodnotu „ano“. Graf níže prezentuje výsledná data.

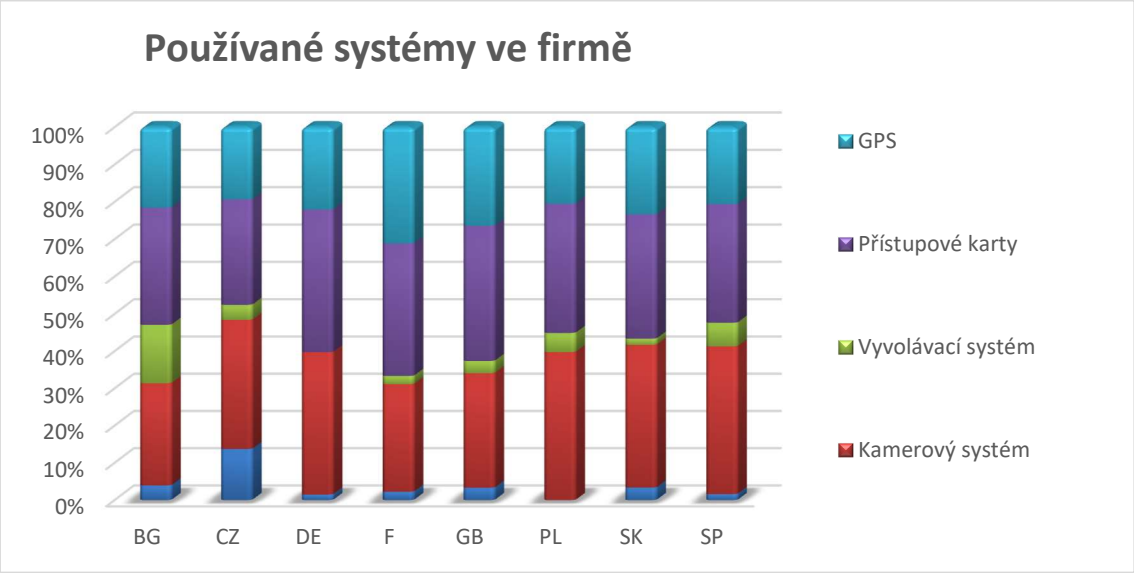


Obrázek 38: Oblasti IDM
Zdroj: Vlastní zpracování

Premisa, že u první otázky, která ověřovala skutečnost, zda mají zaměstnanci přístup do původních systémů i po změně pozice, bude převažovat hodnota 1, se ukázala jako chybná. Celková průměrná hodnota je 1,36. Všechny průměrné hodnoty zemí přesahují číslo 1, tzn. firmy v této oblasti vykazují pochybení. Nejvyšší průměrná známka je u Bulharska (1,6), Polska (1,48), Francie (1,47). Naopak nejnižší hodnoty jsou u Německa a Velké Británie, kde průměrná hodnota dosahuje 1,22. Nejvyšších hodnot dosahují malé (1,43) a velké firmy (1,41). U další otázky respondent vyhodnocoval, zda mají zaměstnanci k dispozici vždy a včas pouze přístupy, které potřebují. Zde celková průměrná hodnota respondentů dosahuje známky 3,53, tzn. spíše souhlasí, ale pod hodnotou 3 se pohybují 2 země: Velká Británie (2,81) a Polsko (2,73). Na úrovni počtu zaměstnanců dosahují nejvyšší průměrné známky velké firmy (4,21), ostatní průměrné známky firem vykazují minimální rozptyl. Poslední otázka zjišťovala obecný pohled, zda jsou přístupy zaměstnanců zcela pod kontrolou, kdy výsledná známka byla 3.6. Jak je evidentní, u většiny zúčastněných států, odpovědi těchto otázek spolu korelují, kromě Velké Británie a Polska. Příčinou může být časová prodleva pro udělení přístupu. Nejvyšší známky v této oblasti dosahují mikro firmy (3,94) a velké firmy (3,74).

5.3.10 Používané systémy ve firmě

Oblast výzkumu byla také zaměřena na systémy používané firmou, typu GPS ve vozidlech, přístupové karty, kamerové systémy apod. Tyto systémy lez používat a využívat bez souhlasu zaměstnance, neboť se jedná o zákonný právní důvod zpracování dat, pokud jsou dodrženy podmínky definované GDPR [GDPR.eu, e, 2019].



Obrázek 39: Používané systémy ve firmě
Zdroj: Vlastní zpracování

Např. monitorování GPS musí být adekvátní, tedy náhodná kontrola např. dodržování trasy, plánovaných schůzek, nikoliv každodenní stalking zaměstnance. Stejně tak kamerové systémy mají sloužit k zajištění bezpečnosti zaměstnanců na pracovišti, ochraně majetku a nesmějí být zneužity. Naopak je tomu u docházkových systémů, kdy je použit biometrický údaj zaměstnance, např. otisk prstu. Zde musí mít zaměstnavatel výslovný souhlas zaměstnance se zpracováním těchto citlivých dat [GDPR.eu, e, 2019]. Dotazníkové šetření ukázalo, že nejpoužívanějšími systémy jsou kamerové systémy a přístupové karty. Souhlas se zpracováním těchto osobních údajů potvrdila více než polovina vzorkovaných (182). Společným jmenovatelem u těchto systémů je informovanost zaměstnance a omezení přístupu k zaznamenaným datům [GDPR.eu, e, 2019]. V případě zneužití dat či nedodržení podmínek, hrozí právnímu subjektu sankce [GDPR.eu, e, 2019]. Zaměstnanec má kdykoliv právo vyžádat si náhled na zpracovávaná data.

6 Vyhodnocení zjištěných parametrů zemí

Tato kapitola se věnuje vyhodnocení dat dle jednotlivých zemí, jejíž respondenti se zúčastnili dotazníkového šetření. Země byly rozděleny do pomyslných dvojic, na základě ekonomických dat a počtu obyvatel, viz tabulka 14. Cílem je prokázat, zda vytvořené dvojice zemí dosahují podobných výsledků. Samotná data určená pro analýzu byla rozdělena do dvou sekcí. První sekce vyhodnocuje soulad jednotlivých subjektů s GDPR, tedy zabezpečenosti dat a proškolení zaměstnanců. Druhý blok je zaměřen na fyzické osoby, tedy respondenty a jejich znalosti z oblasti GDPR a také subjektivní vnímání GDPR.

Tabulka 3: Základní ekonomické ukazatele vybraných zemí EU

Země		Počet respondentů	Počet obyvatel 2019	Tempo růstu HDP - roční změna (2017)	Nezaměstnanost 2019	Míra roční inflace k 2019
CZ		72	10,6 mil.	4,30%	2,20%	2,60%
PL		33	38 mil.	3,60%	3,80%	2,10%
SP		32	47 mil.	3,10%	14,90%	0,80%
F		34	67 mil.	1,80%	8,80%	1,30%
DE		32	83 mil.	2,20%	3,30%	1,40%
GB		36	66,6 mil.	1,80%	3,80%	1,80%
BG		30	7 mil.	3,60%	5,10%	2,50%
SK		38	5,5 mil.	3,40%	6,40%	2,80%

Zdroj: Eurostat, 2020

6.1 Soulad subjektů s GDPR

Metodika zpracování dat této kapitoly je popsána v kapitole 3.2. Pro posouzení byla vybrána následující data:

- Procento proškolených zaměstnanců;
- Obecné zabezpečení dat;

- Zabezpečení elektronických dat;
- Zabezpečení tiskových dat;
- Kontrola tisku;
- Zabezpečení přístupu na mobilní telefon a počítač;
- Šifrování dat.

V tabulce č. 3 jsou uvedeny hodnoty jednotlivých otázek zemí a v tabulce č. 4 výsledné pořadí zemí. Barevně jsou označeny dvojice zemí, tak jak byly definovány v tabulce č. 2.

Tabulka 4: Vykázané hodnoty jednotlivých otázek

Země	Proškoleno (v %)	Obecné zabezpečení dat (v %)	Zabezpeční el.dat (známka)	Zabezpeční tištěných dat	Kontrolovaný tisk (v %)	Zabezpeční přístup MT a PC (známka)	Šifrování dat (v %)
BG	93,43	46,67	4,2	3,3	73,33	3	33,33
CZ	81,94	63,89	4,1	3,5	77,78	2	41,67
DE	96,87	46,88	4,1	3,4	78,12	1	50
F	97,06	64,71	4,5	4,3	91,18	1	26,47
GB	94,44	91,67	3,9	3,7	86,11	1	52,78
PL	100,00	81,82	4,2	3,5	93,94	1	39,39
SK	86,84	68,42	4,4	3,4	60,53	1	26,32
SP	84,37	56,25	4,5	3,4	71,87	1	25

Zdroj: Vlastní zpracování

Tabulka 5: Výsledné pořadí zemí

Země	Proškoleno (v %)	Obecné zabezpečení dat (v %)	Zabezpeční el.dat (známka)	Zabezpeční tištěných dat	Kontrolovaný tisk (v %)	Zabezpeční přístup MT a PC (známka)	Šifrování dat (v %)	Průměrná známka
PL	1	2	3	3	1	1	4	2,14
F	2	4	1	1	2	1	6	2,43
GB	4	1	5	2	3	1	1	2,43
DE	3	7	4	4	4	1	2	3,57
CZ	8	5	4	3	5	2	3	4,29
SK	6	3	2	4	8	1	7	4,43
SP	7	6	1	4	7	1	8	4,86
BG	5	8	3	5	6	3	5	5,00
Celkem								3,64

Zdroj: Vlastní zpracování

Výsledná průměrná známka evaluovaných zemí je 3,64. Nejlepší průměrnou známku získalo Polsko (2,14), které tvoří dvojici s Českou republiku (4,29). Průměrná známka těchto zemí se liší o propastných 2,15 bodu. Nejvíce skóre České

republiky ovlivnila pozice v oblasti proškolení zaměstnanců, obecné zabezpečení dat a kontrolovaný tisk, které mají nejhorší pozici. Obdobného výsledku dosáhla tato dvojice zemí v oblasti zabezpečení elektronických a tištěných dat, jejich šifrování a také v oblasti zabezpečení přístupu na mobilní telefon a počítač.

Na druhém místě je Francie (2,43), která tvoří dvojici se Španělskem (4,86), které se umístilo na předposlední pozici. I tato dvojice vykazuje výrazný rozdíl průměrných známek 2,4. Španělsko se sice v zabezpečení dat a přístupu do mobilního telefonu a počítače umístilo na první pozici, ovšem u ostatních otázek výrazně zaostává. Podobnost dat lze sledovat u zabezpečení elektronických dat, u zabezpečení přístupu na mobilní telefon a počítač. Ostatní hodnocené oblasti se liší o více než 2 pozice. Na druhé pozici se umístila také Velká Británie (2,43), která tvoří dvojici s Německem (3,57). Rozdíl průměrných známek je pouhých 1,14. Přesto mají obě země několik parametrů umístěných na hroší pozici než 3. U Velké Británie je nejslabší stránkou zabezpečení elektronických dat a proškolení zaměstnanců. U Německa je nejhorší pozice u obecného zabezpečení dat, které se následně prolíná i v otázkách týkající se zabezpečení dat, kde se umístilo na 4. pozici. Naopak podobné umístění lze pozorovat u proškolení zaměstnanců zabezpečení elektronických dat, zabezpečením mobilního telefonu a počítače, zabezpečení tisku a šifrování dat. Poslední dvojice, Slovensko (4,43) a Bulharsko (5,0), vykázala nejhorší průměrné známky, a tedy také umístění. Rozdíl mezi známkami je 0,57. Obdobných pozic dosahují tyto země u proškolených osob a zabezpečení elektronických a tištěných dat. U všech dvojic zemí lze nalézt blízké umístění u některé z otázek, ovšem nelze definovat otázku, kde by se odpovědi dvojic zemí nelišily o více než jednu pozici. Stejně tak celkové skóre prokazuje, že u dvou párů byly výsledky výrazně odlišné, naopak u dalších dvou párů byly hodnoty velmi blízké.

6.2 Subjektivní pohled fyzických osob

Poslední vyhodnocovanou oblastí je osobní pohled respondenta na GDPR, jak ovlivnilo jeho samotného z pohledu zvýšení administrativy v zaměstnání nebo kontroly nad daty a pocitu bezpečnosti. Jedná se o zcela subjektivní pocit, který měl vzorkovaný vyjádřit mírou souhlasu či nesouhlasu na stupnici od jedné do pěti.

