Západočeská univerzita v Plzni
Fakulta ekonomická

Dopady implementace GDPR na klíčové činnosti a management rizik malých e-shopů v České republice

Ing. Adam Faifr

disertační práce
k získání akademického titulu doktor
v oboru Ekonomika a management

Školitel: doc. Ing. Jiří Vacek, Ph.D.

Katedra podnikové ekonomiky a managementu

Plzeň 2023

University of West Bohemia
Faculty of Economics

Impacts of GDPR implementation on core activities and risk management of small e-shops in the Czech republic

Ing. Adam Faifr

Ph.D. thesis
for academic degree doctor
in the study field Economics and Management

Supervisor: doc. Ing. Jiří Vacek, Ph.D.

Department of Business Administration and Management

Plzeň 2023

Poděkování

Rád bych na tomto místě poděkoval panu doc. Ing. Jiřímu Vackovi, Ph.D. za jeho vstřícnost, odborné vedení, cenné připomínky a rady, které mi byly velmi nápomocné v průběhu celého studia a při vypracování této disertační práce.

Poděkování na tomto místě patří rovněž kolegům z Fakulty ekonomické, konkrétně pak kolegům z Katedry podnikové ekonomiky a managementu za odbornost a spolupráci, která mi při zpracování této práce byla inspirací i podporou.

Za bezmeznou a neutuchající podporu nakonec děkuji své nejbližší rodině, bez níž by zpracování této práce nebylo možné.

Anotace

Disertační práce se zabývá dopady implementace Obecného nařízení o ochraně osobních údajů, kdy si autor klade za cíl vymezit dopady implementace na řízení klíčových činností malých e-shopů v České republice. Současně se autor klade za cíl empiricky ověřit dříve vymezené teoretické souvislosti mezi problematikou GDPR a oblastí řízení rizik. K řešení problematiky je využit explorativní sekvenční design smíšeného výzkumu, kdy je nejprve proveden kvalitativní sběr a analýza dat za účelem upřesnění metrik pro následnou kvantitativní část výzkumu. V úvodních dvou kapitolách jsou kromě hlavního výzkumného cíle definovány také dílčí výzkumné cíle a je představen metodický přístup k jejich řešení. V navazující třetí kapitole jsou vymezena teoretická východiska, jako základ pro upřesnění následně prováděných výzkumných šetření. Vedle problematiky ochrany osobních údajů, GDPR a jeho implementace v podnikové praxi autor v této části představuje problematiku elektronického podnikání, e-shopů a současných přístupů k řízení rizik v kontextu výzkumné oblasti. V kapitolách čtyři až šest jsou představena jednotlivá výzkumná šetření, jejich metodika a zjištěné poznatky. V kapitole čtyři jsou uvedeny výsledky provedené mnohostranné literární rešerše mapující současné poznání v oblasti implementace GDPR a jejích důsledků pro činnost podniků se zaměřením na malé podnikatelské subjekty. Výsledky provedené vícenásobné případové studie zpracované na případu třech malých českých e-shopů jsou prezentovány v navazující kapitole pět, kdy jsou popsány a s ohledem na předchozí poznatky ověřeny přístupy využívané k implementaci GDPR touto skupinou podniků. Kvantitativní část výzkumu je pak tvořena provedeným dotazníkovým šetřením, jež na základě upřesnění z předchozích částí zkoumá, které činnosti v rámci implementace GDPR provádějí malé e-shopy a jaké jsou souvislosti mezi implementací GDPR a vyspělostí managementu rizik malých e-shopů v České republice. Současně zkoumány faktory, které mají na zmíněné oblasti vliv. V kapitolách sedm a osm jsou následně shrnuty a diskutovány disertačním výzkumem dosažené výsledky a jsou představeny důsledky jak pro oblast praxe, tak oblast akademickou, a to včetně nastínění možného budoucího směřování výzkumu v oblasti dopadů GDPR na podnikovou praxi. Práce jako celek poskytuje syntézu současného poznání v oblasti dopadů implementace GDPR a doplňuje je o dopady a přístupy k implementaci v realitě malých e-shopů, stejně jako přináší kvantitativní zhodnocení dříve teoreticky definovaného vztahu mezi GDPR a managementem rizik.

Klíčová slova: dopady GDPR, implementace GDPR, řízení rizik, vyspělost managementu rizik, malé e-shopy, klíčové činnosti

Annotation

The dissertation deals with the impacts of GDPR implementation, where the author´s goal is to define the impacts of the implementation on core activities of small e-shops in the Czech Republic. At the same time, the author aims to empirically validate the previously defined theoretical link between the GDPR and the area of risk management. An exploratory sequential mixed research design is used to address the issue, where qualitative data collection and analysis is first conducted in order to refine the metrics for the subsequent quantitative part of the research. In the first two chapters, in addition to the main research objective, the sub-research objectives are defined and the methodological approach to addressing them is presented. In the following third chapter, the theoretical background is defined as a basis for refining the subsequent research investigations. In addition to the issues of personal data protection, GDPR and its implementation in corporate practice, the author presents in this section the issues of e-commerce, e-shops and current approaches to risk management in the context of the research area. Chapters four to six present the individual research investigations, their methodology and resulting findings. Chapter four presents the results of a multivocal literature research conducted to map the current knowledge in the area of GDPR implementation and its implications for business activities with a focus on small businesses. The results of the multiple case study conducted on the case of three small Czech e-shops are presented in the following chapter five, where the approaches used to implement the GDPR by this group of businesses are described and verified with respect to previous findings. The quantitative part of the research consists of a questionnaire survey, which, based on the refinement of the previous sections, examines which activities within the GDPR implementation are carried out by small e-shops and what are the links between GDPR implementation and the maturity of risk management of small e-shops in the Czech Republic. The factors influencing the mentioned areas are examined as well. Chapters seven and eight subsequently summarise and discuss the results achieved by the dissertation research and present a consequences for both practice and academia, including an outline of future research directions in the area of GDPR's impacts on business activities. The thesis as a whole provides a synthesis of current knowledge in the area of GDPR implementation impacts and adds new findings in the field of impacts and approaches to implementation GPDR in the reality of small e-shops, as well as brings a quantitative assessment of the theoretically defined relationship between GDPR and risk management.

Keywords: GDPR impacts, GDPR implementation, risk management, risk management maturity, small e-shops, core activities

Čestné prohlášení

Prohlašuji, že jsem disertační práci na téma

„*Dopady implementace GDPR na klíčové činnosti a management rizik malých e shopů v České republice*“

vypracoval samostatně pod odborným dohledem školitele za použití pramenů uvedených v přiložené bibliografii.

Plzeň dne……

.....

podpis autora

Obsah

Seznam tabulek

Seznam obrázků

Seznam zkratek

APEK – Asociace pro elektronickou komerci

B2B – business-to-business

B2C – business-to-customer

BI – Business Intelligence

BPM – procesní řízení (Business Process Management)

BPMN – grafická notace sloužící k modelování podnikových procesů (Business Process Model and Notation)

CASI - Computer Assisted Self Interviewing

CEO – Ředitel společnosti (Chief executive officer)

CMM – Model vyspělosti CMM (Capability Maturity Model)

CMMI – Model vyspělosti CMMI (Capability Maturity Model Integration)

DPA – národní úřad pro ochranu osobních údajů v Evropské Unii (Data Protection Authority)

DPIA – Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment)

DPO – Pověřenec pro ochranu osobních údajů (Data Protection Officer)

EAM – Enterprisse Architecture Management

EC – Evropská komise (European Commission)

EP – Evropský parlament (European Parliament)

ERM – Podnikové řízení rizik (Enterprise Risk Management)

ES – Evropské společenství (European Community)

EU – Evropská unie (European Union)

EUC – Rada Evropské unie (The Council of the European Union)

FRA – Agentura Evropské unie pro základní práva (European Union Agency for fundamental Rights)

GDPR – Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)

HR – lidské zdroje (human resources)

ICT – Informační a komunikační technologie (Information & communication technologies)

ISO – Mezinárodní organizace pro normalizaci (International Organization for Standardization)

IT – Informační technologie (Information Technology)

K-W – Kruskalův-Wallisův test (Kruskal-Wallis test)

MLR – Mnohostranná literární rešerše (Multivocal literature review)

MMR – Ministerstvo pro místní rozvoj České republiky (Ministry of Regional Development of Czech republic)

MPO – Ministerstvo průmyslu a obchodu České republiky (Ministry of Industry and trade of Czech republic)

MSP – Malý a střední podnik

NACE – Klasifikace ekonomických činností vydávaná Evropskou komisí (Statistical Classification of Economic Activities in the European Community)

OÚ – Osobní údaj (Personal data)

PMMM – Model vyspělosti projektového řízení (Project management maturity model)

PRM – Vyspělost managementu projektových rizik (Project Risk Maturity)

PRMM – Model vyspělosti managementu projektových rizik (Project Risk Management Maturity)

QDA – kvalitativní analýza dat (Qualitative Data Analysis)

RM – Řízení rizik (Risk Management)

s.r.o. – společnost s ručením omezeným

SLR – Systematická literární rešerše (Systematic literature review)

SVO – Specifická výzkumná otázka

SW – software

S-W test – Shapiro-Wilkův W test (Shapiro-Wilk W test)

UML – jazyk pro vizualizaci, specifikaci, navrhování a dokumentaci programových systémů (Unified Modeling Language)

ÚOOÚ – Úřad na ochranu osobních údaj

VO – Výzkumná otázka

WoS - Web of Science

Úvod

Podle průzkumu Evropské komise z roku 2019 (Evropská komise [EC], 2019b) má 62 % občanů Evropské unie [EU] pochybnosti týkající se zneužívání osobních údajů, jež poskytují on-line. I vzhledem k neustálému nárůstu lidí využívajících internet, potažmo nárůstu nákupů na internetu (EC, 2019b), stává se zajišťování soukromí zákazníků důležitým aspektem každé podnikající firmy v segmentu B2C, kdy i na podkladu dřívějších poznatků má faktor zabezpečení soukromí vliv na to, jak je společnost vnímána zákazníkem (Annant et al., 2020; Bleier et al., 2020).

Kromě tohoto marketingového aspektu EU přijala v květnu 2016 nařízení, které poskytuje všem občanům EU větší a jednotnou ochranu jejich osobních údajů. Nařízení známé jako Obecné nařízení o ochraně osobních údajů [GDPR] se stalo účinným v květnu 2018. Ačkoliv GDPR legitimně zvyšuje práva občanů v oblasti kontroly vlastních osobních údajů, je zřejmé, že dílčí požadavky, jež z nařízení explicitně či implicitně vyplývají, mají dopad na řízení podnikatelských subjektů.

Povinností každé právnické i fyzické osoby, která zpracovává jakékoliv osobní údaje občanů EU, je nyní bez ohledu na její velikost, výši obratu či technologické, finanční nebo organizační zázemí zapracovat stovky stránek právního textu a s tím související přístup Privacy by Design[1] do všech svých aktivit, v jejichž rámci dochází ke zpracování osobních údajů. Nebo být na druhé straně vystaven riziku vysoké pokuty či reputačním rizikům. Zároveň platí, že nařízením není definován konkrétní postup, jak požadovaného stavu ochrany osobních údajů dosáhnout (Garber, 2018; Tankard, 2016).

Výsledky provedených šetření z období kolem nabytí účinnosti poukazují na poměrně vysokou nepřipravenost na novou regulaci, kdy jen menší část malých organizací v době nabytí účinnosti GDPR implementovala (Faifr & Januška, 2018; Perry, 2019). Právě tato skupina podniků se potýkala a stále potýká s řadou omezení, které věcnou implementaci i s ohledem na časovou i finanční investici buďto ztěžují nebo i znemožňují (Lindgren, 2018). Překážkou mohou být také nedostatečné právní či technické dovednosti této skupiny firem (Garber, 2018). Bleier et al. (2020) v tomto ohledu upozorňují, že jen málo

[1] Privacy by design je přístup, jehož cílem je zabudovat platné požadavky na ochranu osobních údajů do všech operací, v jejichž rámci dochází ke zpracování osobních údajů. Jedná se jak o používané informační systémy, tak i konkrétní operace zpracování a podnikové procesy (European Data Protection Supervisor, n.d.a).

byly akcentovány charakteristiky především malých podniků při přijímání nové regulace. V tomto ohledu následně Gal & Aviv (2020) také zmiňují, že přijímání obdobných regulací může vést k nezamýšleným a dosud nepoznaným negativním účinkům na hospodářskou soutěž a inovace.

Po téměr pěti letech od doby, kdy GDPR vstoupilo v platnost a musí se jejími požadavky řídit (nejen) podniky v Evropské Unii, není dosud souhrnně zmapováno, jaký dopad měla nová regulace na řízení dotčených subjektů, jakým způsobem bylo v daných subjektech GDPR implementováno. Pokud zároveň GDPR explicitně uvádí vazbu na řízení rizik, pak není jasné, jak se implementace GDPR projevuje právě v této oblasti (Voigt & von dem Bussche, 2017; Sharma, 2020). Zároveň není zřejmé, nakolik byly naplněny proklamované pozitivní synergické dopady na podnikové procesy v případě úspěšné implementace (Beckett, 2017; Garber, 2018; Hofman et al., 2019).

Vzhledem k počtu a heterogenitě dotčených subjektů, kdy implementace GDPR vychází z organizačního kontextu (Evropský parlament & Rada Evropské unie [EP & EUC], 2016, důvody č. 60, č. 74, č. 76 či č. 90), bude zkoumání dopadů implementace GDPR na klíčové aktivity a management rizik omezeno na skupinu **malých e-shopů v České republice**[2], jakožto specifického segmentu obchodních podniků, které zpracování osobních údajů nejen v on-line prostředí intenzivně provádějí.

Předložená disertační práce zapracovává autorova šetření v oblastech ochrany osobních údajů a managementu rizik (Faifr & Januška, 2018; Faifr, 2020; Faifr, 2021; Faifr & Januška, 2021; Faifr, 2022). S ohledem na náležitosti této práce je její text členěn následujícím způsobem. V **kapitole 1** jsou prezentovány cíle disertační práce. V navazující **kapitole 2** je následně prezentován metodický přístup k řešení výzkumného projektu. V **kapitole 3** jsou prezentována teoretická východiska sloužící k upřesnění zkoumané skupiny podniků a designu dílčích výzkumných šetření. Výsledky provedených výzkumných šetření jsou následně prezentovány v **kapitolách 4, 5 a 6**. V závěru této disertační práce jsou následně diskutovány hlavní výstupy práce, doporučení a východiska, která z práce vyplývají, pro oblast akademickou, pedagogickou i praxi.

[2] Dle poznatků autora (Faifr & Januška, 2021) se odlišují přístupy k implementaci GDPR u organizací dle jejich velikosti, dle typu a rozsahu zpracovávaných osobních údajů a dle typu právnické osoby (veřejnoprávní právnické osoby a soukromé právnické osoby).

1 Cíle výzkumu

Definice cíle (účelu) výzkumu vyjadřuje ve větě nebo několika větách celkový záměr či hlavní myšlenku navrhované studie (Creswell, 2013). Hlavním cílem této disertační práce je: „**Vymezit dopady na řízení klíčových aktivit a management rizik malých e-shopů[3] v České republice v důsledku implementace požadavků definovaných v Obecném nařízení o ochraně osobních údajů.**“

Pro splnění definovaného cíle je záměr výzkumu následně dekomponován do postupných dílčích výzkumných cílů následovně:

I. Na základě relevantních zdrojů vymezit současné poznání v oblasti implementace GDPR a jejích důsledků na činnosti a oblasti podniků se zaměřením na malé podniky.
II. Popsat a ověřit možné přístupy vedoucí k implementaci GDPR v malých e-shopech s uvážením kritických faktorů.
III. Popsat a zhodnotit souvislosti mezi implementací GDPR a oblastí řízení rizik se zaměřením na malé e-shopy v České republice.

K přijetí GDPR došlo na jaře 2016, přičemž v účinnost vešlo v květnu 2018 (EP& EUC, 2016). I proto, že se tématem dopadů a implementace GDPR zabývají podniky i související vědecká zkoumání takřka výhradně v posledních sedmi, potažmo pěti, letech, je první a základní dílčí cíl definován s ohledem na stále se rozvíjející a neucelené teoretické poznatky v této oblasti. Vzhledem ke specifičnosti zkoumané skupiny malých e-shopů a v důsledku toho možným limitům v dostupnosti relevantních informací, je toto zkoumání zobecněno na skupinu malých podniků.

Zbývající dva dílčí cíle jsou definovány v návaznosti na cíl první. Jejich smyslem je existující teoretické poznatky validovat a rozšířit o nové empirické poznatky v oblasti praktických dopadů GDPR na řízení sledovaných aktivit, kdy vzhledem k dikci nařízení bude důraz kladen rovněž na kvantifikaci dopadů v oblasti managementu rizik.

[3] Upřesnění pojmu „malý e-shop“, který je v této práci využit pro vymezení zkoumané skupiny, je na základě předchozí rešerše a klasifikace uveden v kapitole 3.1.6.

Výše uvedené dílčí cíle jsou dále převedeny do několika konkrétních dílčích výzkumnůch úkolů v následující struktuře (cíl – úkol):

- **Cíl 1 - úkol 1**: Představení Obecného nařízení o ochraně osobních údajů v kontextu řízení podniků.
- **Cíl 1 - úkol 2**: Vymezení dopadů implementace GDPR na provádění s touto problematikou souvisejících činností.
- **Cíl 1 - úkol** 3: Shrnutí dosavadních poznatků v oblasti provádění implementace GDPR malými podniky.
- **Cíl 2 - úkol 1**: Představení možných způsobů a přístupů k implementaci GDPR malými e-shopy.
- **Cíl 2 - úkol 2**: Ověření využití definovaných přístupů k implementaci v praxi malých e-shopů.
- **Cíl 2 - úkol 3**: Vymezení kritických faktorů a bariér implementace GDPR u malých e-shopů.
- **Cíl 3 - úkol 1**: Vymezení vztahu mezi implementací GDPR a managementem rizik.
- **Cíl 3 - úkol 2**: Vymezení existujících přístupů k hodnocení managementu rizik v podniku.
- **Cíl 3 - úkol 3**: Zhodnocení důsledků pro management rizik v souvislosti s implementací GDPR v prostředí malých e-shopů.

Na základě teoretické části a výstupů z realizovaných empirických šetření budou formulovány dopady implementace GDPR na řízení malých e-shopů v České republice, a to se zaměřením na jejich klíčové aktivity a oblast řízení rizik. Práce obsahuje spolu s rešerší literatury i dílčí výzkumná šetření. V jejich rámci jsou formulovány dílčí výzkumné otázky a jsou konkretizovány použité metody (Creswell, 2013).

2 Design výzkumu

V souladu s definicí hlavních i dílčích cílů je pro výzkum vybraného tématu zvolena strategie smíšeného výzkumu (Eger & Egerová, 2014). Výzkum smíšený je takový výzkum, který kombinuje alespoň jeden aspekt kvantitativní s alespoň jedním aspektem kvalitativním (Creswell, 2013). Dle Creswella (2013) tento přístup umožňuje lepší pochopení výzkumného problému, než které by poskytlo jediné ze dvou výše zmíněných paradigmat.

Na základě dělení metod smíšeného výzkumu dle Creswella (2013) se jedná o **explorativní sekvenční výzkum**, kdy je nejprve proveden kvalitativní sběr a analýza dat, aby byly následně takto získané výsledky využity v následující kvantitativní části. Tento přístup je zvolen vzhledem k rozvíjejícímu se teoretickému rámci za účelem upřesnění metrik v části kvantitativní a umožňuje ověřit, zda zákonitosti platné pro užší vzorek lze zobecnit i na vzorek velký (Creswell, 2013).

V této práci lze kvalitativní část výzkumu rozdělit na část teoretickou a empirickou. Teoretická část sestává ze **standardizovaného sběru a analýzy sekundárních dat**, kdy se jedná o knihy, relevantní studie a články publikované komerčními subjekty či články a rešeršemi uvedenými v databázi Web of Science. Metodika tohoto šetření bude blíže představena v **kapitole 4.1.** Poznatky získané tímto zkoumáním jsou pak podkladem jak pro kvalitativní, tak kvantitativní empirickou část.

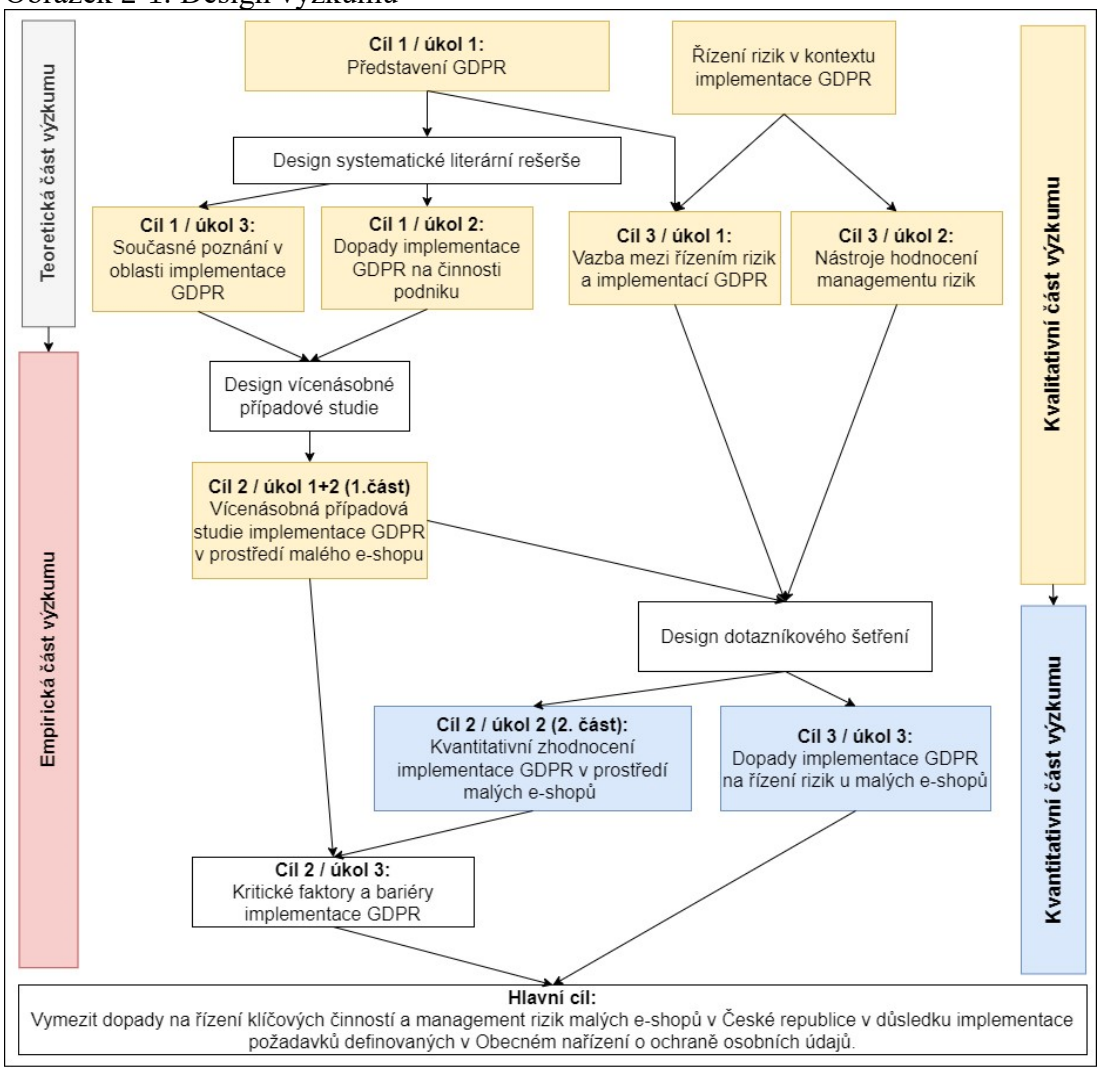
Kvalitativní empirickou část výzkumu v tomto případě tvoří **vícenásobná případová studie**. Yin (2014) tento přístup doporučuje v případě, kdy nejsou jednoznačně vymezeny hranice mezi zkoumaným fenoménem (GDPR a jeho implementace) a kontextem reálného prostředí (podnikání na internetu, realita malých podnikatelských subjektů). Návrh vícenásobné případové studie je představen v **kapitole 5.1** a navazujících podkapitolách.

Výstupy obou výše zmíněných kvalitativních šetření jsou pak podkladem pro upřesnění designu kvantitativního výzkumného šetření, jehož smyslem je zhodnocení a popsání vztahů mezi implementací GDPR a podnikovým řízením rizik. Součástí této části práce je i kvantitativní zkoumání implementace GDPR ve skupině malých e-shopů i faktorů, jež rozsah implementace ovlivňují. Data pro kvantitativní část budou získána **dotazníkovým šetřením**. Analyzována a hodnocena pak jsou prostřednictvím vybraných

statistických metod. Jejich výběr je přizpůsoben s ohledem na předchozí dílčí výstupy disertační práce. Návrh dotazníkového šetření je představen v **kapitole 6.1.**

Výše představený přístup k výzkumu a postup zpracování je ilustrován následujícím obrázkem 2-1, kde jsou barevně rozlišeny části výzkumu dle výzkumné strategie (kvalitativní/kvantitativní) a výzkumné metody (teoretická/empirická část). Žlutě jsou vyznačena kvalitativní šetření a rešerše, modrá barva je použita pro označení empirické části výzkumu.

Obrázek 2-1: Design výzkumu



Zdroj: vlastní zpracování

3 Východiska pro výzkum

V této kapitole budou shrnuta teoretická i empirická východiska v oblasti elektronického obchodování a zkoumané skupiny podniků, zajišťování soukromí a implementace GDPR v podnicích. Vzhledem k tomu, že existuje přímá souvislost s managementem rizik (Voigt & von dem Bussche, 2017; Sharma, 2020), je součásti této části i prezentace současných poznatků v této oblasti řízení, a to v kontextu tématu výzkumu.

3.1 Charakteristiky e-commerce maloobchodu

Jedním z důvodů (důvod 13) přijetí Obecného nařízení na ochranu osobních údajů (zkráceně GDPR) v roce 2016 byla potřeba harmonizovat právní úpravu ochrany osobních údajů na území Evropské unie (EP & EUC, 2016, důvod č. 13), kdy ze své podstaty má nařízení právně závazné důsledky pro všechny podnikatelské subjekty a instituce bez ohledu na jejich velikost či odvětví, ve kterém působí, za předpokladu, že tyto subjekty zpracovávají osobní údaje občanů Evropské unie (EP & EUC, 2016). Vzhledem k počtu a heterogenitě takto dotčených subjektů, kdy implementace GDPR má vycházet z organizačního kontextu (EP & EUC, 2016, důvody č. 60, č. 74, č. 76 či č. 90), bude zkoumání dopadů implementace GDPR na klíčové činnosti omezeno na skupinu **maloobchodních malých e-shopů v České republice**. Níže v této kapitole bude vybraná skupina podniků charakterizována.

3.1.1 Definice pojmu e-commerce

Pro potřeby této disertační práce bude nejprve definován pojem e-commerce jakožto pojem, který je významově nadřazený pojmu e-shop, a budou popsány hlavní charakteristiky elektronického obchodování.

Vývoji významu a různému výkladu pojmu „e-commerce“ se ve své práci například věnovala Kunešová (2017), která poukazuje na vývoj v souvislosti s rozvojem informačních a komunikačních technologií. Základní definicí používanou pro potřeby této práce bude definice dle Eurostat (2015): „*E-commerce může být obecně definováno jako prodej nebo nákup zboží nebo služeb mezi podniky, domácnostmi, jednotlivci nebo soukromými organizacemi, a to prostřednictvím elektronických transakcí prováděných přes internet nebo prostřednictvím jiných počítačových (on-line komunikačních) sítí. E-commerce zahrnuje objednávání zboží a služeb prostřednictvím počítačových sítí; placení a konečné dodání zboží nebo služeb může být prováděno online nebo offline.*“

OECD (2019) ve svém reportu k tomuto upřesňuje, že o zařazení určitého obchodu jakožto elektronického rozhoduje primárně využitá metoda pro objednání zboží či služby, nikoliv charakteristiky samotného produktu, konkrétní subjekty, které se podílejí na obchodu či využitý způsob doručení (OECD, 2019). Rozhodujícím by rovněž neměl být způsob provedení platby (Statistics Canada, 2016). Obdobně je pojem e-commerce definován i dalšími autory (Plunkett, 2017; Qin et al., 2022; Heinemann, 2023).

Dle Laudon & Traver (2022) se pak každý e-commerce podnikatelský model skládá z osmi základních elementů, a totiž hodnotové nabídky (value proposition), příjmového modelu (revenue model), tržní příležitostí, konkurenčního prostředí, konkurenční výhody, organizačního rozvoje (organization development) a tržní strategie.

3.1.2 Klasifikace e-commerce subjektů

Elektronický obchod lze dále klasifikovat dle různých kritérií. Základní členění hovoří o rozdělení dle na obchodu se zúčastněných subjektů (prodávajícího a kupujícího), dle geografické působnosti e-commerce subjektu, dle podílu elektronického obchodu na tržbách společnosti. Dále lze e-commerce subjekty dělit dle přístupnosti.

V následující části bude provedena charakteristika jednotlivých dělení:

- **Dle zúčastněných subjektů**

Jak již bylo zmíněno v předchozí podkapitole, elektronický obchod probíhá vždy mezi dvěma různými subjekty. Tyto modely se dále dělí na:

  - B2B – Business-to-business – interakce mezi dvě podnikatelskými subjekty
  - B2C – Business to consumer – interakce mezi podnikatelských subjektem a spotřebitelem
  - C2B – Consumer-to-business
  - C2C – consumer to consumer – interakce mezi dvěma spotřebiteli (Kunešová, 2017, Laudon & Traver, 2022, Heinemann, 2023)

Nejčastěji uváděným případem elektronického obchodování je situace, kdy dochází k obchodu mezi spotřebitelem a podnikatelským subjektem (B2C). Rozšířením o další subjekty se pak možné e-commerce modely rozšiřují o interakci mezi institucemi veřejné správy („G“), zaměstnanci („E“) či uživateli („P“) (OECD, 2019; Qin et al., 2022; Turban et al. 2018).

- **Dle geografické působnosti**

Další možnou klasifikací je dle Kunešové (2017) rozdělení dle působnosti daného e-commerce subjektu, a to na:

  - Lokální – působnost v části jedné národní ekonomiky
  - Domácí – působnost na území celé národní ekonomiky
  - Přeshraniční – působnost ve více než 1 zemi
  - Globální (Kunešová, 2017)

Heinemann (2023) pak dále klasifikuje e-commerce **dle zdroje příjmů společnosti** na:

  - Pure online trading (čistě internetový obchod) – veškeré tržby jsou tvořeny v on-line prostředí
  - Cooperating Online trade – primárně internetový obchody s využitím ostatních prodejních kanálů
  - Multi-channel commerce (také nazývaný jako „bricks-and-clicks“) – primárně „kamenný obchod“ s využitím on-line prodeje
  - Hybrid on-line trading – kombinace jiného off-line prodejního kanálu (například katalog, TV etc.) a on-line prodeje bez „kamenného obchodu“
  - Vertical on-line trade – výrobce prodávající své zboží zákazníkovi přímo pomocí on-line platformy. Také popisován jako model D2C („Direct-to-Consumer“) (Heinemann, 2023; Laudon & Traver, 2022; Olbrich et al., 2019; Turban et al al., 2018)

Alternativou vůči této klasifikaci je řazení dle Kunešové (2017), která dělí elektronické obchody na čistou e-commerce (veškerý obchod včetně produktů a jejich doručení je elektronické povahy) a částečnou e-commerce (ty se dále dělí na kvazielektronické B2C obchody a plnohodnotné B2B obchody).

Posledním používaným typem klasifikace je pak členění elektronických obchodů **na obchod na otevřených sítích na uzavřených sítích**, kdy je obchod přístupný jen pro uzavřenou skupinu subjektů (Kunešová, 2017).

3.1.3 Elektronický maloobchod

Laudon & Traver (2022) uvádí on-line maloobchod jako jednu ze sedmi forem maloobchodu.[4] Současný e-commerce maloobchod je charakterizován různorodostí obchodních modelů, kdy dochází k jejich dalšímu vývoji, a to ve dvou směrech:

- Nové obchodní modely mohou umožnit provádět více transakcí on-line na daném trhu nebo pro danou skupinu účastníků.
- Nové obchodní modely mohou umožnit vznik zcela nových trhů pro zboží a služby, které dříve nebylo možné koupit nebo prodat on-line, nebo umožnit novým účastníkům na existující on-line trh vstoupit (OECD, 2019).

Nejen v poslední dekádě s ohledem na technologický vývoj tak dochází ke kontinuálnímu nárustu internetového obchodu, kdy širší využití nachází **on-line obchod u malých firem**. Mezi lety 2010 až 2017 činil podíl tržeb získaných v rámci e-commerce u malých podniků 53 % v porovnání s firmami středními (35 %) a velkými (30 %) (OECD, 2019). Ke kontinuálnímu nárůstu dochází ovšem u všech zmíněných skupin podnikatelských subjektů.

V kontextu využití e-commerce v prostředí společností lze dále sledovat i rozvoj smíšených obchodních modelů, které kombinují jak on-line, tak off-line formy prodeje (OECD, 2019; Heinemann, 2023). Vývoj smíšených modelů je dle pozorování viditelný jak u původně čistě elektronických obchodů, tak na druhé straně původně „off-line" maloobchodníků, kdy cílem je kombinovat a synergicky využívat výhody obou těchto modelů (Plunkett, 2023). OECD (2019) v tomto směru zmiňuje, že dochází k postupnému rozostření hranic mezi tím, kdy lze **obchod považovat za čistě on-line a čistě off-line**. Qin et al. (2022) tento model nazývají specificky jako O2O.

V případě původně internetových obchodů (pure online trading) se jedná o rozšíření do fyzických obchodů (Schneider, 2017; OECD, 2019) či kombinaci e-shopu a distribuce katalogů (Schneider, 2017; Turban et al., 2017). Rostoucí používání kombinace on-line a off-line distribučních modelů zároveň znamená, že kamenné obchody stále více plní funkce, které přesahují prostý nákup produktů na místě (OECD, 2019). Dále je zmiňován příklad výrobních společností, jimž on-line obchod umožňuje přímý prodej zákazníkům (Turban et al. 2017).

[4] Dále se do maloobchodu řadí prodej smíšeného zboží, zboží pro dlouhodobou spotřebu, specializovaný prodej, prodej potrav a nápojů, prodej pohonných hmot a MOTO (Český statistický úřad [ČSÚ], 2023).

Maloobchodní obchodní modely

Obchodní model je pojem bez přesné definice, který vzešel z obchodní a ekonomické literatury (Ovans, 2015). Dle Oslo manuálu jej lze chápat také jako set klíčových podnikových procesů (OECD & Eurostat, 2018). Obecně tento termín popisuje strategie a mechanismy, které firmy používají k úspěchu na konkurenčních trzích. Níže jsou uvedené jednotlivé příklady B2C on-line obchodních modelů:

- **E-shop**[5] **- podnikatelský subjekt dodává zboží či služby spotřebiteli prostřednictvím elektronických transakcí prováděných přes internet nebo prostřednictvím jiných počítačových sítí**. Spotřebitelé si mohou prohlédnout zboží prostřednictvím webových stránek. Podmínkou je, že webové stránky musí umožňovat zároveň provedení objednávky a platby (Kunešová, 2017; Tvrdíková, 2008; Schneider, 2017; Qin et. al, 2022; Heinemann, 2023).
- Aukční portál – nabízí výkonné vyhledávací nástroje a integrovaný balíček obsahu a služeb, typicky využívá kombinovaný příjmový model. (Laudon & Traver, 2022)
- Poskytovatel obsahu – informační a zábavní společnosti, které poskytují digitální obsah; obvykle využívá model příjmů z reklamy, předplatného nebo affiliate poplatku za doporučení (Schneider, 2017; Laudon & Traver, 2022).
- Transaction broker – zpracovává online prodejní transakce; obvykle využívá model výnosů z transakčních poplatků (Schneider, 2017; Laudon & Traver, 2022).
- Tvůrce trhu (také známý marketplace) – využívá internetovou technologii k vytváření trhů, které spojují kupující a prodávající; obvykle využívá model výnosů z transakčních poplatků.
- Poskytovatel služeb – nabízí služby online (Schneider, 2017; Olbrich, 2019; Turban et al., 2018; Heinemann, 2023).
- Community provider – poskytuje online komunitu stejně smýšlejících jednotlivců pro vytváření sítí a sdílení informací; příjmy jsou generovány reklamou, poplatky za doporučení a předplatným (Laudon & Traver, 2022).