Hodnota 1 znamená „ne“, hodnota 5 naopak „ano. Odpovědi vzorkovaných souvisí s osobními zkušenostmi, které vzorkovaní mají, ale nelze jednoznačně stanovit premisu, že největší vliv na ně má právnický subjekt, pro který pracují. Proto je tato oblast vyhodnocována zcela odděleně. Naopak vláda a média mohla vzorkované výrazně ovlivnit, což vedlo k vyhodnocení také v rámci státu. Dotazníkové šetření vygenerovala zajímavá, avšak rozdílná data, a proto byla podrobena hlubší analýze v programu SW STATISTICA. V případě, že bodové ohodnocení otázky hodnotou 4 a 5 přesahuje 50 %, je stanovisko respondentů považováno za odsouhlasené.

6.2.1 GDPR – zvýšení administrativa

První otázka zjišťovala, zda respondent zaznamenal zvýšení administrativy v zaměstnání v souvislosti s GDPR. Maximální uvedená hodnota všech zemí dosahuje hodnoty 5, tedy maximální hranice vyjadřující souhlas. Modus čtyř zemí tvoří hodnota 4 a hodnota 5, jednotlivé četnosti jsou uvedeny v tabulce č. 5 a deklarují, že se jedná o četnosti přesahující často 50 % hranici. Minimum těchto hodnot je ovšem v několika zemích hodnota 1 (odpověď „ne“). Vzorkovaní v České republice, Velké Británii a Slovensku, tedy minimálně v jednom případu uvedli, že jim GDPR nezvýšilo administrativu. Ovšem jejich průměrná známka je větší než 3. Průměrné hodnoty vyšší než 4 vykazuje: Polsko (4,03), Španělsko (4,16) a Bulharsko (4,27).

Tabulka 6: GDPR Vám osobně: Zvýšilo administrativu v zaměstnání (1)

	GDPR Vám osobně: Zvýšilo administrativu v zaměstnání						
Proměnná	Průměr	Poč. plat.	Medián	Modus	Četnost modusu	Minimum	Maximum
BG	4,266667	30	4,500000	5,000000	15	3,000000	5,000000
CZ	3,375000	72	4,000000	5,000000	24	1,000000	5,000000
DE	3,906250	32	4,000000	4,000000	12	2,000000	5,000000
F	3,823529	34	4,000000	4,000000	12	2,000000	5,000000
GB	3,750000	36	4,000000	4,000000	16	1,000000	5,000000
PL	4,030303	33	4,000000	4,000000	20	3,000000	5,000000
SK	3,921053	38	5,000000	5,000000	24	1,000000	5,000000
SP	4,156250	32	4,000000	5,000000	13	2,000000	5,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Největší disperzi hodnot vykazuje Česká republika a Slovensko, kde překračuje hodnotu větší než 2, což potvrzuje minima a maxima hodnot těchto zemí. Pravděpodobnost výskytu hodnot značně nadprůměrných je tedy velmi pravděpodobná. Nejnižší variaci vykazuje Polsko, kde je tedy předpoklad téměř symetrického rovnoměrného rozložení.

Tabulka 7: GDPR Vám osobně: Zvýšilo administrativu v zaměstnání (2)

	GDPR Vám osobně: Zvýšilo administrativu v zaměstnání						
Proměnná	25,000. kvantil	75,000. kvantil	Sm.Odch.	Rozptyl	Průměrná odchylka	Rozsah	Kvartilové rozpětí
BG	4,000000	5,000000	0,827682	0,685057	0,733333	2,000000	1,000000
CZ	2,000000	5,000000	1,505272	2,265845	1,309028	4,000000	3,000000
DE	3,000000	5,000000	0,856074	0,732863	0,685547	3,000000	2,000000
F	3,000000	5,000000	0,999108	0,998217	0,816609	3,000000	2,000000
GB	3,000000	4,000000	1,024695	1,050000	0,777778	4,000000	1,000000
PL	4,000000	4,000000	0,636634	0,405303	0,411387	2,000000	0,000000
SK	3,000000	5,000000	1,633791	2,669275	1,375346	4,000000	2,000000
SP	4,000000	5,000000	0,846601	0,716734	0,685547	3,000000	1,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

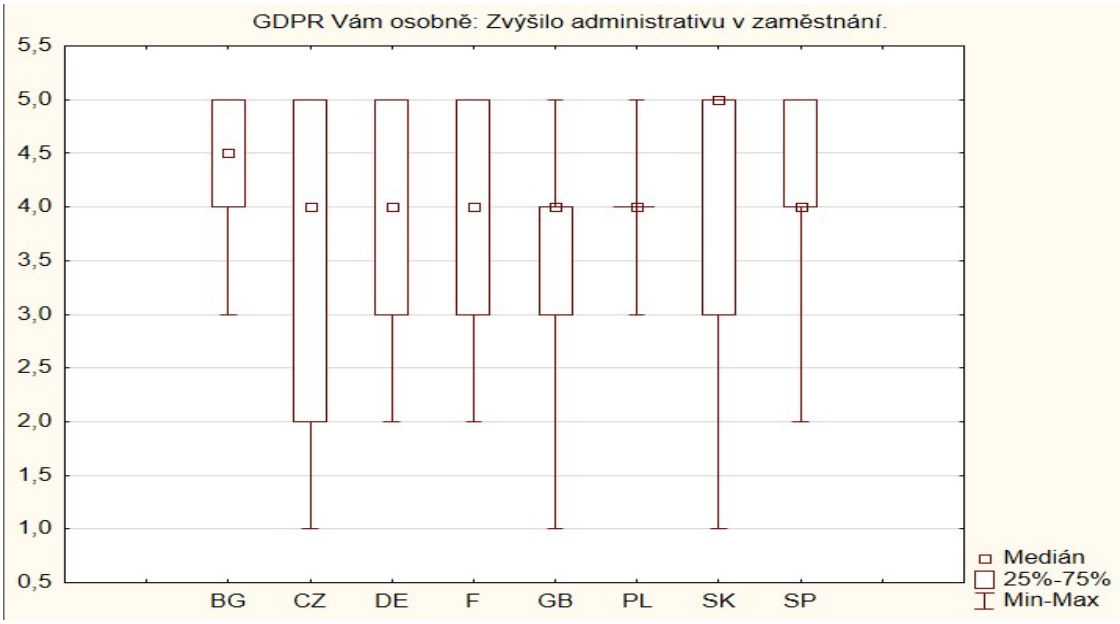
Součet bodů není směrodatným ukazatelem, neboť počet respondentů jednotlivých zemí je odlišný, a tedy nejvyšší skóre u České republiky neznamená, že většina respondentů vyjádřila vyšší míru souhlasu se zvýšenou administrativou. Ale srovnání je možné např. u Německa (125) a Španělska (133), kde je počet respondentů totožný a lze tedy uvést, že obyvatelé Španělska více vnímají zvýšenou administrativu. Záporné hodnoty charakteristiky šikmosti predikují, že jsou pravděpodobné podprůměrné hodnoty.

Tabulka 8: GDPR Vám osobně: Zvýšilo administrativu v zaměstnání (3)

	GDPR Vám osobně: Zvýšilo administrativu v zaměstnání		
Proměnná	Šikmost	Špičatost	Součet
BG	-0,55139	-1,31278	128,0000
CZ	-0,41532	-1,23088	243,0000
DE	-0,14172	-0,92040	125,0000
F	-0,39946	-0,84627	130,0000
GB	-0,98059	1,22262	135,0000
PL	-0,02320	-0,33101	133,0000
SK	-1,12249	-0,50619	149,0000
SP	-0,65423	-0,34603	133,0000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Závěrem je, že všechny země pociťují zvýšení administrativy v zaměstnání v návaznosti na GDPR, což potvrzují data všech zemí, kdy 67 % respondentů hodnotilo otázku známkou 4, nebo 5. Celková průměrná známka je 3,78 z maximálních 5 bodů a pohybuje v intervalu 3,38 – 4,27. Vyjádření, že zvýšení administrativy vzorkovaní nepociťují, je ve výši 7,8 %. Data dokresluje krabicový graf.



Obrázek 40: GDPR Vám osobně: Zvýšilo administrativu v zaměstnání
Zdroj: Vlastní zpracování v programu SW STATISTICA

6.2.2 GDPR – hrozby a rizika úniku a zneužití dat

Druhá otázka prověřovala, zda GDPR poukázalo na hrozby a rizika úniku a zneužití dat, kterou 53,4 % ohodnotilo známkou 4, nebo 5 a 3,78 % nejnižší známkou 1.

Tabulka 9: GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat (1)

Proměnná	GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat						
	Průměr	Poč. plat.	Medián	Modus	Četnost modusu	Minimum	Maximum
BG	3,066667	30	3,000000	4,000000	10	1,000000	5,000000
CZ	3,055556	72	3,000000	4,000000	17	1,000000	5,000000
DE	3,593750	32	4,000000	4,000000	14	2,000000	5,000000
F	3,882353	34	4,000000	4,000000	25	2,000000	5,000000
GB	3,861111	36	4,000000	4,000000	12	1,000000	5,000000
PL	3,606061	33	4,000000	4,000000	21	2,000000	4,000000
SK	2,947368	38	3,000000	3,000000	11	1,000000	5,000000
SP	3,375000	32	3,000000	3,000000	11	1,000000	5,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Modus dat má jednotnou podobu hodnoty 4, kromě Slovenska (3) a Španělska (3). Minima dosahují hodnoty 1, maxima hodnoty 5 a dosahují ho všechny země, kromě Polska (4). Téměř jednohlasný verdikt vykazuje Francie, u které je rozptyl 0,35 a průměrná odchylka 0,37, což potvrzuje první i třetí kvartil s hodnotou 4. Četnost modu 4 je 25, při čemž celkový počet dotazníků je 34. Vzorkovaní z Francie se tedy shodují, že GDPR poukázalo na hrozby a rizika úniku a zneužití dat. Totéž stanovisko lze připisat i respondentům z Polska, kde rozptyl 0,31 a směrodatná odchylka 0,56; s modem 4 při četnosti 21 z celkového počtu 33 dotazníků.

Tabulka 10:GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat (2)

	GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat						
Proměnná	25,000. kvantil	75,000. kvantil	Sm.Odch.	Rozptyl	Průměrná odchylka	Rozsah	Kvartilové rozpětí
BG	2,000000	4,000000	1,337350	1,788506	1,137778	4,000000	2,000000
CZ	2,000000	4,000000	1,452428	2,109546	1,256173	4,000000	2,000000
DE	3,000000	4,000000	0,837021	0,700605	0,707031	3,000000	1,000000
F	4,000000	4,000000	0,591080	0,349376	0,370242	3,000000	0,000000
GB	3,000000	5,000000	0,990030	0,980159	0,788580	4,000000	2,000000
PL	3,000000	4,000000	0,555619	0,308712	0,501377	2,000000	1,000000
SK	2,000000	4,000000	1,272312	1,618777	1,016620	4,000000	2,000000
SP	3,000000	4,000000	1,184578	1,403226	0,984375	4,000000	1,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Šikmost České republiky se blíží nule, což značí zcela symetrickou křivku. Naopak hodnoty Polska vykazují nejvzdálenější rozložení hodnot pod průměrem. Nejvyšší špičatost vykazuje Francie s hodnotou 2,74.

Tabulka 11: GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat (3)

	GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat		
Proměnná	Šikmost	Špičatost	Součet
BG	-0,22215	-1,18300	92,0000
CZ	-0,09917	-1,36808	220,0000
DE	-0,13993	-0,38255	115,0000
F	-0,91604	2,74353	132,0000
GB	-0,64251	0,38113	139,0000
PL	-1,02937	0,11603	119,0000
SK	-0,14596	-0,96933	112,0000
SP	-0,17854	-0,69688	108,0000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Navzdory nejnižším hodnotám Slovenska, je verdikt této otázky opět jednoznačný, vzorkovaní usuzují, že GDPR poukázalo na hrozby a rizika úniku a zneužití jejich dat.