Výjimkou pak není, že společnost kombinuje více výše uvedených modelů (OECD, 2019). **Pro potřeby této práce lze tedy vyvodit, že pokud je společnost definována jako e-shop, nevylučuje to z výše uvedeného paralelní provozování další formy maloobchodního prodeje on-line ani prodej zboží či služeb off-line.**

[5] V angličtině se lze v odborné literatuře setkat hned s několika alternativními výrazy, a to *e-tailer* (Turban et al., 2017), *virtual store* (Qin et al., 2022), *electronic shopping mall* (Qin et al., 2022) *a dalšími*.

3.1.4 Právní náležitosti e-shopu v České republice

Jak uvádí OECD (2019), v oblasti e-commerce a segmentu B2C je značná pozornost věnována problematice ochrany spotřebitele. OECD dále zmiňuje hlavní oblasti regulace e-commerce v poslední dekádě, a to:

- ochrana spotřebitele (zahrnující i ochranu zranitelných spotřebitelů a přeshraniční obchod),
- daňová legislativa (s ohledem na přeshraniční obchod),
- politika hospodářské soutěže,
- obchodní politika,
- ochrana životního prostředí (OECD, 2019).

Jak report rovněž uvádí, technologické změny a vývoj nových obchodních modelů, které kombinují jak on-line tak off-line prostředí (kapitoly 3.1.2 a 3.1.3), stírají rozdíly mezi oběma prostředími.

Vývojem legislativních požadavků v elektronické komerci se v České republice zabývala mimo jiné Kunešová (2017). Jednotlivé právní předpisy upravující elektronický obchod v České republice jsou uvedeny níže:

- *Zákon č. 89/2012 Sb. občanský zákoník*[6]
    - Z pohledu elektronického obchodování upravuje podmínky pro uzavírání smluv distančním způsobem a závazky ze smluv uzavíraných mimo obchodní prostory
    - Podmínky záruky a odpovědnosti za vady
    - Nekalou soutěž (především pak vymezuje klamavou reklamu) (Veverková, 2021)
- *Zákon č. 634/1992 Sb. o ochraně spotřebitele ve znění pozdějších předpisů*
    - Zavádí informační povinnost prodejce
    - informace o vlastnostech prodávaných výrobku nebo charakteru poskytovaných služeb
    - pravidla označování výrobků

[6] Poslední novela Zákona č. 89/2012 Sb. vešla spolu s novelou Zákona č. 634/1992 v platnost 6. ledna 2023. Z pohledu e-shopu došlo ke změnám v oblasti lhůty pro odstoupení od smlouvy (nově 30 dnů), ochraně před umělým navyšováním ceny, podmínkek reklamace, ochrany před netransparentním nákupem on-line (např. publikací falešných recenzí), zákazu používání předem tzv. zaškrtnutých políček, opatření pro transparentní objednání, kdy si spotřebitel musí být vědom, který krok jej zavazuje k objednání. Dále byla stanovena lhůta 30 dnů pro doručení zboží bez zbytečného odkladu, pokud si spotřebitel s prodávajícím neujednal jinak (Česká obchodní inspekce, 2022; Ministerstvo průmyslu a obchodu [MPO], 2022).

    - informace o ceně
    - informace o reklamaci
    - informace o mimosoudním řešení spotřebitelských sporů (Veverková, 2021)
- *Zákon č. 110/2019 Sb. o ochraně osobních údajů*
    - Upravuje podmínky pro zpracování osobních údajů subjekty ze strany správce (e-shopu)
- *Zákon č. 468/2011 Sb. o elektronické komunikaci*[7] (Veverková, 2021)
- *Zákon č. 480/2011 Sb. o některých službách informační společnosti ve znění pozdějších předpisů* (Veverková, 2021)

Informační povinnost e-shopu

Každý obchodník bez ohledu na povahu prodeje má povinnost informovat spotřebitele v dostatečném předstihu před uzavřením smlouvy nebo před předložením závazné nabídky o následujících skutečnostech (§ 1811 Občanského zákoníku):

- Identifikační údaje, případně telefonní číslo nebo adresu pro doručování elektronické pošty nebo jiný kontakt.
- Název zboží nebo služby spolu s popisem jejich hlavních vlastností.
- Cenu zboží nebo služby a způsob výpočtu včetně všech daní a poplatků.
- Způsob platby a dodání nebo plnění objednaného zboží nebo služby.
- Náklady na dodání, případně informaci, že mohou být dodatečně účtovány.
- Informace o právech v případě vadného plnění a podmínky pro uplatňování záruky a dalších práv.

Specifickou povinnost pro e-shop dále upravuje § 1820 Občanského zákoníku. Veverková (2021) v této souvislosti poukazuje na potřebu vyvážit informační nerovnost mezi podnikatelem a spotřebitelem, kdy uvádí, že: „*Lze totiž předpokládat, že spotřebitel nemůže mít o prodávaném zboží či poskytovaných službách tolik informací, jako kdyby smlouvu uzavíral v kamenné prodejně*.“ (Veverková, 2021, s. 204).

[7] Naposledy byl tento zákon novelizován v roce 2021 (MPO, 2021), kdy došlo k úpravě podmínek pro zpracování cookies ze strany e-shopu.

Mezi e-shopem povinně udávané informace patří:

- Náklady na prostředky komunikace na dálku, pokud se liší od základní sazby.
- Informace o případné povinnosti zaplatit zálohu nebo obdobnou platbu.
- Jestliže se jedná o smlouvu, jejímž předmětem je opakované plnění, nejkratší dobu, po kterou bude smlouva strany zavazovat.
- Podmínky, lhůtu a postupy pro uplatnění práva na odstoupení od smlouvy, a to včetně formuláře pro odstoupení od smlouvy.
- Informace o tom, že v případě odstoupení od smlouvy ponese spotřebitel náklady spojené s navrácením zboží. Pokud půjde o smlouvu uzavřenou prostřednictvím prostředku komunikace na dálku, náklady za navrácení zboží, pokud není možné vrátit zboží obvyklou poštovní cestou z důvodu jeho povahy.
- Údaje o existenci, způsobu a podmínkách mimosoudního vyřizování stížností spotřebitelů, včetně informace o tom, zda se lze obrátit se stížností na orgán dohledu nebo státního dozoru. (Veverková, 2021; Zákon č. 89/2012 Sb., 2012).

V souvislosti s informační povinností e-shopu je spojen dokument obecně označovaný jako „Obchodní podmínky“ (Asociace pro elektronickou komerci [APEK], 2023d). Jako takový pojem „Obchodní podmínky“ není definován žádným zákonem (Veverková, 2021). „Obchodní podmínky“ jsou dále považovány za vhodnou formu splnění obchodních podmínek ze strany e-shopu (Veverková & Horáková, 2022).

3.1.5 Klíčové činnosti e-shopu

Dříve než budou v této kapitole definovány klíčové činnosti e-shopu, je třeba nejprve definovat pojem klíčová činnost:

- „***Klíčové (primární) činnosti zahrnují veškeré postupy, které se podílejí na tvorbě konečného produktu pro zákazníka, a to včetně jeho dodání zákazníkovi***.“ (Pearce & Robinson, 2000; Porter, 1985)

S ohledem na klíčové činnosti podniku lze ovšem dále identifikovat i takzvané „*podpůrné (sekundární) činnosti*“, které jsou chápany jako činnosti v rámci podnikové infrastruktury mající za cíl podporovat standardní provádění činností klíčových (Pearce & Robinson, 2000; Porter, 1985; Eurostat, 2013).

V souvislosti s pojmem „*klíčová činnost*“ lze nalézt významově podobné pojmy, a to pojmy:

- **Podnikový proces** jako „*souhrn činností transformujících (pomocí lidí a nástrojů) souhrn vstupů do souhrnu výstupů (zboží nebo služeb) za předpokladu, že tyto výstupy jsou určeny pro jiné lidi nebo procesy*.“ (Řepa, 2007) Podnikové procesy lze dále dělit na procesy řídicí, klíčové/hlavní a podpůrné, přičemž významově nejbližší pojmu „klíčová činnost“ jsou procesy hlavní (Řepa, 2007). Alternativou pro podpůrné činnosti jsou pak „*procesy podpůrné*“. V rámci této práce se ovšem vzhledem k propojení pojmu „podnikový proces“ a konceptu Business process management (BPM) (van Rosing et al., 2014) sbude pracovat s obecnějším pojmem „klíčové činnosti“ definovaným výše v této podkapitole.
- **Podniková (funkční či funkcionální) oblast** jako specifický segment nebo část podniku (oddělení), která se soustředí na určitý druh činností a kolem níž jsou organizováni pracovníci podniku (Keřkovský & Vykypěl, 2006).

V souvislosti se zaměřením této disertační práce bude v jejím dalším průběhu používán primárně pojem „klíčová činnost“. Využití pojmu „podnikový proces“ se bude vázat na případy významově propojené s problematikou řízení podnikových procesů. Pojem „podniková oblast“ pak bude využíván v případech, kdy tak má být označeno funkční oddělení podniku.[8]

Činnosti e-shopu

Každá firma může být charakterizována souborem aktivit, které přidávají hodnotu a jsou vykonávány různými aktéry ve firmě (Laudon & Traver, 2022). Jak dále tito autoři uvádějí, rozvoj elektronického obchodu měl výrazný vliv na podnikatelské prostředí v poslední dekádě. Dopad na strukturu obchodního odvětví, dodavatelsko-odběratelské řetězce (aktivity mezi jednotlivými články – výrobci, dodavateli, přepravci, distributory, obchodníky), strategií firem, ale také v struktuře a provádění jednotlivých podnikových procesů/činností (Laudon & Traver, 2022).

[8] Například marketing lze v literatuře nalézt ve smyslu klíčové činnosti (viz níže v této kapitole), hlavního či podpůrného podnikového procesu (Bititci, 2015) nebo právě jedna z funkční oblast (Keřkovský & Vykypěl, 2006).

Jak dále uvádí Heinermann (2023), bez optimalizovaných procesů (činností) a odpovídající podpory systému nelze realizovat žádné e-commerce obchodní modely. On-line maloobchodní společnost by se měla organizovat jako "soubor klíčových činností" takovým způsobem, aby bylo možné realizovat činnosti kontinuálně od dodavatele k zákazníkovi a tím umožnit zákaznicky orientované celkové zpracování (Heinemann, 2023). Dle MacGragor & Vrazalic (2007) by dále měla vést aplikace webových informačních technologií k automatizaci klíčových činností.

Následující text tvoří rešerši hodnototvorného řetězce e-shopu (value chain) a konkrétních činností, které jsou soudobou literaturou uváděny jakožto klíčové aktivity řízení elektronických obchodů. V následujícím textu jsou zmíněny klíčové aktivity e-shopu, kdy základní členění pro e-commerce se řídí modelem dle Laudon & Trayer (2022)[9]:

- **Vstupní logistika**

Je dle Jenkins (2020): „Způsob, jakým jsou do společnosti přiváženy materiály a další zboží.“ Tato činnost zahrnuje kroky objednávání, přijímání, skladování, dopravy a správy příchozích dodávek. Vstupní logistika se zaměřuje na dodávkovou část rovnice dodávky a poptávky.

V literatuře týkající se e-commerce je tato činnost například uváděna Laudonem & Trayerem (2022) nebo Turbanen et al. (2018), kdy jsou konkrétně uváděny aktivity zahrnující naskladňování zboží (OECD, 2019; Schneider, 2017) či řízení skladových zásob (Kunešová, 2017; OECD, 2019; Shui et al., 2023).

- **Provoz (Operations)**

Provoz zahrnuje postupy pro přeměnu surovin na hotový výrobek nebo službu. To zahrnuje transformaci všech vstupů na výstupy (Tarver, 2021). V kontextu elektronického obchodu sem lze zahrnout aktivity jako řízení produktu (Hall, 2021, Qin et al., 2021, Shui et al., 2023) či řízení webové stránky (Hall, 2021; Laudon & Traver, 2022) a zabezpečení (Schneider, 2017; Turban et al., 2018). Do této skupiny lze dále zařadit také „*Vyřizování zákaznických objednávek*“ (Heinemann, 2023; Shui et al., 2023). Dílčí aktivity se ovšem v tomto mohou prolínat s aktivitami v rámci odchozí a příchozí logistiky.

[9] Tento model pak vychází z původní modelu dle Portera (1985).

- **Odchozí logistika**

Dle Jenkins (2020) se odchozí logistika: „*Zaměřuje na poptávkovou stranu rovnice nabídky a poptávky. Činnost zahrnuje skladování a přesun zboží zákazníkovi nebo koncovému uživateli. Kroky zahrnují vyplnění objednávky, balení, přepravu, doručení a zákaznickou službu související s doručením*.“

V kontextu e-shopu odchozí logistika zahrnuje aktivity vyskladnění a expedici zboží zákazníkovi, které si od e-shopu objednal (OECD, 2019; Hall, 2021; Heinemann, 2023; Shui et al., 2023; Schneider, 2017). Jedním z uváděných modelů odchozí logistiky je pak takzvaný *dropshipping*[10] (Turban et al., 2018).

- **Marketing & prodej**

Marketing je definován jako proces úmyslného stimulování poptávky po zboží a službách s cílem uskutečňování jejich nákupu (Kotler & Armstrong, 2020; Helmond, 2022). Prodej, jakožto proces je pak definován jako plánování, řízení a kontrola osobního prodeje produktu. Prodej dále přispívá k dosažení marketingových cílů firmy (Kotler & Armstrong, 2020).

U e-shopu je nejčastěji coby konkrétní aktivita zmiňován digitální marketing, který zahrnuje veškeré marketingové úsilí, které využívá elektronická zařízení nebo internet. Z pohledu e-shopu se jedná o digitální kanály, jako jsou vyhledávače, sociální média, e-mail a webové stránky (Hall, 2021; Kunešová, 2017).

Dále jsou v této souvislosti s e-shopy zmiňovány aktivity jako propagace (Heinemann, 2023, Turban et al., 2018), marketingový výzkum (Turban et al., 2018), marketingová strategie (Heinemann, 2023), e-mail marketing (Olbrich et al., 2019), affiliate marketing (Olbrich et al., 2019), marketing ve vyhledávačích (Olbrich et al., 2019) a také tvorba obsahu (Turban et al., 2018)

- **Péče o zákazníka**

V souvislosti s e-commerce Tarver (2021) uvádí, že do této oblasti činnosti na udržování výrobků a zlepšování zážitku zákazníků - zákaznický servis, údržba, opravy, vrácení a výměna zboží. Tuto činnost dále v prostředí elektronického obchodů uvádějí také Heinemann (2023) nebo Kunešová (2017).

[10] Dropshipping je obchodní model, kdy elektronický prodejce prodává produkt a poté jej nakupuje od dodavatele, který produkt zabalí a odešle kupujícímu (Turban et al., 2018).

Vedle primárních činností lze identifikovat i **činnosti sekundární**, takzvaně „podpůrné“.[11] Za sekundární (podpůrné) činnosti u e-shopu pak Laudon & Traver (2022) považují správu a řízení, řízení lidských zdrojů, informačních systémů, nákup, finance a účetnictví:

- Správa a řízení

V literatuře o e-commerce se těmito činnostmi zabývá například Hall (2011).

- Řízení lidských zdrojů

Dle některých autorů se jedná o proces získávání, školení, hodnocení a odměňování zaměstnanců a péče o jejich pracovněprávní vztahy, zdraví a bezpečnost a zmírňování obav o spravedlnost (Dessler, 2020).

Pro potřeby e-shopu tento proces zahrnuje specificky aktivity jako automatizované služby pro zaměstnance, vzdělávání (e-learning), získávání nových dovedností (e-training) či nábor pracovníků (Kunešová, 2017; Turban et al., 2018).

- Informační systémy (řízení informací, dat a znalostí)

Zde je v současném kontextu zmiňováno využívání pokročilých informačních technologií (Gao et al., 2022; Schneider, 2017) – například umělá inteligence a její jednotlivé nástroje (OECD, 2019), a to za účelem modelování, data miningu či získávání a diseminace znalostí v organizaci (Gao et al., 2022, Kunešová, 2017, Schneider, 2017). Cílem tohoto procesu by mělo být dále dle OECD (2019) také zlepšování klíčových aktivit podniku.

- Nákup

V kontextu řízení podniku znamená "procurement" (někdy nazývaný také nákup nebo obstarávání) proces získávání zboží, služeb nebo pracovní síly od externích dodavatelů nebo dodavatelů uvnitř organizace za účelem naplnění cílů organizace (Baily et al., 2022). V literatuře o elektronickém obchodování se touto činností zabývají například Kunešová (2017) nebo Shui et al. (2022).

- Finance a účetnictví, controlling

V literatuře o e-commerce uvádí dále například Kunešová (2017), Miles (2021) nebo Turban et al. (2018).

[11] Ačkoliv se jedná o významově související pojem pojmu „podpůrný proces“, autor tento termín explicitně nepoužívá (Laudon & Trayer, 2022).

Nad rámec použitého konceptuálního modelu lze v soudobé literatuře týkající se e-commerce a e-shopů nalézt v různé struktuře řadu dalších různě popsaných činností. V této práci jsou uvedeny pouze výčtem:

- Výzkum a vývoj (2017)
- Právní záležitosti (Miles, 2021; Turban et al., 2018) – zahrnující činnosti jako daně, privacy, regulace. Obecně se jedná o zajišťování shody s platnými právními požadavky.
- Strategické řízení (Sinning, 2021)
- Řízení rizik (Zhang et al., 2023)

3.1.6 Upřesnění výběru zkoumané skupiny

Na základě výše uvedených charakteristik a definicí bude v této části upřesněna skupina podniků, jež je předmětem zkoumání této disertační práce.

Pro potřeby této práce se za e-shop (nebo také elektronický obchod) v souladu s předchozí klasifikací bude považovat maloobchodní podnikatelský subjekt, který **dodává zboží či služby spotřebiteli prostřednictvím elektronických transakcí prováděných přes internet nebo prostřednictvím jiných počítačových sítí** (Kunešová, 2017; Tvrdíková, 2008) za splnění podmínky, že spotřebitel si může produkt prostřednictvím webových stránek nejprve prohlédnout a následně také objednat a zaplatit (Heinemann, 2023; Schneider, 2017; Qin et. al, 2022; Heinemann, 2023).

3.1.6.1 Pojem malý e-shop

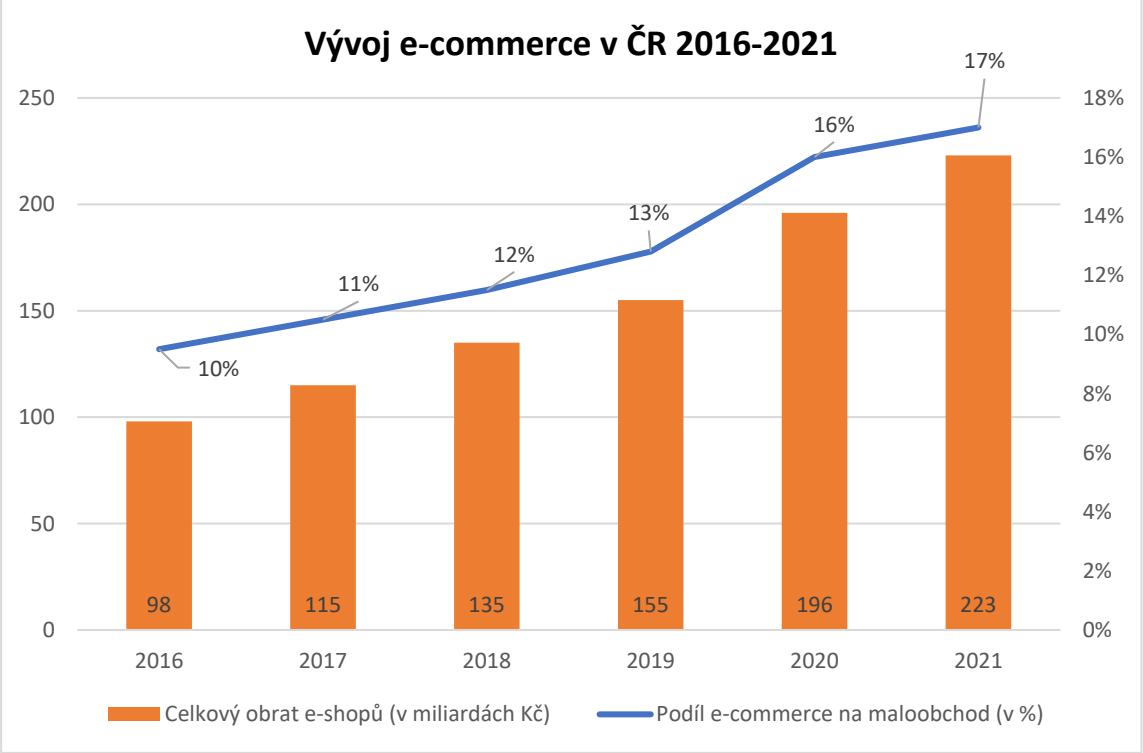
Za malý e-shop se v této práci považuje takový subjekt, který současně svými charakteristikami odpovídá výše uvedené **definici e-shopu** (3.1.6) a také **definici malého podniku dle Evropské komise** (2019a).[12] Skupina malých e-shopů byla vybraná vzhledem ke své předpokládané relativní homogenitě, ale i úzké vazbě na problematiku ochrany osobních údajů a GDPR. K přijetí nového právního rámce totiž došlo v souvislosti s rozvojem internetu a elektronické výměny dat v předchozích 20 letech (European Data Protection Supervisor, n.d.b). Subjekt podnikající v segmentu B2C zpracovává osobní údaje spotřebitelů. V případě podnikání na území EU či zpracování

[12] Za malý se dle uvedeného doporučení považuje podnik, který: „který zaměstnává méně než 50 osob a jehož roční obrat a/nebo roční bilanční suma nepřesahuje 10 milionů Euro.“ (Evropská komise, 2019a). Implicitně se rovněž jedná o podnik, který alespoň v jedné charakteristice neodpovídá mikropodniku téhož doporučení. Tedy, že roční obrat či bilanční suma je vyšší než 2 miliony Euro nebo že podnik zaměstnává více 10 osob. Podmínkou definice MSP je rovněž jeho vlastnická struktura a přístup ke zdrojům (Evropská komise, 2019a).

osobních údajů občanů EU se na takovýto subjekt vztahuje i podmínka implementace GDPR. Skupina e-shopů byla vybrána i vzhledem ke kontinuálnímu růstu počtu lidí využívajících internet pro nákup zboží a služeb (EC, 2019b; ČSÚ, 2019; ÚOOÚ, 2019).

Rozvoj internetového obchodování mimo jiné potvrzují i informace APEK, které ukazují, že v České republice dochází ke kontinuálnímu růstu segmentu e-shopů jak z hlediska obratu, tak i podílu v maloobchodu v České republice[13]. Na základě dat z roku 2021 zaznamenaly české e-shopy v tomto roce obrat v odhadované výši **223 miliard Kč** s podílem **17 % v maloobchodu**. Vývoj českých e-shopů v letech 2016 až 2021 je znázorněn na následujícím obrázku 3-1. Odhady o počtu e-shopů z roku 2023 se pohybují v rozmezí mezi 51000 až 57000[14] e-shopy (APEK, 2023a; CzechCrunch s.r.o., 2023). Jak velkou část z nich tvoří e-shopy odpovídají charakteristikám malého podnikání není jednoznačně známo (APEK, 2023a).

Obrázek 3-1: E-commerce v ČR - vývoj v letech 2016 až 2021



Zdroj: APEK (2023a), zpracováno autorem

[13] Výjimkou je rok 2022, kdy dle průzkumu APEK a Heuréka.cz došlo k poklesu o 12 % (APEK, 2023b)
[14] Odhady zaokrouhleny na celé tisíce e-shopů.

3.1.6.2 Geografická působnost e-shopu

Výzkum je dále omezen geograficky, podmínkou je zahrnutí malých e-shopů podnikajících na území **České republiky**. Takovým e-shopem může být pro potřeby této disertační práce považován kterýkoliv ze čtyř výše uvedených kategorií e-shopů v kapitole 3.1.2. (lokální, domácí, přeshraniční, globální).

U zkoumané skupiny podniků bude dále zohledněno možné působení právního subjektu i mimo oblast České republiky, neboť to může mít vliv na podobu dopadů a implementace GDPR v daném podnikatelském subjektu, a to s ohledem na možnou rozdílnost v implementaci v ostatních státech EU.

Tato rozdílnost je dána tím, že nařízení je legislativně adaptováno v jednotlivých členských státech na základě zvláštního zákona, který umožňuje zavedení dílčích výjimek v dané zemi EU. Výklad normy, stejně jako její vymáhání, je ponecháno národním autoritám pro ochranu osobních údajů dané země. Individuální posuzování pak může mít důsledky pro rozsah a náročnost implementačních projektů (EP & EUC, 2017; Custers et al., 2018).

3.1.6.3 Omezení dle role e-commerce

Dle předchozích charakteristik platí, že v případě elektronického obchodu je běžná kombinace vícero obchodních a příjmových modelů (Schneider, 2017; Turban et al., 2017; OECD, 2019). Ty se dále neustále vyvíjejí (OECD, 2019). Kromě provozování on-line prodeje prostřednictvím e-shopu spotřebiteli, může být rovněž:

- provozován obchod v jiném než on-line prostředí (Cooperating On-line Trade, Multi-channel commerce, Hybrid on-line trading),
- může být vedle činnosti obchodní vykonávána rovněž činnost výrobní (např. Vertical on-line trade),
- na obchodu mohou být zúčastněny i jiné subjekty (například B2B, B2G či B2E),
- romě e-shopu může být provozován i jiný obchodní model (například webová stránka kromě e-shopu slouží rozvněž jako on-line tržiště – marketplace).

S ohledem na téma této disertační práce budou uvažovány **všechny podnikatelské subjekty provozující B2C on-line obchod ve formě e-shopu**, a to z důvodu, že pro tyto subjekty jsou platné stejné právní náležitosti týkající se ochrany spotřebitele, daňové

legislativy, politiky hospodářské soutěže, obchodní politiky, legislativy v oblasti životního prostředí, stejně jako oblasti ochrany soukromí.

V tomto ohledu se i implemenace GDPR v daných podnicích řídí shodnými právními podmínkami. **Paralelní provozování kterékoliv jiné obchodní činnosti (jiný druh on-line obchodu, jiný než B2C obchod) nebo činnosti výrobní není pro zařazení zkoumaných subjektů vylučující podmínkou.**

3.2 Současný management rizik

Pro snazší práci s konceptem řízení rizik je třeba nejprve definovat pojem rizika jako pojmu využívaného v oblasti podnikové ekonomiky a managementu. Z existujících definic jsou níže uvedeny dvě:

„*Za riziko se považuje nebezpečí vzniku škody, poškození, ztráty či zničení, případně nezdaru při podnikání.*“ (Smejkal & Rais 2013, s. 78)

„Riziko je jev, který může způsobit odchylku od očekávaného výsledku, a jako takový může ovlivnit dosažení obchodních cílů a výkon celkové organizace.“ (Lam, 2017, s. 4)

Z těchto definic lze odvodit, že za riziko lze uvažovat jakýkoliv jev, který má pro organizaci negativní či dopředu neočekáváné nebo nežádoucí důsledky (Hubbard, 2020). Neočekávaný jev může mít ovšem na druhé straně na organizaci i dopad pozitivní (Lam, 2017), v tomto případě bývá označováno jako riziko pozitivní či jako příležitost (Merna & Al-Thani, 2007; Benjamin, 2017).

Jako disciplína zabývající se systematickým řízením rizik se management rizik etabloval po druhé světové válce (Smejkal & Rais 2013).[15] Z počátku byl management rizik spojen s pojišťovnictvím a zmírňováním negativních finančních důsledků (Harrington & Niehaus, 2004). Tento přístup zahrnoval nekoordinované činnosti směřují ke zmírnění finančních rizik, a to pojišťovacích a derivátových nástrojů na ochranu společnosti před finanční ztrátou (Mishkin & Eakins 2018). Nicméně postupně začal být princip řízení rizik využíván ve společnostech globálně, na začátku 90. let minulého století došlo ke konvergenci do té doby izolovaných přístupů k řízení rizik finančních a rizik operativního charakteru[16] (Dionne, 2013). Ferreira de Araújo et al. (2020) v této souvislosti zmiňují především metodiky týkající se zdravotních, bezpečnostních

[15] Za vznik tohoto oboru se považuje období let 1955-1964 (Dionne, 2013).
[16] Lam (2017) dále uvádí, že finanční a operativní rizika jsou mezi sebou provázána.

či s informačními technologiemi souvisejících rizik (Lam, 2017). Bez ohledu na povahu rizika totiž management rizik uvažuje vždy dvě zásadní proměnné, a to velikost dopadu v případě výskytu a nejistotu (pravděpodobnost), že k tomuto výskytu dojde (Girling, 2013; Crovini, 2019; Green; 2016). Takto integrovaný přístup k řízení podnikových rizik je v anglické literatuře označován jako Enterprise Risk Management (Hunziker, 2019). Kromě již výše uvedených finančních a operativních rizik zahrnuje také řízení strategických rizik (Bérard & Teyssier, 2017; Lam, 2017) a rizik vyplývajících z plnění regulatorních opatření a reputačních/zákaznických rizik (Elmaallam & Kriouile, 2011; Hunziker, 2019; Lam, 2017; Girling, 2013).

Jak bylo uvedeno výše, význam pojmu riziko i oblastí, jež management rizik zahrnuje, se s postupem času neustále vyvíjí (Hubbard, 2020; Crovini, 2019), i proto se neustálé vyvíjí také poslání samotného managementu rizik. Pro vymezení cíle managementu rizik budou opět použity dvě definice:

„*Cílem (managementu rizik) je pomoci organizaci proaktivně a efektivně pracovat s neustálé se měnícími rizikovými faktory*." (Farrel & Gallagher, 2019, s. 627)

„*Management rizik je o efektivním řízení v rizikovém a nejistém světě (prostředí)*." (Anderson, 2013, s. 2)

Pro porovnání s předchozím pojetím tedy není cílem řízení rizik pouhé ošetření rizik (Gibson & Igonor, 2020; Lam, 2017; Hubbard, 2020). Proaktivní řízení rizik nejen usnadňuje dosažení cílů společnosti, ale také jí umožňuje lépe reagovat a adaptovat se na překvapení a narušení, která lze přičíst vnějšímu i vnitřnímu prostředí (Bérard & Teyssier, 2017). Obecně současné paradigma vnímá management rizik jako proces, který:

- Je integrovaný se všemi aspekty a funkcemi organizace (Green, 2016; Khan et al., 2016; Lam, 2017; Lark, 2015).
- Je uvažován ve strategickém kontextu organizace (Elmaallam & Kriouile, 2011; Lam, 2017; Da Costa Lewis, 2012; Wieczorek-Kosmala, 2014).
- Vede ve svých důsledcích k dosažení lepších výsledků, přičemž výsledky jsou vnímány z perspektivy výkonnosti organizace (Benjamin, 2017) a minimalizace odchylek od očekávaného stavu efektivním ošetřením rizik (Lam, 2017).
- Vede k zajištění rovnováhy mezi náklady vyplývajícími z rizik a přínosů (Lam, 2017; Mohammed & Knápková, 2016).

Ze své podstaty tak klíčovou roli v tomto procesu sehrává pochopení příčin a následků (Anderson, 2013). I proto je zdůrazňována role dostatečných informací a znalostí (Ferreira de Araújo et al., 2020; Lark, 2015; Durst et al. 2019). Významnost managementu rizik je dále zmiňována i v rámci standardů týkajících se kvality procesů, například ISO 9000 nebo modelů CMM a CMMI (Durst et al. 2019).

3.2.1 Proces řízení rizik

Proces řízení rizik je založen na plánování a preventivních úkonech[17] před nastáním rizikové události (Anderson, 2013). Smyslem tohoto konání je schopnost přijímat plně informovaná rozhodnutí při zvažování všech různých typů omezení v rámci své společnosti a při zachování vnitřní rovnováhy organizace (Bérard & Teyssier, 2017). Pro dosažení této rovnováhy lze dále uvažovat princip rozhodování na základě takzvané cost-benefit analýzy, kdy při každém rozhodnutí o opatření je uvažována jak rovina přínosů, tak rovina nákladů s tím spojených (Gibson & Igonor, 2020). I z této podstaty vyplývá, že se jedná o proces kontinuální s opakujícími se fázemi.

Definované dílčí kroky managementu rizik pak plně vycházejí z doposud publikovaných mezinárodně platných referenčních rámců, které se managementem primárně zabývají. V tomto případě je výchozími standardy pro management rizik v organizaci skupina standardů ISO 31000 (Bérard & Teyssier, 2017; Hardy, 2014). ISO 31000 je skupina norem vztahujících se k řízení rizik kodifikovaná Mezinárodní organizací pro normalizaci (Barafort et al., 2017). ISO 31000 poskytuje zásady a obecné pokyny pro řízení rizik, kterým čelí organizace (Ferreira de Araújo et al., 2020). Standard také harmonizuje procesy a definice řízení rizik ve stávajících a budoucích standardech. Standard lze použít na širokou škálu činností, rozhodnutí a operací jakéhokoli veřejného, soukromého nebo komunitního podniku, sdružení, skupiny nebo jednotlivce (Kouns & Minoli, 2010; Oliva, 2016). Tento standard uvažuje těchto pět základních fází managementu rizik:

- Vytvoření organizačního kontextu
- Identifikace rizik
- Analýza rizik
- Evaluace rizik
- Opatření vůči rizikům (Hassel & Cedergren, 2021; ISO, 2018b)

[17] Reaktivními úkony v případě nastání rizik se zabývá krizový management, který je některými autory rovněž považován za integrální součást managementu rizik (Aba-bulgu & Islam, 2006).

Alternativně se metodiky zmiňují i o třífázových (Bissonette, 2016) nebo čtyřfázových postupech (Da Costa Lewis, 2012; Ackermann, 2013; Gibson & Igonor, 2020). Oproti standardům ISO dále obsahují například fázi monitoringu a průběžné aktualizace plánu rizik (Merna & Al-thani, 2007, Benjamin, 2017; Lam, 2017; Lark, 2015).

Bez ohledu na možné odchylky proces strategického řízení rizik předpokládá zapojení velkého množství aktérů tak (Bérard & Teyssier, 2017), aby došlo ke zvýšení účinnosti využívaných kvalitativních či kvantitativních nástrojů, jež jsou součástí managementu rizik (Benjamin, 2017). Výsledkem procesu řízení rizik jsou pak opatření vůči možným rizikům. V tomto ohledu jsou známy čtyři základní strategie ošetření, a to vyhnutí se riziku, přenos rizika, zmírnění dopadu rizik nebo jejich akceptace. Dále je také uváděna strategie sdílení rizika (Gibson & Igonor, 2020).

3.2.2 Řízení rizik v kontextu regulatorních opatření

Postupné přijímání nových regulatorních opatření pro jednotlivá odvětví či aktivity organizací je spojeno s počátkem 90. let minulého století, a to dle některých autorů v důsledku potřeby zvyšovat kvalitu (Harkins, 2016). Přijímání legislativních opatření probíhá v souvislosti se zdůrazněním významu užívání technik řízení rizik v důsledku předchozího rizikového chování subjektu v jednotlivých odvětvích (Lam, 2017) či potenciálnímu vystavení riziku.