Obrázek 41: GDPR Vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat
Zdroj: Vlastní zpracování v programu SW STATISTICA

6.2.3 GDPR – zvýšení pocitu kontroly nad osobními daty

Předposlední otázka zjišťovala, zda GDPR samotným vzorkovaným zvýšilo pocit kontroly nad jejich osobními údaji. A tato otázka přinesla diverzifikaci odpovědí. Hodnocení známkou 4, nebo 5 uvedlo 49 %. Minimem 1 ohodnotilo odpověď celkem 11 % vzorkovaných. Zatímco nejvyšší pocit kontroly přineslo GDPR vzorkovaným z Německa, což dokazuje průměr 3,94; četnost 16 u modu 4 a nízká hodnotu variace 0,51.

Tabulka 12: GDPR Vám osobně: Zvýšilo pocit kontroly nad Vašimi osobními údaji (1)

Proměnná	GDPR Vám osobně: Zvýšilo pocit kontroly nad vašimi osobními údaji						
	Průměr	Poč. plat.	Medián	Modus	Četnost modusu	Minimum	Maximum
BG	3,166667	30	4,000000	4,000000	10	1,000000	5,000000
CZ	2,736111	72	3,000000	3,000000	22	1,000000	5,000000
DE	3,937500	32	4,000000	4,000000	16	3,000000	5,000000
F	3,882353	34	4,000000	4,000000	21	2,000000	5,000000
GB	3,972222	36	4,000000	5,000000	13	1,000000	5,000000
PL	3,393939	33	4,000000	4,000000	18	2,000000	4,000000
SK	2,500000	38	2,000000	2,000000	17	1,000000	5,000000
SP	3,250000	32	3,000000	4,000000	11	1,000000	5,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Minimální hodnota odpovědí německých respondentů je 3, nejvyšší minimum ze všech vzorkovaných zemí. Velkou rozdílnost odpovědí vykazuje Bulharsko, Slovensko a Španělsko. Průměr Slovenska je nejnižší ze všech zemí, pouhých 2,5 a modus (17 hodnot z 38) vykazuje hodnotu 2. Slovensko je tak zemí, kterému GDPR nedodalo pocit kontroly nad osobními daty stejně tak jako České republice. Hodnotu 1, uvedlo 11 %, tzn., že jim GDPR nezvýšilo pocit kontroly nad osobními daty.

Tabulka 13: GDPR Vám osobně: Zvýšilo pocit kontroly nad Vašimi osobními údaji (2)

	GDPR Vám osobně: Zvýšilo pocit kontroly nad vašimi osobními údaji						
Proměnná	25,000. kvantil	75,000. kvantil	Sm.Odch.	Rozptyl	Průměrná odchylka	Rozsah	Kvartilové rozpětí
BG	2,000000	4,000000	1,464131	2,143678	1,288889	4,000000	2,000000
CZ	1,500000	4,000000	1,332086	1,774452	1,113426	4,000000	2,500000
DE	3,000000	4,000000	0,715609	0,512097	0,527344	2,000000	1,000000
F	4,000000	4,000000	0,685994	0,470588	0,474048	3,000000	0,000000
GB	3,000000	5,000000	0,999603	0,999206	0,760802	4,000000	2,000000
PL	3,000000	4,000000	0,747470	0,558712	0,661157	2,000000	1,000000
SK	2,000000	3,000000	1,108932	1,229730	0,921053	4,000000	1,000000
SP	2,000000	4,000000	1,135924	1,290323	0,953125	4,000000	2,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

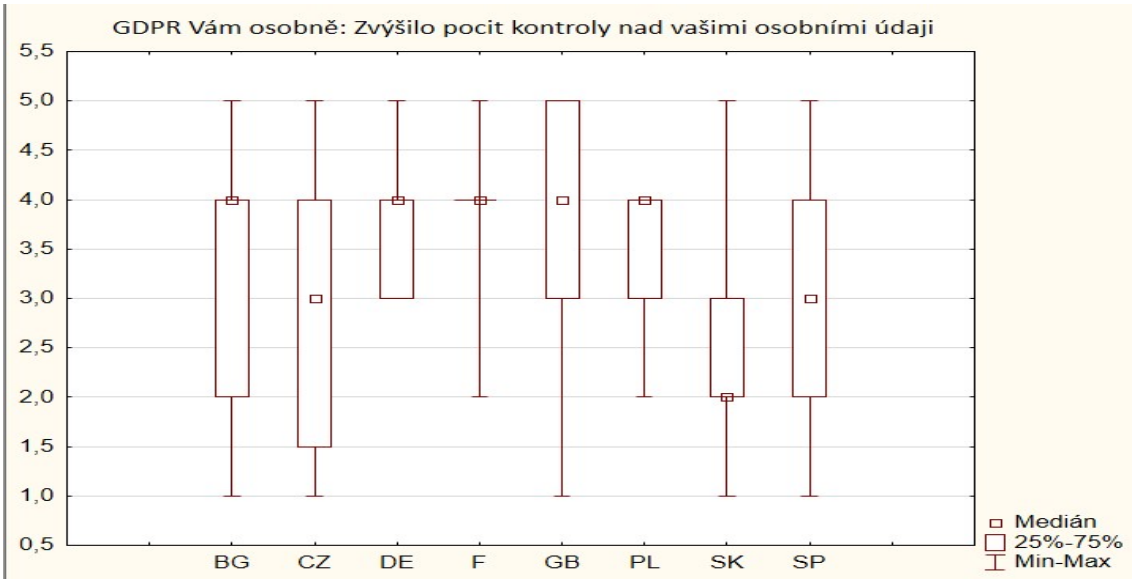
Tabulka 14: GDPR Vám osobně: Zvýšilo pocit kontroly nad Vašimi osobními údaji (3)

	GDPR Vám osobně: Zvýšilo pocit kontroly nad vašimi osobními údaji		
Proměnná	Šikmost	Špičatost	Součet
BG	-0,308671	-1,36099	95,0000
CZ	0,171989	-1,03001	197,0000
DE	0,092427	-0,94377	126,0000
F	-0,445190	0,74527	132,0000
GB	-0,850639	0,65586	143,0000
PL	-0,808266	-0,70086	112,0000
SK	0,627605	-0,30868	95,0000
SP	-0,246495	-0,74159	104,0000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Zjištěné hodnoty dokazují, že pocit bezpečí a kontroly nad osobními daty vzorkovaných jednotlivých zemí se liší a nebylo dosaženo jednoznačného verdiktu, kdy by ohodnocení 4 nebo 5 body vykazovalo více než 50 % všech odpovědí.

Zatímco v Německu evokovalo GDPR pocit kontroly, nedá se tento fakt přenést na ostatní země, neboť Slovensko a Česká republika vykazují nejnižší hodnoty.



Obrázek 42: GDPR Vám osobně: Zvýšilo pocit kontroly nad Vašimi osobními údaji
Zdroj: Vlastní zpracování v programu SW STATISTICA

6.2.4 GDPR – zvýšení pocitu bezpečí a ochrany dat

Otázka na zvýšení pocitu bezpečí a ochrany dat přinesla podobné výsledky jako předcházející otázka, což se dalo predikovat, neboť spolu velmi úzce souvisí. Nejvyšších hodnot dosahuje Francie, Německo a Velká Británie. Nejnižší hodnoty opět vykazuje Česká republika a Slovensko.

Tabulka 15: GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat (1)

Proměnná	GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat						
	Průměr	Poč. plat.	Medián	Modus	Četnost modusu	Minimum	Maximum
BG	3,033333	30	3,000000	1,000000	8	1,000000	5,000000
CZ	2,527778	72	3,000000	3,000000	25	1,000000	5,000000
DE	4,000000	32	4,000000	4,000000	13	2,000000	5,000000
F	4,205882	34	4,000000	vícenás.		2,000000	5,000000
GB	4,111111	36	4,000000	4,000000	18	1,000000	5,000000
PL	3,787879	33	4,000000	4,000000	11	2,000000	5,000000
SK	2,342105	38	2,000000	2,000000	13	1,000000	5,000000
SP	3,093750	32	3,000000	3,000000	11	1,000000	5,000000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Zatímco v předchozí otázce činilo minimum u Německa hodnotu 3, zde se ještě snížila, a to na hodnotu 2. Zajímavostí je, že v této otázce vykazují všechny země maximální hodnotu 5 a takováto shoda byla vykázána pouze u otázky týkající se zvýšení administrativy.

Tabulka 16: GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat (2)

	GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat						
Proměnná	25,000. kvantil	75,000. kvantil	Sm.Odch.	Rozptyl	Průměrná odchylka	Rozsah	Kvartilové rozpětí
BG	1,000000	4,000000	1,564329	2,447126	1,368889	4,000000	3,000000
CZ	1,000000	3,000000	1,321248	1,745696	1,122685	4,000000	2,000000
DE	3,000000	5,000000	0,842424	0,709677	0,625000	3,000000	2,000000
F	4,000000	5,000000	0,808268	0,653298	0,653979	3,000000	1,000000
GB	4,000000	5,000000	0,854493	0,730159	0,592593	4,000000	1,000000
PL	3,000000	5,000000	1,053493	1,109848	0,876033	3,000000	2,000000
SK	1,000000	3,000000	1,121686	1,258179	0,940443	4,000000	2,000000
SP	2,500000	4,000000	1,201058	1,442540	0,923828	4,000000	1,500000

Zdroj: Vlastní zpracování v programu SW STATISTICA

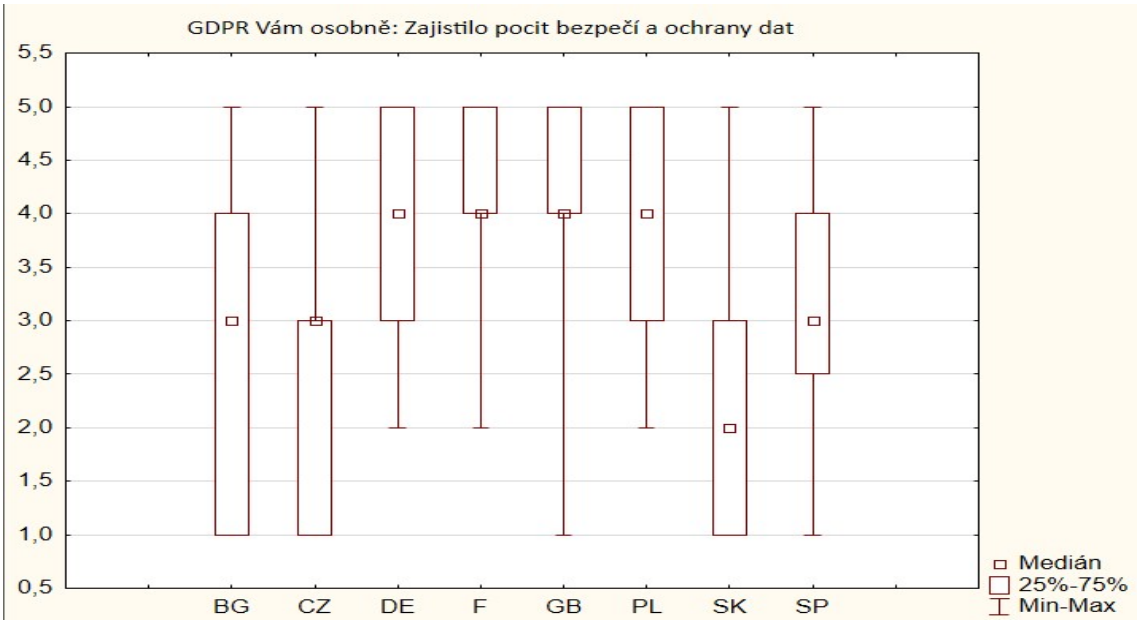
Nejvyššího špičatosti dosahují hodnoty Velké Británie, což značí pravostrannou asymetrii, tedy rovnoměrné rozložení hodnot vlevo od průměru, což je krásně vidět i na krabicovém grafu. Naopak Francie poukazuje na symetrické rozložení.

Tabulka 17: GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat (3)

	GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat		
Proměnná	Šikmost	Špičatost	Součet
BG	-0,11676	-1,55126	91,0000
CZ	0,37164	-0,84596	182,0000
DE	-0,34532	-0,67053	128,0000
F	-0,76904	0,10015	143,0000
GB	-1,38519	3,64659	148,0000
PL	-0,40073	-0,99556	125,0000
SK	0,47910	-0,66188	89,0000
SP	-0,42904	-0,55272	99,0000

Zdroj: Vlastní zpracování v programu SW STATISTICA

Známkou 4, nebo 5 ohodnotilo stanovisko 49 %, průměrná vykázaná známka je 3,3 bodu a odpověď s hodnotou 1 uvedlo celých 15 % respondentů, což je o 4 % více než v předchozí otázce.