V souvislosti se zaváděním těchto opatření došlo k úpravě přístupu k managementu rizik v organizacích. Z pohledu organizace lze důsledky pro management rizik chápat v několika rovinách, které jsou významově provázány a které jsou uvedeny níže:

- **Regulatorní opatření jako zdroj rizik**

Adaptace na platné regulace je běžnou součástí managementu organizací. Případné neplnění regulatorních požadavků má pro organizace potenciálně celou řadu negativních důsledků v podobě snížení kvality, zvýšení nákladů, ztráty výnosů, udělení pokut a dalších sankcí (Green, 2016; Hunziker, 2019). V širší rovině pak lze definovat i negativní vliv na reputaci organizace, a to jak ve vztahu k potenciálním partnerům, tak zákazníkům (Green, 2016). V důsledcích se tedy tato skupina rizik může významově prolínat s riziky reputačního charakteru.

Kategorie rizik s výše uvedenými projevy a příčinami doposud nemá v anglické literatuře ustálenou jednotnou terminologii, kdy lze nalézt pojmy jako legal risks

(Elmaallam & Kriouile, 2011), compliance risks (Gibson & Igonor, 2020; Girling, 2013; Hunziker, 2019), regulatory risk (Girling, 2013; Green, 2016), případně libovolně uvedená kombinace výše uvedených pojmů (Girling, 2013). Nicméně i tak je již tento typ rizika ustálen mezi ostatními podnikovými riziky (Girling, 2013; Elmaallam & Kriouile, 2011; Hunziker, 2019).

Pro potřeby tohoto textu bude dále používán pojem regulatorní rizika, který lze definovat takto: „*Regulatorní rizika zahrnují neočekávané změny, které vyplývají například z právních sankcí a poškození dobré pověsti nebo z porušení zákonných požadavků.*“ (Hunziker, 2019, s. 217)
Dle jiného způsobu kategorizace Anderson (2013) tato rizika řadí do skupin externích rizik. Samotné regulace spadající do této kategorie mohou vycházet jak z platné legislativy, tak odvětvových standardů.

- **Změna přístupu k řízení rizik**

Výše uvedený náhled na regulatorní opatření jako na zvláštní kategorii rizik má svůj analogický dopad i na praktiky současného managementu rizik v organizaci (Lam, 2017). V důsledku přijímání nových opatření musely metodiky managementu rizik zahrnout i aktivity směřující k monitoringu aktuálních požadavků a jejich implementaci do podnikového prostředí, jakožto opatření vůči výše definovanému typu rizik.

Vzhledem k záměru jednotlivých regulací, jež se týkaly pouze vybraných podnikových oblastí (finance a daňové povinnosti, lidské zdroje, ochrana spotřebitele, ochrana soukromí, životního prostředí, kyberbezpečnost a podobně), došlo k propojení managementu rizik s těmito oblastmi (Lam, 2017). Proto moderní management rizik předpokládá plnou integraci managementu rizik v podnikových strukturách, jeho propojení se všemi funkcemi a strategickým kontextem tak, aby bylo zajištěno, že procesy řízení tohoto typu rizik a dodržování platných předpisů v rámci jednotlivých procesů jsou vzájemně propojeny (Girling, 2013; Lam, 2017). Dle studie Deloitte z roku 2013 81 % výkonných pracovníků pohlíží na řízení rizik spíše ze strategické perspektivy, nežli jako na disciplínu zabývající se riziky v jednotlivých oblastech činností podniku odděleně (Deloitte Touche Tohmatsu Limited, 2013). Další autoři poukazují na fakt, že nově vzniknuvší metodiky týkající se managementu rizik musí již ve svém designu uvažovat potřebu shody s regulatorními opatřeními (Harkins, 2016). Konkrétním

projevem takovéto reflexe může být například transparentní přístup k ošetření rizik vzhledem k tomu, že to regulace takto vyžadují.

Přehled platných regulatorních opatření, jež mají své důsledky pro management rizik uvádí též Lam (2017), Hubbard (2020) či Girling (2013).

- **Adopce metod managementu rizik v souvislosti s implementací regulatorních opatření**

Třetí perspektivou náhledu na dopady regulatorních opatření na management rizik je z hlediska toho, jak ovlivňují četnost adopce praktik managementu rizik do podnikové praxe. Přijímání regulatorních požadavků je považováno za jeden z pěti faktorů, jež podporují adopci rizikových přístupů v organizacích.[18] (Lam, 2017).

Níže jsou na základě dostupné literatury uvedeny důvody, proč ke zvýšené adopci v důsledku platných regulatorních opatření dochází:

- Management rizik poskytuje holistický přístup, jež může adaptaci na jednotlivé regulace zastřešovat (Harkins, 2016; Lam, 2017).
- Regulatorní opatření prvky managementu rizik nepřímo implikují (Girling, 2013; Harkins, 2016).
- Podmínkou plnění regulatorních opatření je i adopce prvků managementu rizik (Gibson & Igonor, 2020; Hubbard, 2020).

Aplikace platných standardů jsou postaveny na metodice pro řízení rizik (Kouns & Minoli, 2010). V souvislosti se vzrůstající adopcí managementu rizik v organizacích ovšem Fraser & Simkin (2010) či Chapman (2019) poukazují na fakt, že rovněž záleží na přístupu k samotné adopci. Řízení rizik je stále vnímáno hlavně jako regulační požadavek bez významné přidané hodnoty (Hunziker, 2019). Dle některých autorů (Fraser & Simkin; 2010; Lam, 2017) tento přístup ovšem výrazně snižuje přínosy z adopce systému řízení rizik. Adopci RM v podniku dále ovlivňuje průmyslový sektor, v němž organizace podniká, velikost organizace či zkušenosti majitelů (Henschel, 2010; Bérard & Teyssier, 2017).

[18] Dalšími faktory jsou finanční a jiné podnikové pohromy v organizacích, iniciativy podporující adopci managementu rizik v průmyslových odvětvích, ratingové agentury a investoři a korporátní programy (Lam, 2017).

3.2.3 Implementace procesu řízení rizik v organizaci

V kontextu současného pojetí výkonnosti podniku vědecké poznatky poukazují na synergický vztah mezi managementem rizik a výkonností hned v několika různých aspektech. Baxter et al. (2013), Farrell & Gallagher (2015) nebo Hoyt & Liebenberg (2011) poukazují na zvýšení tržní hodnoty firem, jež implementovaly systém řízení rizik. Rostami et al. (2015), Brustbauer (2016) nebo Durst et al. (2019) demonstrují souvislost mezi pokročilými praktikami managementu rizik a výkonností či podnikatelským úspěchem, a to v možné souvislosti s lepším rozhodovacím procesem (Hoyt & Liebenberg; 2011, Oliva, 2016).

Andersen (2008) nebo Farrel & Gallagher (2019) poukazují na snížení nákladů na kapitál nebo zefektivnění pro firmu specifických investic. Farrel & Gallagher (2019) poukazují také na výraznější pozitivní efekty v případě velkých a komplexních prostředí, a to i proto, že implementace ERM umožňuje získání komplexního pohledu na všechna rizika, příležitosti i jejich vzájemné souvislosti.

O efektivitě managementu rizik rozhoduje také přístup k implementaci a všem souvisejícím oblastem (Chapman, 2019; Bérard & Teyssier, 2017). Již v předchozí části bylo uvedeno, že adopce managementu rizik je stále vnímána primárně jako regulatorní požadavek, nikoliv příležitost (Hunziker, 2019).

Implementace účinného programu ERM není jednorázovou událostí. Adopce vyžaduje nepřetržitý proces zdokonalování, který je spojen s výraznou investicí jak z hlediska času, tak i nutných zdrojů finančních a lidských (Hardy, 2014; Lam, 2017). Níže je bodově uveden na základě použitých zdrojů seznam předpokladů úspěšné implementace managementu rizik v organizaci:

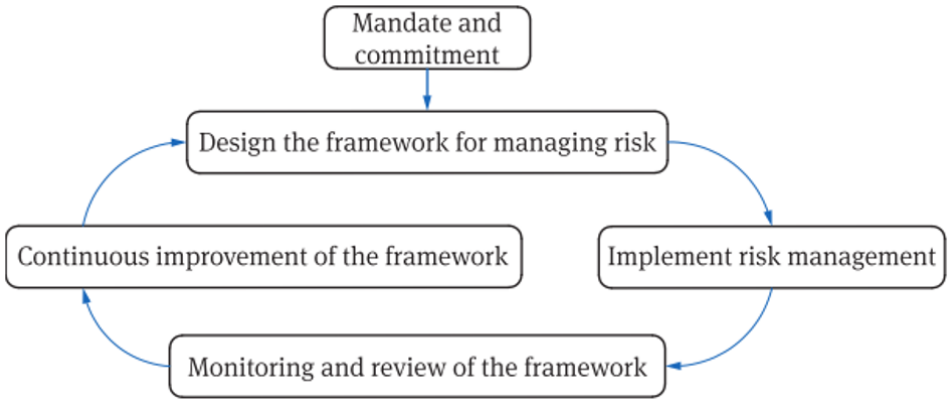
- Pochopení kontextu organizace (Lark, 2015)
- Jednoznačná zodpovědnost za RM v organizaci (Lark, 2015; Lam, 2017)
- Jendoznačná zodpovědnost za zavedení systému v organizaci (Da Costa Lewis, 2012; Lark, 2015)
- Aktivní podpora vrcholového vedení organizace (Lam, 2017; Hardy, 2014)
- Zasazení risk managementu v hodnotovém prostředí organizace (kapitola 3.2)
- Implementaci pozitivně nastavené á kultura (Lam, 2017; Lark, 2015; Hardy, 2014)
- Zapojení všech zainteresovaných stran do procesu (Lam; 2017)

- Formalizace implementace – směrnice, procesní návody apod. (Da Costa Lewis, 2012; Lam, 2017)
- Rovnováha v rámci nastavení systému z hlediska vnímání dílčích rizik (Lam, 2017)

Existuje celá řada bariér, jež jsou s implementací RM rovněž spojeny. Lam (2017) kategorizuje bariéry na bariéry organizačního charakteru, psychologické bariéry či analytické a datové bariéry. Dle (Rostami et al., 2015, O´Hara et al., 2005; Bérard & Teyssier, 2017) prozatím neexistuje dostatečná formální podpora ve formě podkladů, standardů a příruček, jež by poskytly dostatečný zdroj pro správnou implementaci.

Dle ISO 31000:2009 sestává implementace systému rizik z pěti základních kroků, jež jsou zobrazeny na obrázku 3-2:

Obrázek 3-2: Implementace managementu rizik dle ISO 31000



Zdroj: Lark, J. (2015).

3.2.4 Hodnocení a zlepšování procesu řízení rizik

V oblasti řízení organizací se za vyspělost považuje docílení takového stavu, kdy za současných okolností už není možné docílit dalšího zlepšení. Jedná se tedy o cestu směrem z nižšího stupně schopností a kompetencí do stupně vyššího[19] (Antonucci, 2016).

Posuny mezi jednotlivými úrovněmi jsou popsány takzvanými modely vyspělosti. Současné modely vyspělosti vychází z modelu CMM vyvinutého v 80. letech minulého století (Crawford, 2014; Helgesson et al. 2012; Wieczorek-Kosmala, 2014). Modely

[19] Schopnostmi jsou označovány specifické dovednosti, kompetence nebo další charakteristiky organizace, které jí umožňují kolektivně plnit cíle organizace tváří v tvář hrozbám a využívat příležitostí. Schopnosti mohou zahrnovat nevyužité a nerozvinuté nebo stále se rozvíjející dovednosti, které umožňují posouzení, jak úplné jsou v jakémkoliv okamžiku, nebo jaké mohou být v cílovém časovém období (Antonucci, 2016).

pracují se současným stavem, tedy v jaké fázi zralosti se společnosti nachází nyní, a stavem budoucím, tedy jakým směrem se organizace vyvíjí. Jedná se o jeden z nástrojů strategického řízení podniku. Pro potřeby managementu organizací byly postupně vyvinuty modely i pro jednotlivé organizační složky, mimo jiné i pro systém řízení rizik nebo například projektový management (Kerzner, 2001; Rohrbeck, 2011).

Model vyspělosti systému řízení rizik[20] byl konceptualizován za účelem zhodnocení úrovně řízení rizik v daném podniku, strategického rozvoje a zlepšování tohoto procesu v organizaci (Wieczorek-Kosmala, 2014; Čech et al., 2018; Lark, 2015) či ověření aktuálního stavu implementace procesu v podniku (Hardy, 2014). Dle některých autorů neexistuje univerzálně platný model, vždy je třeba využít takový model, který nejlépe reprezentuje potřeby podniku, jeho poslání, kontextu a profilu podnikových rizik. V případě potřeby je možné vyjít z existujících modelů a adaptovat je na podmínky konkrétní organizace nebo oboru. Z této podstaty by měl být model vždy využíván účelně, nikoliv však univerzálně (Tahri & Drissi-Kaitounni, 2015). Dle Antonucci (2016) bylo navrženo více než 77 různých modelů vyspělosti určených pro management rizik. Ty lze dále dělit dle možností jejich využití na:

- Modely určené pouze pro management rizik (Čech et al., 2018; Čech & Januška, 2020).
- Modely určené pro dílčí podprocesy managementu rizik (Faifr, 2020; Chapman, 2019).
- Modely platné pro více procesů (například CMMI, OPM3 a další).

Zralý ERM je definován strategickou integrací agendy ERM s širší podnikovou strategií, závazkem vedení organizace k ERM, jednoznačným vykazováním podnikových rizik, portfoliovým přístupem k řízení rizik a efektivním sdílením rizika mezi zúčastněnými stranami (Farrel & Gallagher, 2019).

3.2.5 Řízení rizik v prostředí malého a středního podniku

Malé a střední podniky tvoří klíčovou část evropského hospodářství. V těchto subjektech je zaměstnáno 67,4 % všech zaměstnanců v Evropské Unii, kteří tvoří 58,1 % HDP EU (Ecorys, 2012). Ve srovnání s velkými firmami mají malé a střední podniky specifické rysy, které je odlišují od ostatních firem (Dickinson, 2011).

[20] Risk Maturity Model, zkratka RMM

Malé a střední podniky se vyznačují především těmito charakteristikami:

- má relativně malý podíl na konkrétním trhu, na kterém působí (Ekwere, 2016; Henschel & Durst, 2016),
- je řízen vlastníky (jednotlivci, skupinami nebo rodinou) a organizační struktura je méně formalizovaná (Ekwere, 2016; Dickinson, 2011; Crovini, 2019),
- maji omezené finanční zdroje a omezený přístup na kapitálové trhy (akciové trhy) (Henschel & Durst, 2016; Ferreira de Araújo et al., 2020),
- mají omezené zdroje a znalosti v oblasti IT (Harris and Patten, 2014; Ambroise & Prim-Allaz, 2017; Crovini, 2019),
- existuje informační neprůhlednost (Ekwere, 2016; Henschel & Durst, 2016),
- investiční a finanční rozhodnutí spolu úzce souvisí (Henschel & Durst, 2016),
- vedení účetnictví a přípravu účetní závěrky provádí daňový poradce, zejména v malých a mikro firmách. (Henschel & Durst, 2016; Crovini, 2019).

Vzhledem k těmto charakteristikám a pozici na trhu čelí MSP celé řadě specifických rizik (Julien et al., 1997; Bérard & Teysier, 2017). Kromě již implicitně zmíněných rizik v oblasti financí a IT (Crovini, 2019; ICAEW, 2005) jsou dále zmiňována rizika související s budováním vlastní důvěryhodnosti (ICAEW, 2005), rizika spojená s růstem, rizika spojená s řízením a zaměstnanci (ICAEW, 2005), environmentální rizika či další rizika operativního charakteru (ICAEW, 2005; Crovini, 2019; Ambroise & Prim-Allaz, 2017).

I vzhledem ke zranitelnosti těchto podniků a specifické povaze rizik, kterým tyto společnosti čelí, existuje shoda, že právě u této skupiny podniků existuje vyšší potřeba pro adopci RM, než je tomu u podniků velkých (Yeo & Lai, 2004; Kirytopoulos et al., 2001; Bérard & Teyssier, 2017). V souvislosti s tím se objevuje i potřeba vývoje specifických metodik pro řízení rizik pro malé podnikání (Crovini, 2019; Ferreira de Araújo et al., 2020). V kontrastu s tím však část výzkumů poukazuje na fakt, že v současně době existující metodiky pro management rizik nikterak nereflektují potřeby této skupiny podniků (Crovini, 2019).

Ačkoliv i v případě skupiny malých a středních podniků bylo potvrzeno, že podniky implementující risk management dosahují lepších výsledků a větší stability než podniky ostatní, obecné výsledky, co se chování jednotlivých subjektů týče, se značně odlišují (St-Pierre & Lacoursiére, 2017), a to právě v souvislosti s výše uvedenými

charakteristikami této skupiny organizací. Mnohým firmám totiž chybí znalosti, zdroje a spolehlivé nástroje na podporu aplikace RM (Bérard & Teyssier, 2017; Crovini et al., 2021; Ferreira de Araújo et al., 2020). V důsledku nedostatku finančních prostředků si malé podniky nemohou dovolit najímat specialisty, díky čemuž není možné nedostatečné znalosti nabýt ani externí cestou (Bérard & Teyssier, 2017). Obecně existuje v prostředí malých a středních podniků jen malé povědomí o RM (Bérard & Teyssier, 2017).

Bérard & Teyssier (2017) v této souvislosti uvádí jako klíčové pro implementace RM u MSP nutnost školení RM k definování kultury rizik a rizikové strategie, dostatek času k provedení činností RM a zapojení klíčových zúčastněných stran do procesu RM. Dle Seville & Teyssiér (2017) se primárně jedná o vlastníka organizace.

Podnětem pro rozvoj či adopci RM v prostředí MSP mohou být nově přijímaná legislativní či jiná normativní opatřením (viz kapitola 3.2.2), jimž tato skupina podniků musí vyhovět (Aureli & Salvatore, 2013).