Obrázek 43: GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany dat
Zdroj: Vlastní zpracování v programu SW STATISTICA

Závěrem lze tedy shrnout, že zatímco u prvních dvou otázek týkajících se zvýšení administrativy a poukázáním na hrozby a rizika úniku a zneužití dat zazněla takřka jednohlasná odpověď respondentů, tedy vyšší než 50 % odpovědí hodnoty 4, nebo 5, na pocit bezpečí a kontroly jednoznačný pohled nemají a rozdílnost mezi zeměmi je významná.

7 Shrnutí výsledků práce

Diplomová práce byla vypracována na základě praktického výzkumu probíhajícím v 8 zemích EU. Sesbíraná data byla sjednocena a podrobena analýzám na třech úrovních:

- Globální úroveň;
- Úroveň státu;
- Úroveň respondenta.

Pohled na několik úrovní a rozsah otázek přinesl zajímavé poznatky z oblasti GDPR.

7.1 Globální úroveň

Základním stavebním kamenem diplomové práce bylo získat minimálně 30 vzorkovaných z každé země, čehož se podařilo dosáhnout, neboť průměrná hodnota počtu vzorkovaných dosáhla počtu 38 vzorkovaných. Minimum činí 30 vzorkovaných z Bulharska a maximum 72 vzorkovaných z České republiky. Respondenti z České republiky, Slovenska a Velké Británie nejvíce ovlivnili globální pohled na dotazníkové šetření, což potvrdil i chí-kvadrát test. Z oslovených osob (2456), celkem 296 osob dotazník pouze otevřelo a 307 osob dotazník zodpovědělo. Hlavními faktory ovlivňující počet vyplněných dotazníků je bezesporu období sběru dat (konec roku, vánoční svátky) a dále složitost problematiky GDPR a roztříštěnost odpovědností za dílčí úkoly související s GDPR v rámci firmy. Výzkum byl zacílen za firmy všech velikostí. Získanou cílovou skupinou výzkumu tvoří převážně malé a střední firmy, které tvoří 70 % vzorkovaných. Majoritní podíl tvoří firmy z oboru stavebnictví (33,6 %), e-shopů (22 %) a průmyslu (16 %). Hlavní podíl respondentů je ze skupiny „ostatní“, tedy nedefinovaného oboru (38 %), kde jsou zastoupeny firmy typu: armáda, advokacie apod., pro které nebyl vhodný obor definována. Z definovaných oddělení vykazuje nejvyšší zastoupení marketing (20 %), IT oddělení (17 %), logistika (8 %) a vedení firmy (7 %).

Firmy investovaly do GDPR nemalé finance, ačkoliv třetina respondentů uvedla, že neznají výši investice do oblasti GDPR, kterou musel jejich zaměstnavatel vynaložit, zbylé dvě třetiny vykazují nejvyšší četnosti v intervalech nákladů 1000 – 9 9999 €

(35 %), 10 000 – 49 999 € (33 %). Relevantnost těchto hodnot podporuje výpočet Hospodářské komory, která uvádí, že většina firem zaplatí za GDPR do 50 tis. Kč [Hospodářská komora, 2018], GDPR Survay z května 2019, které uvádí, že firmy nejvíce investovaly v intervalu 1 000 – 999 € (27 %) a 10 000 – 49 999 € (24 %) [GDPR.eu, 2019]. Investované náklady souvisí např. i se zřízením pozice pověřence, kterou má 64 % respondentů, ačkoliv legislativa GDPR tuto povinnost ukládá pouhým 10 % vzorkovaných. Obdobná situace je u zpracování záznamu o činnostech, které je povinné pro 18,9 % vzorkovaných, ale dokument má zpracovaný 81,4 % respondentů. Správné označení odpovědi, koho GDPR chrání, a naopak kdo musí dodržovat jeho regule, správně zodpovědělo 64,17 %. Vzorkovaní nemají jasno v oblasti E2EE, 29 % respondentů neví, zda firma používá E2EE, ačkoliv v dalších odpovědích uvedou jako firemní komunikační nástroj aplikaci WhatsApp, která E2EE používá, k tomuto závěru dospělo i GDPR Survey z května 2019 [GDPR.eu, 2019]. Zatímco právo na ochranu osobních údajů, které nese samotný název: „General Data Protection“, správně označilo 95,1 % vzorkovaných, správnost označení dalších práv je výrazně nižší. Právo odmítnout zpracování osobních dat 62,54 %, právo na výmaz osobních údajů 57,65 %, právo vyžádat si data, které o fyzické osobě právnický subjekt zpracovává, označilo pouze 47,88 %. Pokud neznají svá práva respondenti, tedy zaměstnanci firmy, lze dedukovat, že ani samotná firma nemá jasné povědomí o právech fyzických osob, jinak by své zaměstnance upozornila, že je zákazník či obchodní partner může požádat např. o data, která o nich firma zpracovává, a jak mají v takovém případě postupovat. Na základě výše prezentovaných dat přijímáme hypotézu, že GDPR je pro firmy nesrozumitelné:

- **54 % vzorkovaných má pověřence, ačkoliv jim to legislativa GDPR neukládá a pozice pro ně znamená zvýšení nákladů;**
- **62 % vzorkovaných má zpracovaný záznam o činnostech, ačkoliv jim to legislativa GDPR neukládá;**
- **35,83 % respondentů nemá jasno, koho GDPR chrání a kdo musí dodržovat zákonné regule;**
- **29 % respondentů neví, zda používají E2EE;**
- **Firmy nemají povědomí o tom, jaká práva GDPR fyzickým osobám dává.**

Jedním z faktorů ovlivňující znalosti respondentů je jistě školení zaměstnanců v oblasti GDPR. Školení by nemělo být jednorázovou záležitostí, ale opakujícím se a pravidelným procesem reflektujícím zjištěná rizika a hrozby ve společnosti. Z celkového počtu proškolených zaměstnanců bylo 49,6 % vzorkovaných proškoleno opakovaně a 50,4 % pouze jednou. 9,4 % naopak nebylo proškoleno. Vyšší erudovanost může pomoci zaměstnanců uvědomovat si rizika v pracovním procesu a schopnost upozornit na ně a zároveň lépe hájit svá práva i v soukromém životě. Firmy se snaží zodpovědně chránit svá data. Zejména chrání elektronická data, kde průměrná známka je 4,2 bodu z maximálních 5 bodů, využívají pro to např. i šifrování, anonymizaci a pseudoanonymizaci. Zatímco tištěná data nemají adekvátní ochranu a průměrná známka vykazuje hodnotu 3,6 bodu. Tato oblast je obzvlášť citlivá pro mikro firmy, kde je průměrná známka 3, zatímco velké firmy vykazují známku 4,2. Problematickou oblastí je také tisk samotných dokumentů. Chráněný tisk, tedy tisk pod heslem (37,79 %), nebo na tiskárnu s omezeným přístupem (41,04 %), uvedlo celkem 78,83 % vzorkovaných. Pokud je tisk na tiskárnu bez kontroly, měli by být zaměstnanci minimálně poučeni, že vytištěný dokument se v tiskárně musí nacházet jen pouze po nezbytně nutnou dobu, aby nedošlo ke zneužití dat, ideální je ovšem mít tisk zabezpečen heslem nebo na tiskárnu s omezeným přístupem. Naopak mají společnosti zabezpečen přístup na mobilní telefon a počítač, pouze 3 respondenti uvedli, že přístup není zabezpečen. Ostatní respondenti využívají zabezpečení především prostřednictvím biometrického údaje (v průměru 25 respondentů z každé země), číselného kódu a grafického znaku. Mnohem složitější proces představuje přidělování a odnímání přístupů uživatelů, v praxi se často ukazuje jako bolestivým bodem firmy, který není zcela pod kontrolou. Tvrzení, že jsou přístupy zaměstnanců zcela pod kontrolou, získalo průměrnou známku 3,6 bodu z maximálních 5 bodů.

19 % vzorkovaných používá kontakty ze zakoupených databází. Jak na svých stránkách uvádí ÚOOU, je vysoce nepravděpodobné, že by kontakty nějaké databáze udělily takovýto konkrétní souhlas a obecný souhlas zahrnující více oblastí nelze použít [ÚOOU, a, 2019]. Direct mailing, tedy hromadné rozesílání informací zákazníkům využívá 65 vzorkovaných a z nich 29 % nemá uvedený odkaz na

odhlášení z rozesílky v e-mailu. Naopak se jeví jako dobře podchycenou oblastí souhlas se zpracování údajů, který má 92 % respondentů před jejich zpracováním, Tuto skutečnost potvrzuje i GDPR Survay, kde respondenti uvedli plný nebo částečný souhlas s výrokem, že zaměstnavatel má vždy souhlas fyzické osoby před zpracováním jejich dat, ve výši 82 % [GDPR.eu, 2019].

Další stanovená hypotéza v úvodu diplomové práce předpokládala, že většina oslovených podnikatelských subjektů se dopouští pochybení v oblasti ochrany soukromí. Asociace profesionálů v oblasti ochrany soukromí (IAPP) na základě výzkumu z listopadu 2018 uvedla, že z 550 respondentů celkem 56 % nedodržuje legislativu GDPR [GDPR.365, 2019], CISCO ve své zprávě z ledna 2019 uvedlo 41 % firem z 3 200, které nejsou v souladu s GDPR [GDPR.365, 2019]. Luxatia International uvádí, že v současné době je 1 ze 3 společností plně v souladu s GDPR [Luxatia International, 2019]. Na základě těchto faktů a výsledků dotazníkové šetření níže, hypotézu přijímáme.

- **9,4 % vzorkovaných nebylo proškoleno v oblasti GDPR;**
- **3 % vzorkovaných nemá zajištěnu bezpečnost dat neboli data jsou volně přístupná;**
- **21,17 % vzorkovaných uvedlo nekontrolovaný tisk;**
- **1 % vzorkovaných nemá zabezpečen přístup na mobilní telefon nebo počítač;**
- **19 % vzorkovaných používá kontakty ze zakoupených databází;**
- **6 % vzorkovaných uvádí viditelně adresáty e-mailu při hromadné rozesílce;**
- **29 % vzorkovaných nemá uveden odkaz na možnost odhlášení se z direct mailingu v e-mailu;**
- **Přidělování a odnímání přístupů zaměstnancům není zcela pod kontrolou, průměrná známka 3,6 bodu z maximálních 5 bodů.**

Většina uvedených pochybení je snadno odstranitelná, problém tkví v nevědomosti firmy, která se jich dopouští. Nutno zde ovšem také vyzdvihnout přístup firem

k GDPR, kde se firmy skutečně snaží naplňovat požadavky GDPR, což dosvědčují zjištěná fakta:

- **90,6 % vzorkovaných bylo proškoleno v oblasti GDPR;**
- **Zabezpečení elektronických dat ohodnotili vzorkovaní známkou 4,2 z maximálních 5 bodů;**
- **81,4 % vzorkovaných má zpracovaný záznam o činnostech, jsou si tedy vědomi manipulace s daty a případných rizik;**
- **78,83 % vzorkovaných má chráněný tisk dokumentů;**
- **99 % vzorkovaných uvedlo, že přístup na počítač a mobilní telefon mají zajištěn;**
- **37,46 % vzorkovaných má šifrovaná data v mobilním telefonu nebo počítači.**
- **Vzorkovaní používají E2EE, anonymizaci, pseudoanonymizaci dat;**
- **Vzorkovaní používání spolehlivé a ověřené nástroje a poskytovatele z oblasti VPN, komunikačních nástrojů nebo nástrojů umožňujících spolupráci.**

Navzdory výše uvedeným skutečnostem zamítáme stanovenou hypotézu, která uváděla, že GDPR přineslo firmám uvědomění si hrozeb a rizik související se zpracováním dat. Firmy si bezesporu uvědomují rizika a hrozby, snaží se jim předcházet, ale nelze stanovit, že je to právě na základě GDPR. Tuto skutečnost dotazníkové šetření nezjišťovalo.

7.2 Úroveň státu a respondenta

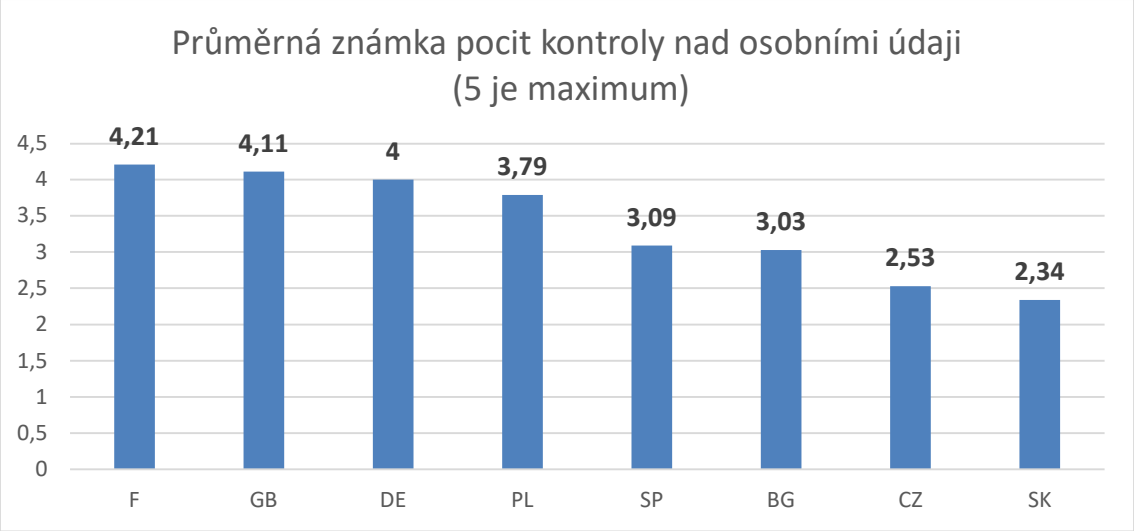
Vyhodnocování na úrovní zemí probíhalo v oblasti:

- Procento proškolených zaměstnanců;
- Obecné zabezpečení dat;
- Zabezpečení elektronických dat;
- Zabezpečení tiskových dat;
- Kontrola tisku;
- Zabezpečení přístupu na mobilní telefon a počítač;

- Šifrování dat.

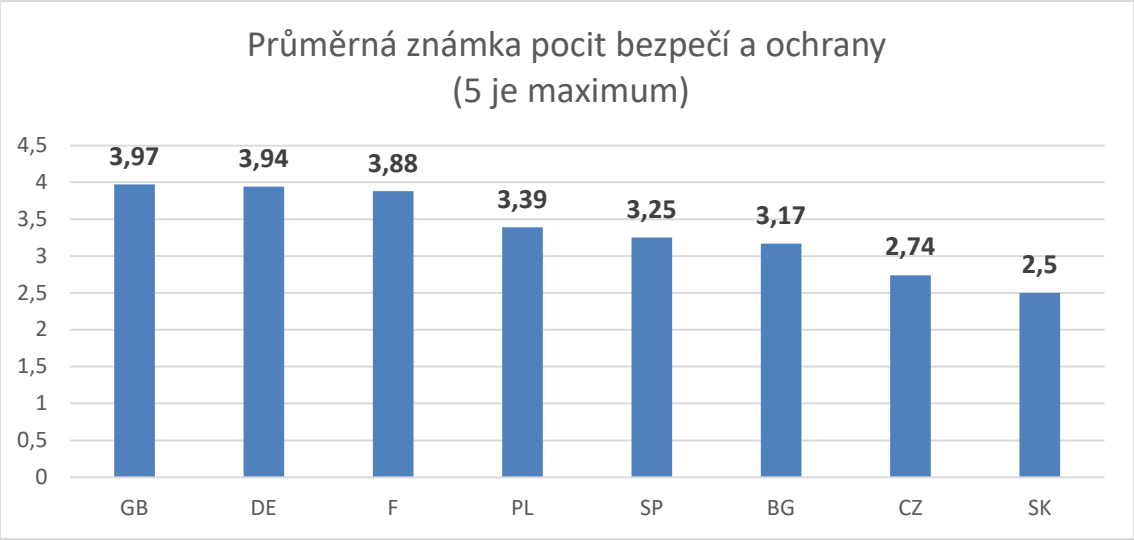
Analýzou dat dle zemí bylo zjištěno, že data vytvořených dvojic jsou bezesporu zajímavá, ale rozdílná a také prokázala, že každá země vnímá vyhodnocovanou oblast GDPR rozdílně. Hodnota udává průměr umístění země v uvedených oblastech. Pořadí zemí je následující: Polsko (2,14), Francie (2,43) a Velká Británie (2,43), Německo (3,57), Česká republika (4,29), Slovensko (4,43), Španělsko (4,86), Bulharsko (5). Závěrem tedy je, že v souladu s GDPR v definovaných oblastech je nejvíce Polsko, Francie, Velká Británie a Německo.

Skutečnost, že GDPR zvýšilo pocit kontroly na osobními daty nejvíce pociťují respondenti z Velké Británie s průměrnou známkou 3,97 z maximálních 5, umístění ostatních zemí je patrné z grafu č. 44.



Obrázek 44: GDPR Vám osobně: Zvýšilo pocit kontroly nad Vašimi osobními údaji
Zdroj: Vlastní zpracování

Přínos GDPR v oblasti zajištění bezpečí a ochrany pociťují nejvíce vzorkovaní z Velké Británie (3,97) a Německa (3,94), naopak nejméně respondenti ze Slovenska (2,5) a České republiky (2,74). Společnost Varonis uvádí, že 62 % britských zákazníků se, po zavedení GDPR, cítí při sdílení dat bezpečněji [Varonis, 2020].



Obrázek 45: GDPR Vám osobně: Zajistilo pocit bezpečí a ochrany
Zdroj: Vlastní zpracování

Poslední část diplomové práce se týkala subjektivního pohledu vzorkovaných. V této oblasti bylo prokázáno, že se názory vzorkovaných shodují ve dvou bodech, kdy jejich ohodnocení známkou 4 a 5 přesahuje 50 %: **GDPR zvýšilo administrativu v zaměstnání** a **GDPR poukázalo na hrozby a rizika úniku a zneužití dat.** Zvýšení administrativy dokazuje hodnocení známkou 4, nebo 5 u 67 % vzorkovaných. 7,8 % uvedlo, že jim GDPR administrativu nezvýšilo. Průměrná zjištěná známka je 3,8 bodu z maximálních 5. Fakt, že GDPR poukázalo na hrozby a rizika úniku a zneužití dat ohodnotilo 53,4 % vzorkovaných známkou 4, nebo 5, průměrná vykázaná známka je 3,78. Rozdílných výsledků dosahovali vzorkovaní v oblasti **zvýšení pocitu kontroly nad osobními daty a zvýšení pocitu bezpečí a ochrany.** V první odpovědi, tedy zvýšení pocitu kontroly nad osobními daty uvedlo známku 4 a 5 celkem 49 % respondentů a průměrná známka je 3,3 bodu, negativní odpověď „ne“ uvedlo 11 %. Obdobný výsledek byl zjištěn u stanoviska, že GDPR zvýšilo u respondentů pocit bezpečí a ochrany. I zde 49 % respondentů ohodnotilo odpověď známkou 4, nebo 5 a také průměrná známka je 3,3 bodu, rozdílný je počet respondentů, který uvedl odpověď „ne“ – 15 %. Tyto výsledky potvrzují zjištěné údaje firmou Luxatia International, která uvádí, že 45 % občanů EU je stále nespokojeno s ochranou osobních údajů [Luxatia International, 2019].

GDPR nemá být negativně vnímaným zákonem asociující zvýšenou administrativu. Vnímání respondentů může souviset s nedostatečnou znalostí legislativy a snahou mít raději na vše souhlas než pochybit. Naopak GDPR byl dobře míněný zákon na ochranu osobních údajů, který měl firmám otevřít oči a ukázat cesty, kterými může dojít ke zneužití dat. Příkladem špatné prezentace a informovanost o GDPR veřejnosti je Česká republika, kde byl tento zákon od samého počátku spojován se zvýšenou administrativou a vyplývajícími povinnostmi pro firmu, obzvláště byl strašákem pro společnosti podnikající v oblasti e-shopu. S přibývajícími měsíci se GDPR tiše vytratilo z médií a zmiňováno je pouze v případě sankcí udělených firmám.

8 Závěry a doporučení

GDPR označovaný také jako „zlatý standard“ kybernetických zákonů (Andrew, 2019, s. 2) je bezesporu zákon, který má své opodstatnění. Díky špatné prezentaci médií a nedostatečné informovanosti ze strany vlády, nebyl, např. v České republice, pozitivně přijat. Navzdory této skutečnosti si každý z nás uvědomuje potřebu chránit své soukromí, a tedy svá data, mít přehled kdo a jak s daty manipuluje. Již samotným narozením se člověk dostává do spirály elektronických dat a zanechává za sebou digitální stopu a jen těžko si lze představit, že může mít člověk svá data stoprocentně pod kontrolou. Digitální stopy byly použity i v rámci politických kampaní, např. v roce 2012 v kampani Obamy [Bach, 2019]. IoT (Internet of Things) vnesl do našeho života pohodlí, učinil ho také rychlejší, ale technologie okolo nás se neustále vyvíjí vysokou rychlostí, důkazem jsou inteligentní sítě, města, automobily, ale důležitým prvkem musí být i důsledná ochrana dat od samého počátku [Abdulghani, 2019, s. 29]. Základním prvkem ochrany je zamezení narušení dat IoT, což je z důvodu pokroku velmi obtížné [Abdulghani, 2019, s. 28].

V rámci diplomové práce byla zjištěna pochybení podnikatelský subjektů v několika oblastech. Jako příklad může být uvedeno pochybní v oblasti používání dat ze zakoupených databází, chybějící IDM, nedostatečná ochrana tištěných dokumentů, nedostatečné proškolování zaměstnanců. GDPR přináší ochranu všech dat a nutno zde znovu zopakovat, že firmy mají dobře zajištěna elektronická data, ale tištěná data jsou opomíjena nebo zanedbávána.

Jednoznačné doporučení pro všechny podnikatelské subjekty je následující:

- **Pravidelně proškolovat zaměstnance v oblasti GDPR;**
- **Monitorovat a vyhodnocovat hrozby a rizika související s ochranou dat;**
- **Aplikovat nápravná opatření a provádět jejich kontrolu;**
- **Zaměřit se na ochranu tištěných dat a samotný tisk mít pod kontrolou;**
- **Nastavit proces pro IDM a mít zabezpečen přístup do počítače a mobilního telefonu;**
- **Nevyužívat data ze zakoupených databází;**

- **Při hromadném rozesílání e-mailu uvádět adresáty ve skryté kopii, nebo odesílat e-maily každému adresátovi zvlášť;**
  V rámci direct mailingu mít uvedený link pro odhlášení z rozesílky.

Hrozby a rizika spojená se zneužitím dat by měly vyhodnocovat nejen právnické subjekty, ale rovněž i fyzické osoby a eliminovat rizika. Cílem je tedy data chránit a mít připraveny postihy pro ty, kteří data zneužívají, což GDPR bezesporu přináší. Již nyní lze ovšem predikovat, že GDPR je pouze první vlaštovkou v oblasti ochrany dat, neboť Evropská komise se již nyní zabývá digitální strategií EU, která zahrnuje kybernetickou bezpečnost, infrastrukturu, ale i digitální vzdělávání. Kromě této strategie představila „bílou knihu“, která definuje cíle pro důvěryhodné používání umělé inteligence [Novinky.CZ, 2020]. Vizí je umožnit lidem maximalizovat užitek umělé inteligence, aniž by měli obavy o svá data a soukromí [Novinky.CZ, 2020]. V budoucnu lze tedy očekávat další zákony zajišťující ochranu osobních dat, jak moc bude ovšem účinná, prokáže až samotná praxe.