3.3 Ochrana soukromí a řízení osobních údajů v organizaci

Všechny podniky, včetně veřejných institucí, mohou vlastnit anebo zpracovávat některé osobní údaje (Bakhoum et al., 2018).

Problematika ochrany osobních údajů úzce souvisí s problematikou zajišťování soukromí. Dörr & Weaver (2014) uvádějí, že „soukromý život“ je pojem, pro který není možné vytvořit vyčerpávající definici. Jako takové totiž soukromí sestává z celé řady podoblastí týkajících se fyzického soukromí, soukromí při sdružování se, soukromí v komunikaci nebo také informačního soukromí (Dammann & Simitis; 1997).

Právní úprava, a tedy i pojetí toho, co se za soukromí považuje, se neustále vyvíjí. Některými autory je právo na soukromí vykládáno jako právo být o samotě (Bracanović, 2018). Ačkoliv historicky existoval právní rámec ochrany soukromí (Dörr & Weaver, 2014; Sharma, 2020), k častějším úpravám v této oblasti dochází v souvislosti s rozvojem informačních technologií (Sharma, 2020). Kromě již dříve uvažované koncepce, která se do té doby vztahovala na fyzickou existenci, a informace související s jednotlivcem (jeho domovem, dokumenty a osobním životem), byla postupně zahrnuta i perspektiva další – a to sběru a poskytování osobních údajů (Sharma, 2020).

K přijetí prvních regulací v prostředí EU docházelo v 70. letech minulého století, a to na národních úrovních (Newman, 2008; Dörr & Weaver; 2014). Následně v roce 1995 byla přijata Směrnice o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (EP & EUC, 1995), jež byla platná pro všechny země EU (Dörr & Weaver, 2014; González Fuster, 2014). Soukromí lze v kontextu regulatorních opatření z toho období definovat jako kontrolu nad vlastními osobními údaji (Bracanović, 2018; Alford, 2020; Sharma, 2020). Jinými slovy jde o právo rozhodnout, co se má a může (smí) s osobními údaji dít (Golbeck, 2020), a to na základě právního rámce, který stanovuje hranice mezi osobním a veřejným zájmem (Dörr & Weaver, 2014). V tomto kontextu tak lze právo na soukromí také vykládat jako ochranu osobních údajů před nezákonným zpracováním a užitím (Bakhoum et al.; 2018).[21]

Právní úprava soukromí má rovněž návaznost na řadu dalších právních oblasti. Dle Bakhoum et al. (2018) na tuto problematiku musí být brán zřetele v oblastech, jako jsou:

- Smluvní právo
- Spotřebitelské právo
- Zákony týkající se hospodářské soutěže
- Majetkové právo
- Právo duševního vlastnictví
- Antidiskriminační zákony (Bakhoum et al. (2018)

3.3.1 Osobní údaje

Dle Bakhoum et al. (2018) jsou osobní údaje a jejich použití základním stavebním kamenem digitální ekonomiky, a to vzhledem k faktu, že rostoucí počet organizací je na osobních údajích, jakožto klíčovému vstupu své činnosti, závislých. Platný úzus považuje za osobní údaje:

„*Veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů), kdy identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat.*“ (ÚOOÚ, 2017)

[21] V anglicky psané literatuře je tématika ochrany osobních údajů také označována jako data privacy (Martin et al., 2020; Jaatinen, 2016) nebo information privacy (Smith et al., 2011; Presthus & Sorum, 2019; Dammann & Simitis, 1997). Specificky pro prostředí internetu také jako online privacy (Bashir et al., 2016; Anic et al. 2019; Barth et al., 2019)

Tato definice je fakticky totožná s výkladem pojmu jak v Nařízení na ochranu osobních údajů (Alford, 2020), tak i s definicemi užívanými ve Spojených státech amerických (de Hert et al., 2016). Evropská legislativa dále tento pojem upřesňuje tím, že se jedná o údaje fyzické osoby, která je naživu (Alford, 2020; Agentura Evropské unie pro základní práva & Rada Evropy [FRA & Rada Evropy], 2018).[22]

Identifikovatelnost v tomto případě nevyžaduje, aby soubor informací obsahoval jméno či intimní údaje dané osoby. Primárním kritériem je, zda na základě daných informací lze danou osobu ztotožnit (Sharma, 2020). ÚOOÚ (2017) dále odkazuje zejména na identifikační čísla (např. rodné číslo) nebo na jeden či více zvláštních prvků fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity. I proto lze za osobní údaj považovat takzvané on-line identifikátory (Alford, 2020), jako jsou například IP adresa, cookies, lokalizační data, aplikace, identifikátory využívaných zařízení a podobně (Alford, 2020; Sharma, 2020; Voigt & von dem Bussche, 2017).

FRA & Rada Evropy (2018) dále specifikují možné kategorie osobních údajů jako:

- Údaje poskytované v elektronické komunikaci
- Údaje o zdravotním stavu
- Údaje získané za účelem výzkumu
- Finanční údaje (FRA & Rada Evropy, 2018)

Kategorizace osobních údajů, jež organizace zpracovávají, je dle Sharma (2020) důležitým aspektem při plánování řízení osobních údajů v organizaci, a to vzhledem k tomu, že ne všem typům osobních údajů je věnována stejná právní ochrana. Takzvané citlivé údaje, uvedené v Modernizované úmluvě č. 108 a v právních předpisech EU o ochraně údajů vyžadují zvýšenou ochranu, a proto podléhají zvláštnímu právnímu režimu (FRA & Rada Evropy; 2018). GDPR tyto údaje označuje souhrnně jako speciální (zvláštní) kategorie osobních údajů (EP & EUC, 2016). Zvláštní kategorie osobních údajů jsou údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech. Dále se jedná o genetické údaje, biometrické údaje, údaje týkající zdravotního stavu, sexuálního života či údaje odhalující

[22] Dle výkladu Ministerstva pro místní rozvoj České republiky [MMR] (2018) se GDPR na údaje o zemřelých osobách nevztahuje za podmínky, že se tyto údaje zároveň netýkají jiné žijící osoby (zpravidla osoby blízké), jejíž právo na ochranu soukromého života by mohlo být dotčeno (MMR, 2018). Zároveň Článek 27 obecného nařízení upřesňuje, že právní úpravu zpracování osobních údajů mohou stanovit jednotlivé členské státy (EP & EUC, 2016, č. 27).

kriminální minulost (FRA & Rada Evropy, 2018; Alford, 2020; Mali, n.d.; Kindt, 2018; Kounoudes & Kapitsaki, 2020; Kuner et al., 2020). V neposlední řadě se jedná o údaje o dětech (Starčevič et al. 2018; Tikkinen-Pirri et al., 2018).

3.3.2 Zajišťování soukromí v on-line prostředí

Spotřebitelem vnímaná potřeba soukromí se analogicky promítá i v jeho spotřebitelském chování. I vzhledem k neustálému nárůstu lidí využívajících internet a růstu nákupů na internetu (EC, 2019b) stává se zajišťování soukromí zákazníků důležitým aspektem řízení každé firmy podnikající nejen v segmentu B2C[23] (Bakhoum et al., 2018).

I na podkladu dostupných poznatků má totiž faktor zabezpečení soukromí vliv na to, jak je společnost vnímána zákazníkem (Bleier et al., 2020), přičemž platí, že již samotné zpracování osobních údajů může vyvolávat celou řadu pochybností (Slepchuk & Milne, 2020). Jako další příčiny vzniku pochybností byly dále identifikovány potenciální zranitelnost a netransparentnost správce osobních údajů vnímané spotřebitelem (Martin & Murphy, 2017; van der Waerdt, 2020).

Dalším z možných podpůrných důvodů narůstajících pochybností je i fakt, že stále méně zákazníků rozumí metodám, které společnosti ke zpracovávání využívají (Slepchuk & Milne, 2020). V tomto ohledu tak i mnohé pokusy o zmírnění znepokojení technickými metodami mohou být vzhledem ke své sofistikovanosti paradoxně neúčinné (Cloarec, 2020). V neposlední řádě jsou dalším pramenem pochybností takzvané informační asymetrie (Bashir et al., 2016; van der Waerdt, 2020).

Na druhé straně možné pochybnosti, ba dokonce zneužití osobních údajů nutně nemusí znamenat, že subjekt osobních údajů (v tomto případě spotřebitel) automaticky omezí přístup/spolupráci. Golbeck (2020) definuje tři skupiny spotřebitelů:

- Fundamentalisty, kteří za žádných okolností nejsou ochotni poskytovat své osobní údaje.
- Neznejistěné, kteří v protikladu k fundamentalistům poskytují jakékoliv osobní údaje.
- Pragmatiky, kteří zvažují možný benefit plynoucí z poskytovaných osobních údajů.

[23] Vzhledem k předchozímu výkladu pojmu soukromí se regulace vztahují i na pracovněprávní vztahy (Lueck, 2020; Hamilton & Sodeman, 2020).

Stran poslední skupiny Bleier et al. (2020) nebo Sharma (2020) uvádějí, že vždy záleží na míře benefitů, které z poskytnutí osobních údajů spotřebitel získá v porovnání s cenou (riziky zneužití), přičemž vnímání rizika či získané protihodnoty je vždy zcela individuální (Smith et al., 2011). Jak dále Bleier et al. (2020) dodávají, společnosti se nutně nemusejí vydávat směrem snižování pochybností, ale naopak mohou poskytovat adekvátní protihodnotu, například poskytnutím prémiového obsahu (Choi et al., 2019), lepší personalizací či finančními odměnami (Smith et al., 2011). Pravděpodobnost udělení souhlasu správci ke zpracování (poskytnutí osobních údajů) zvyšuje například i relevance a zábavnost obsahu (Xu et al., 2011; Krafft et al., 2017).

I s ohledem na předchozí fakt je proto široce doporučován zákaznicky centrický přístup k zákazníkem individuálně nastavované úrovni soukromí (Banerjee et al., 2020; Rust, 2020; Thomaz et al., 2020). Annant et al. (2020) dále zmiňují uchopení této problematiky jako součást marketingového vyznění značky (Annant et al., 2020).

3.3.3 Koncepce řízení osobních údajů

Zpracování osobních údajů je dle ÚOOÚ (2018) jakákoli operace nebo soubor operací, která je prováděna s osobními údaji (nebo jejich soubory). Jmenovitě jsou pak jmenovány činnosti jako shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo jakékoliv jiná manipulace s osobními údaji. Za zpracování se dále považuje pouze systematická, nikoliv nahodilá činnost (ÚOOU, 2018).

Na konkrétní podobu těchto činností v organizaci pak mají vliv alespoň dva aspekty. Tím prvním je platný právní rámec řízení osobních údajů, jimiž se musí organizace řídit. V prostředí České republiky je závazná jak legislativa schválená českými orgány, tak orgány EU, přičemž evropská legislativa je do českého právního systému zpravidla implementována či formálně adoptována (EC, 2020). Jakékoliv činnosti, jež jsou předmětem platné regulace, musí odpovídat takto definovaným požadavkům.

Druhou perspektivou jsou požadavky normativní zakotvující soubor doporučení vedoucí k adekvátnímu řízení v této oblasti[24] (Škeřík, 2016).

[24] Uvažována může být i třetí perspektiva, a to plnění vlastních požadavků v podnikovém systému řízení osobních údajů, které si společnosti mohou definovat nad rámec legislativy a odvětvových norem. Ze své podstaty mohou nabývat takřka jakékoliv formální i obsahové podoby. Vzhledem ke své podstatě nebudou dále popisovány. I tak ovšem budou uvažovány při prováděném výzkumu.

Zatímco perspektiva legislativní stanovuje **minimální požadavky**, jež musí společnost dodržovat, plnění odvětvových standardů je na dobrovolnosti každé organizace (de Hert et al., 2016; Hatto, 2013). Jejich certifikací ovšem společnost v dané oblasti deklaruje svou kompetenci a aplikaci přístupů takzvané **dobré praxe v organizaci** (de Hert et al., 2016).

Zmíněné perspektivy nemají vylučující charakter a jejich prvky a ustanovení se mohou vzájemně prolínat. Z hlediska řízení osobních údajů znamená certifikace požadavků ISO 27001 i splnění některých kroků vyplývajících z požadavků GDPR (Mesquida & Mas, 2015; Diamantopoulou et al., 2020). To bude popsáno dále (v kapitole 3.3.3.1). Na straně druhé Nařízení o ochraně osobních údajů kodifikuje náhled na řízení osobní údaje z perspektivy jejich rizikovosti (EP & EUC, 2016). Právě tento přístup byl dříve definován normami ISO skupiny 27000 (Politou et al., 2018). Souvislosti mezi standardizovanými postupy dle existujících norem, legislativními požadavky a managementem rizik budou popsány níže v kap. 3.3.3.2.

3.3.3.1 Legislativní perspektiva zajišťování soukromí

Jak již bylo zmíněno v kapitole 3.3.3, minimální požadavky řízení osobních údajů, jimiž se musí organizace řídit, jsou definovány platnými legislativními opatřeními. Jak uvádějí Bakhoum et al. (2018), legislativní rámec prochází neustálou úpravou, a to i vzhledem k narůstajícímu znepokojení spotřebitelů v této oblasti a vzrůstající významnosti tohoto druhu aktiva pro podnik. Regulace v tomto ohledu umožňuje zmírňovat negativní efekty, jež jsou se zpracováním spojené, kdy z obecného hlediska je dle některých autorů cílem evropských zákonů o zpracování osobních údajů a o smlouvách v oblasti B2C zajistit transparentnost, poskytnout práva slabší straně a uložit obchodníkům a správcům údajů povinnosti (Bakhoum et. al, 2018).

Primární legislativní úpravou je v tomto ohledu Obecné nařízení o ochraně osobní údajů (zkráceně známo jako GDPR), což je směrnice EU vymezující právní rámec ochrany osobních údajů všech občanů EU. Toto nařízení nahrazuje směrnici předchozí z roku 1995 (EP & EUC, 1995). Projednávání nové směrnice začalo v roce 2012, kdy se všeobecně etablovalo pod označením GDPR (EC, 2012). Nařízení bylo přijato v roce 2016, přičemž účinnosti nabylo 25. května 2018 (EP & EUC, 2016).

V českém prostředí se problematice řízení osobních údajů týkají následující zákony a vyhlášky:

- Zákon č. 110/2019 Sb. o zpracování osobních údajů:
    - Adaptační zákon provádějící určitá ustanovení obecného nařízení (GDPR).
    - Nad rámec GDPR upřesňuje zásady zpracování a ochrany osobních údajů, na něž se obecné nařízení nevztahuje.
    - Nahradil předchozí Zákon č. 101/2000 Sb. o ochraně osobních údajů (ÚOOU, 2019; ÚOOU, 2021a).
- Zákon č. 89/2012 Sb., občanský zákoník:
    - Upravuje nakládání s osobními údaji, jež není považováno za zpracování dle dříve uvedené definice (ÚOOU, 2021a).
- Zákon č. 181/2014 Sb. o kybernetické bezpečnosti:
    - Upravuje práva a povinnosti osob v oblasti kybernetické bezpečnosti.
    - Upravuje zajišťování bezpečnosti elektronických komunikací a informačních systémů (Národní úřad pro kybernetickou bezpečnost, n.d.)
- Zákon č. 365/2000 Sb. o informačních systémech veřejné správy:
    - stanoví práva a povinnosti správců informačních systémů veřejné správy (ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.
- Zákon č. 480/2004 Sb. o některých službách informační spolehlivosti:
    - Tento zákon upravuje v souladu s právem Evropských společenství odpovědnost a práva a povinnosti osob, které poskytují služby informační společnosti a šíří obchodní sdělení.
- Zákon č. 262/2006 Sb., zákoník práce.
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti:
    - upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.
- Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti.

Dle ÚOOÚ se na právní úpravě zpracování osobních údajů věnuje následujících sedm evropských regulací, které se týkají digitální agendy:

- Akt o správě dat
- Akt o digitálních trzích
- Akt o digitálních službách
- Návrh aktu o datech
- Návrh aktu o umělé inteligenci
- Návrh nařízení o evropské digitální identitě
- Návrh nařízení o soukromí a elektronických komunikacích (anglicky ePrivacy regulation) (ÚOOU, 2023a)

3.3.3.2 Normativní perspektiva zajišťování soukromí

Standardy ochrany údajů nabývají na důležitosti, společnosti čelí stále složitějšímu úkolu vyhodnotit, zda jsou jejich činnosti zpracování údajů v souladu s právními požadavky, a to zejména v mezinárodním kontextu (Voigt & von dem Bussche, 2017; Barafort et al., 2017). Mezinárodní organizace pro standardizaci (ISO) jako standard definuje „*dokument vytvořený na základě širokého konsenzu a schválený uznaným orgánem, který pro běžné a opakované použití stanoví pravidla, pokyny nebo charakteristiky pro činnosti nebo jejich výsledky, zaměřený na dosažení optimálního stupně pořádku v daném kontextu*.“ (NBN Shop, 1998)

Mezinárodní standardy tak představují nástroj pro sjednocení praktik organizací s existující právní úpravou. Ze své podstaty jsou mezinárodní standardy dobrovolnými soubory předpisů (de Hert, 2018; Hatto, 2013), které v případě širokého přijetí v odvětví, či žádné legislativní alternativy, mohou dosáhnout statusu „měkkého zákona“[25] (de Hert, 2018). Pro oblast informačních technologií, a tedy i zpracování osobních údajů, lze uvažovat celou řadu standardů (Barafort et al., 2017; de Hert, 2018). Vzhledem k podobnosti s GDPR bude dále v této práci prezentována skupina standardů ISO 27000 (Mesquida & Mas, 2015; Diamantopoulou et al., 2020).

[25] De Hert et al. (2018) uvádějí pojem „soft law“.

Standardy ISO 27000

V oblasti bezpečnosti informací je obecně přijímanou skupina norem ISO 27000 upravující systém řízení bezpečnosti informací (Meriah & Ben Arfa Rabai, 2019; ISO, 2018b). Bezpečnost informačních systémů je v rámci této skupiny standardů dle Čermáka (2009) hodnocena z perspektivy hodnocení a zvládání rizik. V systému ISO 27000 se za riziko považuje možnost, kdy hrozba využije zranitelnosti systému a způsobí poškození aktiva (ISO, 2018b). Za bezpečný je informační systém považován tehdy, jsou-li zachovány atributy důvěrnosti, integrity, dostupnosti a spolehlivosti (Čegan, 2020).