9 Seznam použité literatury

[1] ABDULGHANI, Hezam Akram, Niels Alexander NIJDAM, Anastasija COLLEN a Dimitri KONSTANTAS. A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. Symmetry [online]. 2019, 11(6) [cit. 27.11.2019]. DOI: 10.3390/sym11060774. ISSN 2073-8994. Dostupné z: https://www.mdpi.com/2073-8994/11/6/774

[2] AHMADIAN, Amir Shayan, Daniel STRÜBER, Volker RIEDIGER a Jan JÜRJENS. Supporting privacy impact assessment by model-based privacy analysis. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing-SAC '18 [online]. New York, New York, USA: ACM Press, 2018, 2018, s. 1467-1474 [cit. 29.08.2019]. DOI:10.1145/3167132.3167288. ISBN 9781450351911.Dostupné z: http://dl.acm.org/citation.cfm?doid=3167132.3167288

[3] AirVPN - The air to breathe the real Internet - AirVPN. AirVPN - The air to breathe the real Internet - AirVPN [online]. [cit. 10.08.2019]. Dostupné z: https://airvpn.org/

[4] ALSAYED KASSEM, Jamila, Sarwar SAYEED, Hector MARCO-GISBERT, Zeeshan PERVEZ a Keshav DAHAL. DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. Applied Sciences [online]. 2019, 9(15) [cit. 27.11.2019]. DOI: 10.3390/app9152953. ISSN 2076-3417. Dostupné z: https://www.mdpi.com/2076-3417/9/15/2953

[5] ANDREW, Jane a Max BAKER. The General Data Protection Regulation in the Age of Surveillance Capitalism. Journal of Business Ethics [online]. [cit. 2019-09-07]. DOI: 10.1007/s10551-019-04239-z. ISSN 0167-4544. Dostupné z: http://link.springer.com/10.1007/s10551-019-04239-z

[6] Are the Real Costs of GDPR Compliance? - GDPR365. GDPR Compliance Software, Tools & Services - GDPR365 [online]. Copyright © [cit. 24.02.2020]. Dostupné z: https://www.gdpr365.com/what-are-the-real-costs-of-gdpr-compliance/

[7] BACH, Ruben L., Christoph KERN, Ashley AMAYA, Florian KEUSCH, Frauke KREUTER, Jan HECHT a Jonathan HEINEMANN. Predicting Voting Behavior Using Digital Trace Data. Social Science Computer Review [online]. 2019 [cit. 05.11.2019]. DOI: 10.1177/0894439319882896. ISSN 0894-4393. Dostupné z: http://journals.sagepub.com/doi/10.1177/0894439319882896

[8] BENDIEK, Annegret a Magnus RÖMER. Externalizing Europe: the global effects of European data protection. Digital Policy, Regulation and Governance [online]. 2019, 21(1), 32-43 [cit. 03.11.2019]. DOI: 10.1108/DPRG-07-2018-0038. ISSN 2398-5038. Dostupné z: https://www.emerald.com/insight/content/doi/10.1108/DPRG-07-2018-0038/full/html

[9] BIČÍKOVÁ, Zuzana a IDNES.CZ. Cisco: Požadavky GDPR zatím splňuje pouze 59 % podniků. Channelworld.cz [online]. 2019, 12.02.2019 [cit. 31.08.2019]. Dostupné z: https://channelworld.cz/analyzy/cisco-pozadavky-gdpr-zatim-splnuje-pouze-59-podniku-22240

[10] BOLOGNINI, Luca a Camilla BISTOLFI. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law & Security Review [online]. 2017, 33(2), 171-181 [cit. 06.08.2019]. DOI: 10.1016/j.clsr.2016.11.002. ISSN 02673649. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0267364916302151

[11] BOTTA, Marco a Klaus WIEDEMANN. The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey. The Antitrust Bulletin [online]. 2019 [cit. 11.08.2019]. DOI: 10.1177/0003603X19863590. ISSN 0003-603X. Dostupné z: http://journals.sagepub.com/doi/10.1177/0003603X19863590

[12] BRODIN, Martin. A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises. European Journal for Security Research[online]. [cit. 10.08.2019]. DOI: 10.1007/s41125-019-00042-z. ISSN 2365-0931. Dostupné z: http://link.springer.com/10.1007/s41125-019-00042-z

[13] BURRI a SCHÄR. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. Journal of Information Policy [online]. 2016, 6 [cit. 11.08.2019]. DOI: 10.5325/jinfopoli.6.2016.0479. ISSN 21583897. Dostupné z: http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.0479

[14] Cisco - Global Home Page. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/

[15] COHEN, Manny. Fake news and manipulated data, the new GDPR, and the future of information. Business Information Review [online]. 2017, 34(2), 81-85 [cit. 06.08.2019]. DOI: 10.1177/0266382117711328. ISSN 0266-3821. Dostupné z: http://journals.sagepub.com/doi/10.1177/0266382117711328

[16] ČTK a IDNES.CZ. Rekordní pokuta. Facebook zaplatí pět miliard dolarů za porušení soukromí. IDnes.cz [online]. 2019, 12.07.2019 [cit. 31.08.2019]. Dostupné z: https://www.idnes.cz/ekonomika/zahranicni/facebook-pokuta-poruseni-ochrana-soukromi-miliard-usa.A190712_221657_eko-zahranicni_pmk

[17] DE HERT, Paul, Vagelis PAPAKONSTANTINOU, Gianclaudio MALGIERI, Laurent BESLAY a Ignacio SANCHEZ. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review [online]. 2018, 34(2), 193-203 [cit. 10.8.2019]. DOI: 10.1016/j.clsr.2017.10.003. ISSN 02673649. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0267364917303333

[18] Digital Technologies of the European Union in Personal Data Protection. International Journal of Innovative Technology and Exploring Engineering [online]. 2019, 8(12), 3600-3604 [cit. 26.10.2019]. DOI: 10.35940/ijitee.L3798.1081219. ISSN 2278-3075. Dostupné z: https://www.ijitee.org/wp-content/uploads/papers/v8i12/L37981081219.pdf

[19] DUNCAN, Bob a Yuan ZHAO. Risk Management for Cloud Compliance with the EU General Data Protection Regulation. In: 2018 International Conference on High Performance Computing & Simulation (HPCS) [online]. IEEE, 2018, 2018, s. 664-671 [cit. 06.08.2019]. DOI: 10.1109/HPCS.2018.00109. ISBN 978-1-5386-7878-7. Dostupné z: https://ieeexplore.ieee.org/document/8514414/

[20] Evropská komise chce pravidla pro bezpečné sdílení dat - Novinky.cz. Novinky.cz – nejčtenější zprávy na českém internetu [online]. Copyright © 2003 [cit. 23.02.2020]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/evropska-komise-chce-pravidla-pro-bezpecne-sdileni-dat-40314158

[21] GDPR Statistics From The First Year [Infographic] | Luxatia International Home | Luxatia International [online]. Copyright © 2010 Luxatia International [cit. 24.02.2020]. Dostupné z: https://www.luxatiainternational.com/article/gdpr-statistics-from-the-first-year-infographic

[22] GDPR.eu, a. GDPR Archives - GDPR.eu. General Data Protection Regulation (GDPR) Compliance Guidelines [online]. Copyright © 2019 Proton Technologies AG. All Rights Reserved. [cit. 10.08.2019]. Dostupné z: https://gdpr.eu/tag/gdpr/

[23] GDPR.eu, b. Millions of small businesses aren't GDPR compliant, our survey finds - GDPR.eu. General Data Protection Regulation (GDPR) Compliance Guidelines [online]. Copyright © 2019 Proton Technologies AG. All Rights Reserved. [cit. 10.08.2019]. Dostupné z: https://gdpr.eu/2019-small-business-survey/

[24] GDPR.eu, c. Millions of small businesses aren't GDPR compliant, our survey finds - GDPR.eu. General Data Protection Regulation (GDPR) Compliance Guidelines [online]. Copyright © 2019 Proton Technologies AG. All Rights Reserved. [cit. 10.08.2019]. Dostupné z: https://gdpr.eu/ data-anonymization-taxa-4x35/

[25] GDPR.eu, d. Millions of small businesses aren't GDPR compliant, our survey finds - GDPR.eu. General Data Protection Regulation (GDPR) Compliance Guidelines [online]. Copyright © 2019 Proton Technologies AG. All Rights Reserved. [cit. 10.08.2019]. Dostupné z: https://gdpr.eu/checklist/

[26] GDPR.eu, e. Millions of small businesses aren't GDPR compliant, our survey finds - GDPR.eu. General Data Protection Regulation (GDPR) Compliance Guidelines [online]. Copyright © 2019 Proton Technologies AG. All Rights Reserved. [cit. 10.08.2019]. Dostupné z: https://gdpr.eu/compliant-services/

[27] GDPR's Impact So Far: Must-Know Stats and Takeaways - Varonis. Data Security & Insider Threat Detection | Varonis [online]. Copyright © 2020 Inside Out Security [cit. 24.02.2020]. Dostupné z: https://www.varonis.com/blog/gdpr-effect-review/

[28] GEORGIADOU, Yola, Rolf DE BY a Ourania KOUNADI. Location Privacy in the Wake of the GDPR. ISPRS International Journal of Geo-Information [online]. 2019, 8(3) [cit. 27.11.2019]. DOI: 10.3390/ijgi8030157. ISSN 2220-9964. Dostupné z: https://www.mdpi.com/2220-9964/8/3/157

[29] Google is first company hit with major GDPR fine. Computer Fraud & Security [online]. 2019, 2019(2), 1-3 [cit. 27.11.2019]. DOI: 10.1016/S1361-3723(19)30013-2. ISSN 13613723. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S1361372319300132

[30] HEURIX, Johannes, Michael KARLINGER a Thomas NEUBAUER. PERiMETER – pseudonymization and personal metadata encryption for privacy-preserving searchable documents. Health Systems [online]. 2017, 1(1), 46-57 [cit. 09.09.2019]. DOI: 10.1057/hs.2012.5. ISSN 2047-6965. Dostupné z: https://www.tandfonline.com/doi/full/10.1057/hs.2012.5

[31] Home - Eurostat. European Commission | Choose your language | Choisir une langue | Wählen Sie eine Sprache [online]. Copyright © Joachim Wendler [cit. 09.02.2020]. Dostupné z: https://ec.europa.eu/eurostat/home?

[32] H-Square ICT Solutions. H-Square ICT Solutions [online]. Copyright © 2015 – 2019 [cit. 09.09.2019]. Dostupné z: https://www.h-square.cz/sluzby/bezpecnost-ict/ngfw/

[33] Hushmail - Enhanced email security to keep your data safe. Hushmail - Enhanced email security to keep your data safe [online]. Copyright © 1999 [cit. 10.08.2019]. Dostupné z: https://www.hushmail.com/

[34] JACOBSON, Gunnar. The Public Key Muddle – How to Manage Transparent End-to-end Encryption in Organizations. REIMER, Helmut, Norbert POHLMANN a Wolfgang SCHNEIDER, ed. ISSE 2015 [online]. Wiesbaden: Springer Fachmedien Wiesbaden, 2015, 2015-10-16, s. 25-35 [cit. 07.09.2019]. DOI: 10.1007/978-3-658-10934-9_3. ISBN 978-3-658-10933-2. Dostupné z: http://link.springer.com/10.1007/978-3-658-10934-9_3

[35] Joplin - an open source note taking and to-do application with synchronisation capabilities. Joplin - an open source note taking and to-do application with synchronisation capabilities [online]. Dostupné z: https://joplinapp.org/

[36] KASSEM, Jamila, Sarwar SAYEED, Hector MARCO-GISBERT, Zeeshan PERVEZ a Keshav DAHAL. DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network. Applied Sciences [online]. 2019, 9(15) [cit. 26.10.2019]. DOI: 10.3390/app9152953. ISSN 2076-3417. Dostupné z: https://www.mdpi.com/2076-3417/9/15/2953

[37] KHAIR Eddin Sabri, HAZEM Hiary, Algebraic. Model for Handling Access Control Policies. Procedia Computer Science. Volume 83. 2016. Pages 653-657. ISSN 1877-0509. Dostupné z:[cit. 06.09.2019] https://doi.org/10.1016/j.procs.2016.04.146

[38] KUNZ Michael, PUCHTA Alexander, GROLL Sebastian, FUCHS Ludwig, Günther Pernul,Attribute quality management for dynamic identity and access management. Journal of Information Security and Applications. Volume 44, 2019. Pages 64-79. ISSN 2214-2126. [cit. [cit. 06.09.2019]. https://doi.org/10.1016/j.jisa.2018.11.004

[39] LAYBATS, Claire a John DAVIES. GDPR. Business Information Review[online]. 2018, 35(2), 81-83 [cit. 11.08.2019]. DOI: 10.1177/0266382118777808. ISSN 0266-3821. Dostupné z: http://journals.sagepub.com/doi/10.1177/0266382118777808

[40] Maifence.com: This is how Mailfence provides a secure email service. Secure and private email | Mailfence encrypted email service [online]. Copyright ©2019 [cit. 10.08.2019]. Dostupné z: https://mailfence.com/en/secure-email.jsp

[41] MALGIERI, Gianclaudio. Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations. Computer Law & Security Review [online]. 2019, 35(5) [cit. 28.10.2019]. DOI: 10.1016/j.clsr.2019.05.002. ISSN 02673649. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0267364918303753

[42] MARANO, Pierpaolo. Navigating InsurTech: The digital intermediaries of insurance products and customer protection in the EU. Maastricht Journal of European and Comparative Law [online]. 2019, 26(2), 294-315 [cit. 15.8.2019]. DOI: 10.1177/1023263X19830345. ISSN 1023-263X. Dostupné z: http://journals.sagepub.com/doi/10.1177/1023263X19830345

[43] Matomo: #1 Secure Open Web Analytics Platform. Matomo: #1 Secure Open Web Analytics Platform [online]. Copyright © 2019 matomo.org [cit. 10.08.2019]. Dostupné z: https://matomo.org/

[44] MCDOWELL, Brett. Three ways in which GDPR impacts authentication. Computer Fraud & Security [online]. 2019, 2019(2), 9-12 [cit. 15.11.2019]. DOI: 10.1016/S1361-3723(19)30019-3. ISSN 13613723. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S1361372319300193

[45] Mendeley - Reference Management Software & Researcher Network. Mendeley - Reference Management Software & Researcher Network [online]. Copyright © 2019 Mendeley Ltd. All rights reserved. [cit. 09.02.2020]. Dostupné z: https://www.mendeley.com/?interaction_required=true

[46] NAUTSCH, Andreas, Abelino JIMÉNEZ, Amos TREIBER, et al. Preserving privacy in speaker and speech characterisation. Computer Speech & Language [online]. 2019, 58, 441-480 [cit. 25.10.2019]. DOI: 10.1016/j.csl.2019.06.001. ISSN 08852308. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0885230818303875

[47] NCKB. Národní úřad pro kybernetickou a informační bezpečnost: NCKB. NCKB [online]. [cit. 10.08.2019]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/hrozby/

[48] NÚKIB, a. České energetické firmy čelily cvičným kybernetickým útokům. Úvodní stránka [online]. 2019 [cit. 10.08.2019]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/aktuality/1350-ceske-energeticke-firmy-celily-cvicnym-kybernetickym-utokum/

[49] NÚKIB, b. Ministerstva, úřady i firmy vzaly varování NÚKIB vážně. Úvodní stránka [online]. 2019 [cit. 10.08.2019]. Dostupné z: https://www.nukib.cz/cs/informacni-servis/aktuality/1349-ministerstva-urady-i-firmy-provedly-predepsane-analyzy-prijimaji-opatreni-ke-snizeni-rizika/

[50] O'BRIEN, Ralph. Privacy and security. Business Information Review[online]. 2016, 33(2), 81-84 [cit. 06.08.2019]. DOI: 10.1177/0266382116650297. ISSN 0266-3821. Dostupné z: http://journals.sagepub.com/doi/10.1177/0266382116650297

[51] PHILLIPS, Mark a Bartha M. KNOPPERS. Whose Commons? Data Protection as a Legal Limit of Open Science. The Journal of Law, Medicine & Ethics [online]. 2019, 47(1), 106-111 [cit. 27.11.2019]. DOI: 10.1177/1073110519840489. ISSN 1073-1105. Dostupné z: http://journals.sagepub.com/doi/10.1177/1073110519840489

[52] PRISMA Diagram Generator. PRISMA Diagram Generator [online]. Dostupné z: http://prisma.thetacollaborative.ca/

[53] ProtonMail. Secure email: ProtonMail is free encrypted email.. Secure email: ProtonMail is free encrypted email. [online]. Copyright © 2019 Proton Technologies AG. All Rights Reserved. [cit. 10.08.2019]. Dostupné z: https://protonmail.com/

[54] ProtonVPN: Secure and Free VPN service for protecting your privacy. ProtonVPN: Secure and Free VPN service for protecting your privacy [online]. Dostupné z: https://protonvpn.com/Areknawo . The state of web analytics. Areknawo [online]. Copyright ©2019 [cit. 10.08.2019]. Dostupné z: https://areknawo.com/the-state-of-web-analytics/

[55] PSP. Poslanecká sněmovna parlamentu České republiky [online]. 2019 [cit. 10.08.2019]. Dostupné z: https://www.psp.cz/docs/laws/listina.html

[56] Reference | AMI Praha a.s.. AMI Praha - Softwarová řešení chytře a efektivně | AMI Praha a.s. [online]. 2014, Copyright © Copyright 1998 [cit. 06.09.2019]. Dostupné z: https://www.ami.cz/reference?solution=3

[57] SIRY, Lawrence. Cloudy days ahead: Cross-border evidence collection and its impact on the rights of EU citizens. New Journal of European Criminal Law [online]. 2019 [cit. 29.08.2019]. DOI: 10.1177/2032284419865608. ISSN 2032-2844. Dostupné z: http://journals.sagepub.com/doi/10.1177/2032284419865608

[58] SØRENSEN, Jannick Kirk a Hilde VAN DEN BULCK. Public service media online, advertising and the third-party user data business. Convergence: The International Journal of Research into New Media Technologies [online]. 2018 [cit. 06.08.2019]. DOI: 10.1177/1354856518790203. ISSN 1354-8565. Dostupné z: http://journals.sagepub.com/doi/10.1177/1354856518790203

[59] ŠKALOUDOVÁ, PH.D., Alena. Konstrukce dotazníku [online].2011, [cit. 10.09.2019]. Dostupné z: http://kps.pedf.cuni.cz/skalouda/diplom.htm

[60] Threema: What is a Threema ID? - Threema. 301 Moved Permanently [online]. Copyright © 2019 Threema GmbH [cit. 10.08.2019]. Dostupné z: https://threema.ch/en/faq/threema_id

[61] TIBCO SW STATISTICA™ Trial Download for Windows | TIBCO Software. Global Leader in Integration and Analytics Software | TIBCO Software [online]. Copyright © 2020 TIBCO Software [cit. 09.02.2020]. Dostupné z: https://www.tibco.com/resources/product-download/tibco-SW STATISTICA-trial-download-windows

[62] TROUSIL, Michal a Veronika JAŠÍKOVÁ. Úvod do tvorby odborných prací. Hradec Králové: Gaudemaus [i.e. Gaudeamus], 2014. [cit. 27.11.2019]. ISBN 978-80-7435-380-2.

[63] Tutanota: Bezpečný e-mail: Tutanota poskytuje zdarma šifrování e-mailů. Secure email: Tutanota makes free encrypted emails easy. [online]. [cit. 10.08.2019]. Dostupné z: https://tutanota.com/cs/

[64] Účet za GDPR? Podnikatele nařízení vyjde na 25 miliard korun | Hospodářská komora ČR. Úvod | Hospodářská komora ČR [online]. Copyright © 2017 [cit. 24.02.2020]. Dostupné z: https://www.komora.cz/press_release/ucet-za-gdpr-podnikatele-narizeni-vyjde-na-25-miliard-korun/

[65] Understanding the GDPR Cost of Continuous Compliance - CPO Magazine. Data Protection, Privacy and Cyber Security Leaders - CPO Magazine [online]. Copyright © 2020 Data Privacy Asia Pte. Ltd. [cit. 24.02.2020]. Dostupné z: https://www.cpomagazine.com/data-protection/understanding-the-gdpr-cost-of-continuous-compliance/

[66] ÚOOU, a. GDPR (obecné nařízení): Úřad pro ochranu osobních údajů. Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 09.08.2019]. Dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

[67] ÚOOU, b. Úřad pro ochranu osobních údajů. Absurdní rok s GDPR. [online]. 2019. Copyright © [cit. 30.08.2019]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=35982

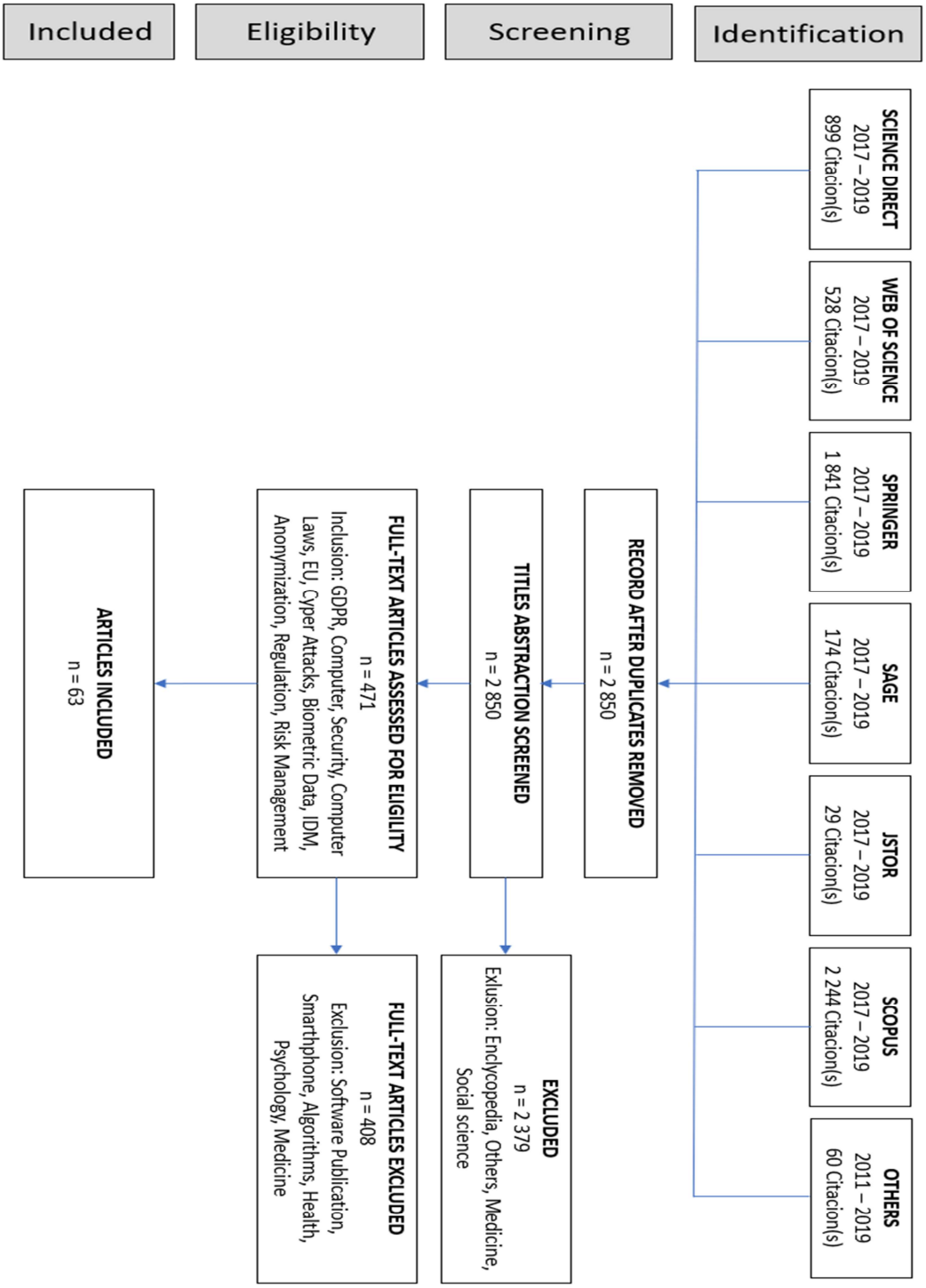
[68] VAN OOIJEN, I. a Helena U. VRABEC. Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. Journal of Consumer Policy [online]. 2019, 42(1), 91-107 [cit. 27.11.2019]. DOI: 10.1007/s10603-018-9399-7. ISSN 0168-7034. Dostupné z: http://link.springer.com/10.1007/s10603-018-9399-7

10 Přílohy

Příloha č. 1

PRISMA diagram

Zdroj: Vlastní zpracování



Příloha č. 2

Dotazník – český jazyk

Zdroj: Vlastní zpracování v Survio

survio CZ - GDPR

Příloha: dotazník

CZ - GDPR

Vážená paní, vážený pane,

jsem studentkou druhého ročníku magisterského studia Univerzity Hradec Králové v České republice, oboru Informační management a dovoluji si Vás touto cestou požádat o vyplnění anonymního dotazníku týkající se problematiky GDPR.