Normy této skupiny jsou zároveň považovány za standardy určené pro řízení informačních rizik v organizaci a řízení rizik v prostředí informačních technologií. (ISO, 2018b; Barafort et al., 2017; El Fikri et al., 2019).

Jednotlivé vzájemně související standardy jsou dále kategorizovány na:

- Standardy, které definují požadavky na systémy
- Standardy, které poskytují přímou podporu, podrobné pokyny a / nebo interpretaci celkových procesů a požadavků neustálého zlepšování (PDCA cykly)
- Standardy, které odpovídají požadavkům v jednotlivých odvětvích
- Standardy pro hodnocení souladu s normami (Meriah & Ben Arfa Rabai, 2019)

Norma ISO 27001

Norma ISO 27001 popisuje konkrétní kroky a postupy vedoucí k uchránění informačních aktiv, za která je považován shluk informací a dat, jež mají pro podnik určitou hodnotu (ISO, 2018). Prvním krokem je dle normy stanovení kontextu organizace, jehož cílem je porozumění organizaci, jejím činnostem a potřebách. Už první krok tedy stanovuje, jakým směrem bude následné řízení směřováno. Samotná norma ISO 27000 neurčuje konkrétní náležitosti, pouze definuje interní a externí aspekty, jež by při vypracování měly být brány v potaz. Organizace musí dále definovat základní politiku bezpečnosti informací a také musí stanovit odpovědnosti zaměstnanců za bezpečnost informací. (Škeřík, 2016).

V následující tabulce jsou uvedena primární informační aktiva, a to z hlediska jejich důvěrnosti.[26]

Tabulka 3-1: Dělení informací z hlediska jejich důvěrnosti

Státní organizace	**Soukromé organizace**
Utajované informace	Nechráněné informace
Osobní údaje	Chráněné informace: • Firemní interní informace • Citlivé interní informace
Interní údaje	
Ostatní údaje	
	Osobní údaje

Zdroj: vlastní zpracování (dle Škeřík, 2016)

Norma ISO 27002 definuje jednotlivé techniky vedoucí ke zmírnění rizik (Diamatopoulou et al., 2020). **Norma ISO 27003** poskytuje doporučení pro implementace bezpečnostního systému v organizaci (ISO, 2017).

Problematice osobních údajů je věnována norma ISO 27018. Tato norma poskytuje pokyny pro poskytovatele cloudových služeb, kteří zpracovávají osobní identifikační údaje a nabízí sadu ovládacích prvků, které poskytovatelé cloudových služeb musí implementovat, aby mohli řešit konkrétní rizika (de Hert et al., 2016).

3.4 Nařízení o ochraně osobních údajů (GDPR)

3.4.1 Základní informace

Celým názvem "*Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES*" představuje od 25. května 2018 právní rámec ochrany osobních údajů v evropském prostoru. Zkráceně označované jako GDPR stanovuje obecné nařízení pravidla pro zpracování osobních a vymezuje práva subjektů údajů[27] (ÚOOU, 2017). GDPR konsolidovalo všechny předchozí zákony o ochraně osobních údajů v zemích EU[28] (Alford, 2020; Golbeck, 2020). Oproti předchozím úpravám je primární orientace směřována více na práva a svobody subjektu údajů, než na pravidla zpracování pro organizace (Alford, 2020; Golbeck, 2020).

[26] Zvláštní kategorií státních organizací jsou organizace zdravotnické zpracovávající velké množství dokumentace v listinné i elektronické formě. Ta je upravena zákonem č. 101/2000 Sb., o ochraně osobních údajů. Klasifikace informaci se na rozdíl od ostatních státních organizací mírně liší.

[27] Subjektem údajů se rozumí fyzická osoba, jíž osobní údaje jsou zpracovávány (ÚOOÚ, 2017).

[28] Zatímco Směrnice EU je právním aktem Evropské unie, který má pro členské státy doporučující charakter a k její platnosti ve vybrané zemi dochází až po jejím zapracování v legislativě členské země, nařízení je platné bez ohledu na zapracování v místní legislativě (EC, 2020).

Proces úpravy předchozí právní úpravy započal v roce 2009, kdy Evropská komise zahájila veřejnou konzultaci o budoucím právním rámci pro zpracování osobních údajů. Následně v lednu 2012 předložila Evropská komise svůj návrh (EC, 2012), k jehož přijetí došlo v dubnu 2016 (FRA & Rada Evropy, 2018). Dle Steppe (2017) nebo Zerlang (2017) je přijetí GDPR možnou obecnou odpovědí na poptávku po zvýšení efektivity data managementu firem a zvýšení kyberbezpečnosti. Tyto poznatky tak korespondují i s poznatky z kapitoly 3.2.2.

Smyslem přijetí nařízení byla modernizace právních předpisů EU o ochraně osobních údajů tak, aby vyhovovaly ochraně základnách práv v kontextu ekonomických a sociálních výzev digitálního věku (FRA & Rada Evropy, 2018) a také sjednocení pravidel ochrany osobních údajů v EU[29] (ÚOOU, 2017), kdy k revizi bylo přikročeno z toho důvodu, že *„předchozí právní rámec založený směrnicí 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, již přestal odpovídat současné době, zejména pokud jde o prostředky, které jsou ke zpracování využívány, a též i pokud jde o zpracování jako takové, které je daleko komplexnější, než bylo před několika desítkami let (např. v oblasti profilování, automatizace zpracování osobních údajů atd.), a tudíž je i rizikovější pro práva a svobody fyzických osob.“* (ÚOOU, 2017)

Dle ÚOOÚ (2018) GDPR nemění základní zásady zpracování ani základní pojmy, nicméně klade vyšší nároky primárně na velké správce osobních údajů, kteří zpracovávají jejich rozsáhlé množství, díky čemuž je i toto zpracování vysoce rizikové. Platné je ovšem pro všechny subjekty bez výjimky (Sharma, 2020). Vzhledem ke své definici je GDPR platné i za hranicemi EU, neboť se vztahuje na jakýkoliv subjekt, který zpracovává osobní údaje občanů Evropské unie (Sharma, 2020).

[29] Předchozí právní fragmentace a výsledná právní nejistota byla rovněž považována za překážku ve výkonu hospodářských činností na úrovni EU, a to především na správce působící ve více zemích EU (Voigt & von dem Bussche, 2017; ÚOOÚ, 2017).

3.4.2 Zásady pro zpracování osobních údajů dle GDPR

Dle FRA & Rady Evropy (2018) existuje sedm základních principů, jimž musí zpracování osobních údajů dle GDPR odpovídat. Dle ÚOOÚ (2018) jsou zásady zpracování základním kamenem každého zpracování (ÚOOU, 2017):

- **Princip zákonnosti, férovosti a transparentnosti zpracování**

Každé zpracování osobních údajů musí být prováděno na základě konkrétního právního důvodu (EC, 2016; Sharma, 2020). Právní důvody jsou nezbytné pro doložení legálnosti zpracování (Alford, 2020). V případě, že neexistuje právní důvod ke zpracování, musí být údaje zlikvidovány. Dle GDPR lze zpracovávat osobních údaje na základě těchto šesti právních důvodů:

  - subjekt údajů udělil souhlas se zpracováním za konkrétním účelem (účely),
  - zpracování je nezbytné pro plnění smluvních povinností – uzavření smlouvy, doručení zásilky apod.,
  - zpracování je nezbytné pro splnění jiné právní povinnosti, jež se na správce vztahuje – vedení účetnictví,
  - zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
  - zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu, případně při výkonu veřejné moci,
  - zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů[30], kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů – za určitých předpokladů marketingové aktivity (ÚOOU, 2018; EC, 2016; ÚOOU, 2018a).

Například v případě přímého marketingu lze údaje zpracovávat na základě oprávněného zájmu, nebo souhlasu (EC, 2016; ÚOOU, 2018a). Hranice, kdy je souhlas vyžadován a kdy nikoliv, ovšem v Nařízení není explicitně zmíněna, což kriticky zmiňují i někteří autoři. (van der Corput & van der Stroom, 2019; Hanáková, 2020) V tomto případě je výklad ponechán národním autoritám.

[30] Dále je specifikováno, že tento právní důvod lze využít, když před těmito zájmy nemají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů (ÚOOÚ, 2017).

V GDPR je dále stanoveno, že zpracování by mělo probíhat férově, přičemž by měl být subjekt údajů obeznámený s možnými riziky, a to v pro něj srozumitelném jazyce (FRA & Rada Evropy, 2018).

- **Zásada omezení účelu zpracování**

Účel zpracování údajů musí být definován před zahájením zpracování (Kuner et al., 2020). Nelze zpracovávat údaje způsobem, který je neslučitelný s původním účelem, ačkoli obecné nařízení o ochraně údajů stanoví výjimky z tohoto pravidla pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu a pro statistické účely. Zásada omezení účelu v podstatě znamená, že jakékoli zpracování osobních údajů musí být provedeno pro konkrétní přesně definovaný účel a pouze pro další, konkrétní účely, které jsou slučitelné s původním. (FRA & Rada Evropy, 2018)

- **Princip minimalizace dat**

Zpracování údajů musí být omezeno na to, co je nezbytné pro splnění legitimního účelu. Zpracování osobních údajů by mělo probíhat pouze tehdy, když účel zpracování nelze přiměřeně splnit jinými prostředky. Zpracování údajů nesmí nepřiměřeně zasahovat do příslušných zájmů, práv a svobod (FRA & Rada Evropy, 2018).

- **Princip přesnosti dat**

Zásadu přesnosti údajů musí správce implementovat ve všech operacích zpracování. Nepřesná data musí být neprodleně vymazána nebo opravena. Pro zajištění přesnosti může být nutné data pravidelně kontrolovat a aktualizovat. (FRA & Rada Evropy, 2018)

- **Princip omezeného uchovávání**

Princip omezení ukládání znamená, že osobní údaje musí být vymazány nebo anonymizovány, jakmile již nejsou potřebné pro účely, pro které byly shromážděny. (FRA & Rada Evropy, 2018)

- **Princip zabezpečení dat**

Každá organizace by se měla ujistit, že snižuje pravděpodobnost, že dojde k narušení bezpečnosti dat (Alford, 2020). Alford (2020) dále uvádí, že zabezpečování je nutné vzhledem k riziku udělení pokuty, vzhledem k nařízení, negativním dopadů na každodenní činnost organizace nebo z důvodu možného narušení důvěry u spotřebitele.

- **Princip odpovědnosti**

Odpovědnost vyžaduje, aby správci a zpracovatelé aktivně a průběžně prováděli opatření na podporu a ochranu ochrany údajů při svých činnostech zpracování. Správci a zpracovatelé odpovídají za soulad svých operací zpracování s právními předpisy o ochraně údajů a jejich příslušnými povinnostmi. Správci musí být schopni kdykoli prokázat dodržování ustanovení o ochraně údajů subjektům údajů, široké veřejnosti a dozorovým úřadům. Zpracovatelé musí rovněž dodržovat některé povinnosti přísně spojené s odpovědností (například vedení záznamů o zpracovatelských operacích a jmenování inspektora ochrany údajů). (FRA & Rada Evropy, 2018)

3.4.3 Práva subjektů

Jak již bylo zmíněno, GDPR zvyšuje práva subjektů vzhledem k ochraně jejich osobních údajů (Yuan & Li, 2019; Larrucea et al., 2020). Jak ovšem zmiňuje FRA & Rada Evropy (2018), právo na ochranu osobních údajů není právem absolutním a toto právo může být omezeno za účelem veřejného zájem nebo za účelem ochrany práv a svobod ostatních fyzických osob (viz právní základy pro zpracování, u kterých není souhlas potřebný). Účelem nařízení je tedy i vybalancování vztahu mezi správcem a subjektem údajů (ÚOOU, 2017).

GDPR přiznává subjektům údajům především tato práva:

- právo na přístup k osobním údajům,
- právo na opravu,
- právo na výmaz (také označováno jako právo být zapomenut),
- právo na omezení zpracování,
- právo na přenositelnost údajů,
- právo vznést námitku,
- právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, zahrnujíce i profilování. (ÚOOU, 2017).

Oproti předchozí právní úpravě došlo k rozšíření o poslední tři výše zmíněná práva (Alford, 2020; ÚOOU, 2017). Zároveň platí, že každá osoba, která utrpěla hmotnou nebo nemajetkovou újmu v důsledku porušení tohoto nařízení, má právo na náhradu škody od správce nebo zpracovatele (Mali, n.d.; Sharma, 2020; FRA & Rada Evropy, 2018)

3.4.4 Sankce

Oproti předchozí právní úpravě zvyšuje GDPR hranice maximálního možného udělení pokut. Výše udělení pokuty vyplývá ze zpracování osobních údajů, ke kterému dochází v rozporu s obecným nařízením (tedy také v rozporu s definovanými zásadami výše). GDPR uvádí dvě možné kategorie udělení pokuty[31]:

- 20 mil. Eur nebo 4 % z celosvětového obratu organizace loňského roku,
- 10 mil. Eur nebo 2 % z celosvětového obratu organizace loňského roku.

Tato pokuta nemusí být udělena pouze v souvislosti se zpracováváním osobních údajů, ale může být udělena i případě porušení jiných formálních ustanovení (například Správních záležitostí) (Alford, 2020).

Rozdělení do dvou skupin odráží důležitost porušených povinností, kdy ve skupině s vyšší sazbou jsou povinnosti, u jejichž porušení je očekávána vyšší intenzita zásahu do práva na ochranu osobních údajů, které obecné nařízení zajišťuje (ÚOOU, 2017). Za takovéto porušení se dále považuje nedodržení jedné ze zásad ochrany údajů, porušení práv jednotlivce nebo neoprávněné předání údajů do třetích zemí (Alford, 2020; Mali, n.d.). Nižší pokuta pak může být udělena v případě porušení jiných ustanovení právních předpisů (např. porušení ustanovení týkajících se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů) (Alford, 2020).

Pokuta může být udělena nezávislou centrální autoritou[32] v dané zemi EU (Alford, 2020). V případě České republiky se jedná o Úřad na ochranu osobních údajů (ÚOOU, 2017). Zároveň například únik údajů nemusí nutně znamenat udělení sankce (Alford, 2020), stejně jako může být udělena pokuta, aniž by k úniku dat došlo (ÚOOU, 2017).

3.4.5 Implementace GDPR v organizaci

Součástí odpovědi na otázku „Jaké jsou předpoklady úspěšné implementace u malého a středního podniku?“ je nutné nejprve definovat, co se za úspěšnou implementaci považuje. V kontextu této práce bude za úspěšnou implementaci považován takový stav, kdy správce či zpracovatel plní všechny požadavky vyplývající z nařízení, a to v souladu

[31] Maximální možná hranice je stanovena na základě toho, která ze dvou výše uvedených částek je vyšší (FRA & Rada Evropy, 2018; Mali, n.d.).

[32] Centrální autority jsou odpovědné za prosazování nařízení na vnitrostátní úrovni a mají za úkol poskytovat rady a pokyny podnikům a jednotlivcům (Alford, 2020).

se všemi definovanými zásadami (ÚOOU, 2017). Takovýto stav se nazývá „compliance“ (Voigt & von dem Bussche, 2017; Mali, n.d.), v českém překladu „vyhovění“.

Implementující organizace by měla pro ochranu osobních údajů využít pseudonymizaci a šifrování osobních údajů. Dále by měla být schopna:

- udržet trvalou důvěrnost, integritu, dostupnost, přístupnost a odolnost systému a služeb,
- obnovit a zpřístupnit osobní údaje v případě předchozího narušení fyzického nebo technického zabezpečení,
- testovat a hodnotit účinnost technických a organizačních opatření (Mali, n.d.).

Konkrétní postupy a využívané metody jsou dle dikce GDPR na implementujícím subjektu (Mali, n.d.). Článek 32 dále předpokládá, že vybrané metody a postupy budou respektovat současný stav techniky, kontext zpracování, rizikový profil organizace a nákladnost implementace vůči rizikovému profilu organizace[33] (Mali, n.d.; Sharma, 2020; Kuner et al., 2020).

Výše zmíněné aspekty zcela determinují rozsah implementačního projektu v organizaci – jeho časový rámec, nákladnost i výslednou kvalitu.

Jakékoliv zpracování osobních údajů je vždy spojeno s různě závažnými riziky, která se týkají jejich možného zneužití, odcizení či ztráty (Bakhoum et al., 2018; Sharma, 2020). GDPR nařizuje přístup ke zpracování dat založený na riziku explicitně (Voigt & von dem Bussche, 2017), kde se vhodnost zabezpečení dat je odvozena od rizika, které vyplývá ze správcem uchovávaných informací.

Přístup založený na riziku v širším slova smyslu znamená, že správce již od počátku koncipování zpracování osobních údajů musí brát zřetel na možná rizika pro práva a svobody fyzických osob, kterým musí být přizpůsobeno i zabezpečení dat (ÚOOU, 2017). I na základě článku 32 je smyslem celého implementačního projektu možná rizika pro subjekt dat zmirňovat (Hoofnagle et al., 2019; Alford, 2020; Sharma, 2020).

Dle Sharma (2020) lze při rozhodování, zda je úroveň ochrany údajů vhodná, zvažovat tři následující skupiny rizik:

[33] Rizikový profil organizace je: „*Snímek rizikového portfolia v konkrétním časovém okamžiku (minulém, současném nebo budoucím).“* (Lam, 2018, s. 229)

- **Rizika pro organizaci**

Toto pojetí vychází z definice pojmu rizika jakožto jakéhokoliv jevu, který má na organizaci negativní dopad (Hubbard, 2020; Green, 2016; Hunziker, 2019). Správce nebo zpracovatel musí vždy brát v úvahu finanční riziko nedodržení GDPR, které by mohlo vést k udělení pokuty ze strany centrální autority (Sharma, 2020). Další možnou perspektivou je riziko soudních sporů, které by mohly vzniknout z důvodu porušení práv subjektu. V tomto ohledu lze zmínit i nepřímé náklady spojené se ztrátou důvěryhodnosti organizace vůči zákazníkovi (Martin et al., 2020; Yuan & Li, 2019). V neposlední řadě může být pro organizaci rizikem možná ztráta údajů.