Vyplnění dotazníku Vám zabere přibližně 10 minut a bude sloužit jako podklad pro moji diplomovou práci, jejímž cílem je poukázat na chyby při implementaci GDPR. Dotazníkové šetření probíhá v několika zemích EU.

Srdečně děkuji za Váš čas, ochotu a vstřícnost, pokud se rozhodnete dotazník vyplnit.

S pozdravem

Šárka Kaiserová

1. Organizace, ve které pracujete, je:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Státní podnik
- ○ Soukromý podnik
- ○ Příspěvková organizace
- ○ Jiné, prosím, uveďte: ☐

2. Organizace působí v sektoru:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Veřejná správa
- ○ Zdravotnictví
- ○ Školství
- ○ Pojišťovnictví, finance
- ○ Průmysl
- ○ Stavebnictví
- ○ E-shop
- ○ Jiné, prosím, uveďte ☐

3. Celkový počet zaměstnanců:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ 10 <
- ○ 11 - 50
- ○ 51 - 250
- ○ 250 >

4. Na jaké úrovni pracujete?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Zaměstnanec
- ○ Základní (operační) management
- ○ Střední management
- ○ Top management

5. Na jakém oddělení pracujete?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ HR oddělení
- ○ IT oddělení
- ○ Účetní oddělení
- ○ Logistika
- ○ Marketing
- ○ Vedení firmy
- ○ Ostatní

6. Co je, dle vašeho názoru, GDPR?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejich občanů proti neoprávněnému zacházení s jejich daty a osobními údaji, který musí dodržovat pouze firmy se sídlem na území EU.
- ○ Právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva jejich občanů proti neoprávněnému zacházení s jejich daty a osobními údaji, který musí dodržovat všechny firmy, manipulující s daty občanů EU, místo sídla firmy není podstatné.
- ○ Právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva fyzických a právnických osob proti neoprávněnému zacházení s jejich daty a osobními údaji, který musí dodržovat pouze firmy se sídlem na území EU.
- ○ Právní rámec ochrany osobních údajů platný na celém území EU, který hájí práva fyzických a právnických osob proti neoprávněnému zacházení s jejich daty a osobními údaji, který musí dodržovat všechny firmy, manipulující s daty občanů EU, místo sídla firmy není podstatné.

7. Označte vše, co je podle vašeho názoru osobní údaj:

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Údaje typu: jméno, příjmení, adresa, telefon
- ☐ Zdravotní stav
- ☐ Biometrický údaj, např. otisk prstu, snímek krevního řečiště, scan sítnice
- ☐ Kamerový záznam
- ☐ Fotografie
- ☐ IČO, číslo účtu firmy, adresa firmy
- ☐ Služební telefonní číslo
- ☐ Obrat firmy
- ☐ Výroční zpráva
- ☐ Informace o sexuální orientaci

8. Jaké právo vám GDPR přináší?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Ochranu osobních údajů
- ☐ Právo vyžádat si všechny údaje, které o vás subjekt zpracovává
- ☐ Právo na výmaz osobních údajů
- ☐ Odmítnout zpracování osobních údajů

9. Proškolil vás zaměstnavatel v oblasti GDPR?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano, jednou
- ○ Ano, opakovaně
- ○ Ne

10. Jaké náklady firma vynaložila, aby byla v souladu s GDPR?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ 0 €
- ○ 1 – 999 €
- ○ 1 000 – 9 999 €
- ○ 10 000 – 49 999 €
- ○ 50 000 – 99 999 €
- ○ Více než 100 000 €
- ○ Nevím

11. Záznam o činnostech zpracování dat zaměstnavatel:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Má zpracovaný
- ○ Nemá zpracovaný
- ○ Nevím

12. Před použitím osobních údajů má zaměstnavatel souhlas poskytovatele:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Plně souhlasím
- ○ Částečně souhlasím
- ○ Nesouhlasím
- ○ Nevím

13. Firma má pověřence:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano
- ○ Ne
- ○ Nevím

14. Pokud ano, máte uvedeny kontaktní údaje na pověřence na:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Webových stránkách
- ○ Úřední desce
- ○ Pověřence máme, kontakt není uveden

15. Jsou osobní údaje (vaše, zákazníků) fyzicky zabezpečeny? Např. uzamčená skříň, serverovna, archiv.

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano, jsou zabezpečeny
- ○ Ne, jsou volně přístupné
- ○ Částečně jsou zabezpečeny, částečně jsou volně přístupné

16. Jak jsou zabezpečena elektronická data? (kontrolované přístupy, nahlížení na data, omezený přístup do serverovny, šifrování atd.)

Nápověda k otázce: *(1 nejméně, 5 nejvíce)*

☆☆☆☆☆ ☐ / 5

17. Jak jsou zabezpečena tištěná data? (uzamčené skříně, zásuvky, politika čistého stolu atd.)

Nápověda k otázce: *(1 nejméně, 5 nejvíce)*

☆☆☆☆☆ ☐ / 5

18. Tisk dokumentů je:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Chráněn heslem
- ○ Na tiskárnu s omezeným přístupem
- ○ Nekontrolovaný

19. Máte zabezpečen přístup na mobilní telefon a počítač?

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Ano, biometrický otisk
- ☐ Ano, číselný kód
- ☐ Ano, grafický znak
- ☐ Ne

20. Jsou data ve vašem služebním telefonu a počítači šifrovaná?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano
- ○ Ne
- ○ Nevím

21. Využívá zaměstnavatel "end-to-end" šifrování?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano
- ○ Ne
- ○ Nevím

22. Napište jméno poskytovatele zajišťující "end-to-end" šifrování.

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Tresorit
- ○ Sync.com
- ○ Boxcryptor
- ○ Jiné, prosím, uveďte: ☐
- ○ Nevím
- ○ Nepoužíváme

23. Označte, zda firma používá některý z níže uvedených systémů.

Nápověda k otázce: *Vyberte jednu nebo více odpovědí*

- ☐ Zveřejňování informací o přítomnosti zaměstnanců organizace na pracovišti
- ☐ Přístupové karty – foto, údaje
- ☐ Kamerový systém
- ☐ Vyvolávací systém
- ☐ GPS
- ☐ Ani jeden z výše uvedených

24. Dali jste svému zaměstnavateli souhlas se zpracováním dat v uvedených systémech?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano
- ○ Ne
- ○ Částečně

25. Podnikl zaměstnavatel nějaké speciální kroky v oblasti e-reklamy, např. cookies?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ne
- ○ Nevím
- ○ Nepoužíváme
- ○ Ano

26. Ano, uveďte jaké.

27. Ohodnoťte následující tvrzení: Přístupy zaměstnanců jsou zcela pod kontrolou.

Nápověda k otázce: *(1 nejméně pravdivé, 5 nejvíce pravdivé)*

☆☆☆☆☆ ☐ / 5

28. Ohodnoťte následující tvrzení: Zaměstnanci mají přístup do původních systémů i po změně pozice.

Nápověda k otázce: *(1 nejméně pravdivé, 5 nejvíce pravdivé)*

☆☆☆☆☆ ☐ / 5

29. Ohodnoťte následující tvrzení: Zaměstnanec má k dispozici vždy a včas pouze přístupy, které potřebuje.

Nápověda k otázce: *(1 nejméně pravdivé, 5 nejvíce pravdivé)*

☆☆☆☆☆ ☐ / 5

30. Používá firma anonymizaci a pseudoanonymizaci dat?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano
- ○ Ne
- ○ Nevím

31. Využívá vaše firma kontakty ze zakoupené databáze k direct mailingu?

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Ano, v e-mailu je uveden odkaz pro odhlášení z rozesílky
- ○ Ano, v e-mailu není uveden odkaz pro odhlášení z rozesílky
- ○ Ne
- ○ Nevím

32. Při hromadném rozesílání e-mailů zákazníkům, dodavatelům jsou:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Adresáti jsou viditelní v hlavičce e-mailu
- ○ Adresáti jsou ve skryté kopii
- ○ E-maily jsou rozesílány každému jednotlivě

33. Napište jméno poskytovatele VPN:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ProtonVPN
- ○ AirVPN
- ○ Jiné, prosím, uveďte: ☐
- ○ Nevím
- ○ Nepoužíváme

34. Pro firemní komunikace se používá:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Signal
- ○ WhatsApp
- ○ Threema
- ○ Messenger
- ○ Jiné, prosím, uveďte: ☐
- ○ Nepoužíváme

35. Poskytovatel pro e-mailovou komunikaci je:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ ProtonMail
- ○ Hushmail
- ○ Tutanota
- ○ Mailfance
- ○ Microsoft Outlook
- ○ Zoho Mail
- ○ Jiné, prosím, uveďte: ☐
- ○ Nepoužíváme

36. Pro teamovou spolupráci se využívá:

Nápověda k otázce: *Vyberte jednu odpověď*

- ○ Wire
- ○ Trello
- ○ Capterra
- ○ Slack
- ○ Jiné, prosím, uveďte: ☐
- ○ Nepoužíváme

37. GDPR vám osobně: Zvýšilo administrativu v zaměstnání

Nápověda k otázce: *(1 ne, 5 ano)*

☆☆☆☆☆ ☐ / 5

38. GDPR vám osobně: Poukázalo na hrozby a rizika úniku a zneužití dat

Nápověda k otázce: *(1 ne, 5 ano)*

☆☆☆☆☆ ☐ / 5

39. GDPR vám osobně: Zvýšil pocit kontroly nad vašimi osobními údaji

Nápověda k otázce: *(1 ne, 5 ano)*

☆☆☆☆☆ ☐ / 5

40. GDPR vám osobně: Zajistilo pocit bezpečí a ochrany dat

Nápověda k otázce: *(1 ne, 5 ano)*

☆☆☆☆☆ ☐ / 5

Velice Vám děkuji za vyplnění dotazníku :)

Příloha č. 3

Zadání diplomové práce

Zadání diplomové práce

Autor:	**Bc. Šárka Kaiserová**
Studium:	I1800349
Studijní program:	N6209 Systémové inženýrství a informatika
Studijní obor:	Informační management
Název diplomové práce:	**Identifikace problémů při implementaci GDPR**
Název diplomové práce AJ:	Identification of issues during the GDPR implementation

Cíl, metody, literatura, předpoklady:

1. Definovat jasné cíle práce a hypotézy
2. Stanovit metodiku zpracování
3. Literární rešerše, teoretická východiska práce
4. Praktická část práce
5. Shrnutí výsledků
6. Závěry a doporučení

1. ÚOOU. GDPR (obecné nařízení): *Úřad pro ochranu osobních údajů: Titulní stránka [online]. Copyright ? 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 09.08.2019]. Dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938*
2. *BOLOGNINI, Luca a Camilla BISTOLFI. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. Computer Law {\& Security Review [online]. 2017,* ***33(2), 171-181 [cit. 2019-08-06]. DOI: 10.1016/j.clsr.2016.11.002. ISSN 02673649. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0267364916302151***
3. ***DUNCAN, Bob a Yuan ZHAO. Risk Management for Cloud Compliance with the EU General Data Protection Regulation. In: 2018 International Conference on High Performance Computing {\& Simulation (HPCS) [online]. IEEE, 2018, 2018, s. 664-671 [cit. 2019-08-06]. DOI: 10.1109/HPCS.2018.00109. ISBN 978-1-5386-7878-7. Dostupné z: https://ieeexplore.ieee.org/document/8514414/***

Garantující pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	doc. Ing. Vladimír Bureš, Ph.D., MBA
Datum zadání závěrečné práce:	21.10.2014