- **Rizika pro subjekt**

Vzhledem k povaze tohoto rizika je riziko pro subjekt analogicky vždy rizikem i pro samotnou organizaci. Za toto riziko se považuje jakékoliv možné riziko, jež má za následek újmu pro subjekt dat (ÚOOU, 2017; EP & EUC, 2016). Zvýšená pozornost je pak věnována zvláštním kategoriím osobních údajů, která jsou spojená s vyšší potenciální újmou (ÚOOU, 2017) i vyšším rizikem odcizení (Prakash & Singaravel, 2015). Od závažnosti rizika vůči subjektu se dále odvíjí i výše potenciální udělené pokuty (ÚOOU, 2017; EP & EUC, 2016).

- **Rizika způsobená třetími stranami**

Třetí skupina s ohledem na zpracování je spojena s dalšími zainteresovanými stranami. Tato skupina může zahrnovat jak záměrné útoky na vlastní systém ze strany počítačových zločinců, tak i některé zástupce regulačních úřadů (v telekomunikaci, zdravotnictví apod.). Do této skupiny lze dále řadit i skupiny dodavatelů služeb, kteří jsou zpracovateli údajů a u nichž je implementace GDPR rovněž očekávána (ÚOOU, 2018b).

Jiné dělení rizik dle Alforda (2020) rizika kategorizují na fyzická, procesní a softwarová.

Praktiky managementu rizik s ohledem na implementaci GDPR

Druhou perspektivou vazby mezi managementem rizik a GDPR je začlenění dílčích kroků managementu rizik plně do implementačního projektu, konkrétně pak analýzy rizik. Analýza rizik je aplikována v rámci Posouzení vlivu na ochranu osobních údajů (DPIA). Ačkoliv je provedení DPIA taxativně dáno pouze v případě, že budoucí zpracování představuje vysoké riziko pro práva a svobody fyzických osob (ÚOOU, 2018c), někteří autoři doporučují provádět posouzení vždy (Kindt, 2018). Tabulka 3-2

uvádí srovnání postupů pro DPIA s obecným postupem analýzy rizik dle Smejkala & Raise (2013).

Tabulka 3-2: Analýza rizika (Porovnání DPIA a mananegement rizik)

Modelová DPIA dle Microsoft	**Obecný postup analýzy rizik dle Smejkala**
Kritéria pro akceptaci rizik	Stanovení hranice analýzy rizik
Aktiva a jejich hodnoty	Identifikace aktiv
Hrozby a zranitelnosti	Stanovení hodnoty a seskupování aktiv
Ohodnocení rizik	Identifikace hrozeb
Analýza shody	Analýza hrozeb a zranitelností
	Pravděpodobnost jevu
	Měření rizika

Zdroj: vlastní zpracování (dle Microsoft, 2017; Smejkal & Rais 2013)

V tomto kontextu lze tedy soudit na obsahovou podobnost mezi managementem rizik a implementací GDPR. Zmínky o hodnocení a analýze rizik jsou pak přímo zmíněny v GDPR, ve článcích 76 a 77 (EP & EUC, 2016).

V obecné rovině lze nalézt souvislost mezi managementem rizik, standardy ISO 27000 a implementací GDPR vzhledem k tomu, že řízení bezpečnosti informací plně kooptovalo problematiku managementu rizik (Barafort et al., 2017) a analýza rizik je považována za jednu z nejdůležitějších etap za účelem zjištění zranitelných míst informačního systému organizace (viz ISO 27000). To nakonec potvrzují i doposud provedené výzkumy, kdy například Diamantopoulou et al. (2020) uvádějí, že některé společnosti certifikované podle norem ISO 27000 využívaly společné synergické efekty k urychlení implementace GDPR. V některých dalších případech implementaci GDPR usnadnila dříve implementovaná ISO 27000 (Longras et al., 2018). Předchozí adopci těchto standardů dále doporučuje například Bindley (2019), a to právě s ohledem na společný přístup založený na riziku a aplikaci „best practices“.

4 Dopady implementace GDPR na řízení malého podniku

Jak bylo popsáno v cílech výzkumu v úvodu této práce, v rámci smíšeného výzkumu bude v první části realizován výzkum kvalitativní, jehož cílem je **na základě relevantních zdrojů vymezit současné poznání v oblasti implementace GDPR a jejích důsledků na činnosti a podnikové oblasti se zaměřením na malé podniky**.

Důvodem výběru kvalitativního přístupu ke zkoumání v této části disertačního výzkumu je fakt, že kvalitativní výzkum umožňuje kombinovat různé teoretické postoje a postupy. Zároveň v rámci kvalitativní strategie se schéma a procedury mohou v průběhu výzkumu rozvíjet (Gray, 2009; Punch, 2015). To plně vychází z podstaty nařízení, které i přes obecně známé požadavky na implementaci či přímou vazbu na management rizik nedefinuje žádné konkrétní postupy, jak implementace (stavu „compliance“) dosáhnout (Garber, 2018).

V této kapitoly jsou v souladu s dílčími cílem výzkumu vyznačeným výše a na základě teoretických východisek výzkumu definovány jak výzkumná otázka, tak specifické výzkumné otázky.

Smyslem definovaného dílčího cíle je odpovědět na výzkumnou otázku: ***„Jaké je současné poznání v oblasti implementace GDPR a jejích dopadů na činnosti a řízení malých podniků?***“. Takto definována výzkumná otázka je následně rozložena na tyto specifické výzkumné otázky (SVO):

- *SVO1.1. Které činnosti a oblasti podniku jsou implementací GDPR ovlivněny?*

Na základě předchozích poznatků jsou implementací GDPR ovlivněny všechny procesy, oblasti a činnosti, v nichž dochází ke zpracování osobních údajů (kapitola 3.4). Nicméně doposud nedošlo ke shrnutí, o které konkrétní činnosti a oblasti se v prostředí organizace jedná. Jinými slovy, na které konkrétní činnosti má implementace GDPR vliv. Smyslem této dílčí výzkumné otázky je takovéto podnikové činnosti a oblasti (v jiné terminologii také podnikové procesy) identifikovat.

Identifikovány budou nejprve všechny literaturou zmiňované činnosti bez ohledu na organizační kontext (malý podnik, e-shop, obchodní společnost atd.).

- *SVO1.2. Jaké jsou dopady na implementací ovlivněné oblasti a činnosti?*

U výše identifikovaných činností a oblasti dle *SVO1.1.* je dále cílem odpovědět, jaké povahy tyto dopady jsou.

- *SVO1.3. Jakým způsobem jsou definovány stávající postupy pro implementaci GDPR v organizacích?*

Vzhledem k tomu, že GDPR nepředepisuje konkrétní postup nebo teoretický rámec, na jehož základě má být norma v organizacích implementována (Garber, 2018) a požadavky jsou vymezené obecně (kapitola 3.4.2), je smyslem takto položené výzkumné otázky odpovědět, které doposud známé postupy a přístupy k implementaci GDPR lze identifikovat a jaký je pro existující postupy využívaný teoretický rámec.

- *SVO1.4. Které aktivity lze do implementace GDPR zahrnout?*

Má-li být vymezeno současné poznání v oblasti implementace GDPR v případě podniků, je cílem této otázky odpovědět, jaké lze identifikovat všechny činnosti a oblasti, jimiž je nutné se pro splnění požadavků v případě organizací zabývat. Platí-li, že způsob implementace je dán na kontextu konkrétního implementujícího subjektu (Mali, n.d.).

- *SVO1.5. Jaké existují odlišnosti v implementaci v případě malých organizací v porovnání s organizacemi velkými?*

Jelikož nejsou známé charakteristiky skupiny malých e-shopu, pracuje se v této části se skupinou malých podniků, u které jsou na jedné známé její hlavní charakteristiky (například kapitola 3.2.5) a zároveň jsou známy možné odlišnosti se skupinou velkých podniků s ohledem na implementaci GDPR, kdy nařízení definuje dodatečné povinnosti pro velké organizace[34]. Cílem této části je zodpovědět, jaké jsou v této souvislosti rozdíly mezi skupinou malých podniků a skupinou velkých podniků, co se praktické implementace GDPR týče. Vzhledem k možným rozdílům v terminologii, za malý podnik se považují dle definice (EC, 2019) i mikropodniky a podniky střední.

Z výše uvedených dílčích výzkumných otázek vyplývá, že pro splnění dílčího cíle bylo definováno celkem pět specifických výzkumných otázek. Počet definovaných dílčích otázek je v tomto ohledu v souladu s metodickými doporučeními (Creswell, 2013).

[34] Dle kapitoly 3.4.5 lze očekávat vyšší riziko zpracování u společností, které provádějí zpracování OÚ ve větší rozsahu. Obvykle se jedná o podniky velké. Požadavky na ochranu osobních údajů jsou v tomto ohledu analogicky vyšší. Typickým příkladem je provedení DPIA nebo jmenování DPO (ÚOOÚ, 2017).

4.1 Metodika systematické literární rešerše

Pro zodpovězení výše uvedených otázek je zapotřebí definovat takový postup výzkumu, který uvažuje jak zdroje akademické, tak i zdroje komerční. Pro zahrnutí vedle zdrojů akademických i zdrojů komerčních lze uvést následující důvody. Dle Briner & Denyer (2012) je celkovým záměrem výzkumů a studií v oblasti managementu a organizací prohloubení současných znalostí a poskytnutí vhledu do praxe organizací. Zároveň platí, že praktiky organizací jsou zřídka založeny na dostupných akademických publikacích. Místo toho organizace aplikují takzvané nejlepší praktiky a postupy nabízené ze stran konzultačních a jiných komerčních subjektů (Briner & Denyer, 2012). I proto Paez (2018) uvádí takzvanou šedou literaturu[35] jako důležitý zdroj pro systematickou rešerši.

Stejné poznatky platí i v případě implementace GDPR, a to i na základě předchozích teoretických východisek, kdy od nabytí účinnosti regulace doposud nebyl vytvořen jednotný teoretický rámec pro implementaci GDPR v organizacích. Přístup k systematické rešerši založený jak na akademické literatuře, tak šedé literatuře se označuje jako Multivocal Literature Review (Garousi et al., 2019; Zhang et al, 2021). Opisný překlad tohoto pojmu zní „**Mnohostranná literární rešerše**“. Tento přístup je nejčastěji využíván v oblasti počítačové vědy[36]. V oblasti společenských věd nebo podnikové ekonomiky a managementu byl tento přístup již několikrát využit (Fox et al., 2020; Kemell et al., 2020; Shoaib et al., 2021; Sánchez-Gordó & Colombo-Palacios, 2021). Kritéria pro zařazení zdrojů do rešerše jsou uvedeny v následujících podkapitolách.

Kromě již výše zmíněných důvodů je šedá literatura v mnohostranné systematické rešerši uvažována i vzhledem k podobnosti implementace GDPR a norem ISO (Diamantopoulou et al, 2020) či počtu organizací, jež pro implementaci GDPR využívaly služeb komerčních subjektů (Faifr & Januška, 2021; Sirur et al., 2018).

[35] Dle Paez (2018, s. 233) lze šedou literaturu definovat jako: „*zdroj publikovaný ve všech úrovních veřejné, akademické, podnikové i průmyslové sféry v tištěné nebo elektronické podobě, jehož publikování není kontrolováno komerčními vydavateli*.“

[36] Dle Web of Science se jedná o kategorie „Computer Science“

4.2 Zdroje dat a kritéria výběru

Jak u literatury akademické, tak literatury šedé je definován odlišný přístup k výběru relevantních publikaci. V následujících podkapitolách je pro obě skupiny uveden postup.

4.2.1 Akademické publikace

Na základě zavedených metod a postupů (Jesson et al., 2011; Bryner & Denyer, 2012), byla literární rešerše provedena na základě analýzy relevantních publikací, a to prohledáním literárních zdrojů v databázi Web of Science Core Collection.

- **Web of Science Core Collection** je on-line akademická služba založená společností Thomson Reuters umožňující přístup do databází. V současnosti je touto službou indexováno více než 21 tisíc časopisů s více než 79 miliony záznamy (Libguides.com, 2021).

Dle Gusenbauer & Haddaway (2020) je tato databáze vhodná pro sestavování systematických rešerší, neboť splňuje všechny specifické požadavky. Dalším důvodem výběru databáze je její interdisciplinární zaměření.

Vzhledem k cíli výzkumu a v souladu s doporučenými postupy byla následně definována kritéria pro zařazení výstupu definována následujícím způsobem:

Tabulka 4-1: Kritéria pro zařazení výstupu (akademická literatura)

Kritérium	**Podmínka zařazení**
Kategorie	Business; Business & Finance; Economics; Management; Multidisciplinary Sciences; Public Administration; Social Sciences (Interdisciplinary); Information Science & Library Science; Operations Research & Management Science; Computer Science (information systems; artificial intelligence; theory & methods)[37]
Typ výstupu	článek v odborném časopise, konferenční výstup, rešerše, kapitoly v knize
Časový horizont	Leden 2016 – do současnosti[38],[39]
Jazyk	angličtina, čeština
Geografické omezení publikací	bez omezení

Zdroj: vlastní zpracování

[37] Tato kategorie zahrnuje i časopisy, které se zabývají managementem informací a managementem znalostí. Gray (2009) pak doporučuje v rámci výzkumů organizací interdisciplinární přístup ke zkoumání, který jako takový umožní pochopit prostředí organizací z více různých perspektiv.

[38] Mapování publikací bylo provedeno v období měsíců června a července 2021. Zmapované výstupy tedy byly databází Web of Knowledge indexovány před 1. srpnem 2021.

[39] Takto definovaná kritéria dále umožňují i zařazení časopisů, jež jsou zařazené i v jiné než výše uvedené kategorii. Podmínkou ovšem je, aby byl časopis zařazen také alespoň do jedné z výše uvedených kategorií.

Dle typu výstupu byly uvažovány jak články, tak i publikované rešerše, přičemž byly uvažovány výstupy publikované od období přijetí nařízení v dubnu 2016. Pro výběr byly uvažovány všechny výstupy publikované **od ledna 2016**. Vzhledem k teritoriální působnosti GDPR pak jsou uvažovány výstupy publikované v časopisech po celém světě i autory z celého světa.

Na základě výše uvedených kritérií pak byly vyhledány výstupy na základě klíčových slov v kombinacích, které jsou definovány následujícím způsobem:

- Výchozí klíčové slovo - „GDPR“ OR „General Data Protection Regulation“
- AND „implementation“ OR „compliance“ OR „impact“ OR „process“ OR „business“ OR „small business“ OR „SME“

Zadaná fráze je pak hledána v názvu příspěvku, stejně jako v abstraktech či seznamu klíčových slov. V databázi Web of Knowledge je tento způsob hledání označován jako: „Topic“.

4.2.2 Šedá literatura

Druhým zdrojem dat mnohostranné rešerše je již výše zmíněná šedá literatura (Paez, 2018). Na základě doporučení Adams et al. (2017) a v kontextu definovaných specifických výzkumných otázek jsou pro literární rešerši zahrnuty v různých formách následující zdroje:

- Výzkumy a průzkumy
- Případové studie
- Právní výklady
- Návody
- Expertní příspěvky
- Blogové příspěvky
- Reporty

Pro tuto část zdrojů je zřejmý jiný přístup ke sběru a výběru zdrojů, neboť neexistuje žádná relevantní databáze, z níž by mohly být relevantní zdroje vybírány. Dle nastíněného postupu dle Garousi et al. (2019) bude proto pro vyhledání relevantních zdrojů využit **Vyhledávač Google**[40].

[40] Vyhledávač Google byl navržen Sergeyem Brinem a Lawrencem Pagem v rámci výzkumu na Stanfordově univerzitě (Brin & Page, 1998). V současnosti se jedná o celosvětově nejvyužívanější internetový vyhledávač (Statcounter Global Stats, 2022).

Tabulka 4-2 uvádí omezující podmínky (kritéria pro zařazení) pro získání relevantních zdrojů:

Tabulka 4-2: Kritéria pro zařazení výstupu (šedá literatura)

Kritérium	**Podmínka zařazení**
Vyhledávač	Google (www.google.com)
Klíčová slova v anglickém jazykem	GDPR implementation; GDPR compliance; GDPR impact; GDPR business; GDPR process; GDPR small business; GDPR SMEs;
Klíčová slova v českém jazyce	implementace GDPR; dopady GDPR; GDPR procesy; GDPR malé podniky; GDPR MSP
Typ výstupu	dle vymezení výše
Časový horizont publikování	leden 2016 - do současnosti
Jazyk	angličtina, čeština
Geografické omezení	celosvětově (bez omezení)
Kritérium pro ukončení vyhledávání	100 výsledků pro každé klíčové slovo (U každé kombinace klíčových slov prvních 10 stran ve Vyhledávání Google, na každé straně je zobrazeno 10 unikátních výsledků.)

Zdroj: vlastní vypracování

Vyhledávaná klíčová slova jsou definována podobně jako v případě systematické literární rešerše. Dle Garousi et al. (2019) je třeba rovněž vymezit kritéria pro ukončení dalšího hledání. Pro případ této rešerše bylo vyhledávání ukončeno po nalezení 100 relevantních výsledků odpovídajících i ostatním definovaným kritériím.

Následně jsou v tomto textu definována i kritéria pro vyřazení zdrojů, která jsou podstatnou součástí analýzy kvality zdrojů (Garousi et al., 2019). Tato kritéria jsou vymezena v následující tabulce:

Tabulka 4-3: Podmínky pro vyřazení výstupu (šedá literatura)

Kritérium	**Podmínka pro vyřazení**
Autor:	Není známa ani fyzická ani právnická osoba
Kredibilita zdroje:	Nižší než 3. úroveň kvality zdrojů dle Adams et al. (2017)
Zaměření výsledků:	Není souvislost s podnikovou ekonomikou

Zdroj: vlastní zpracování

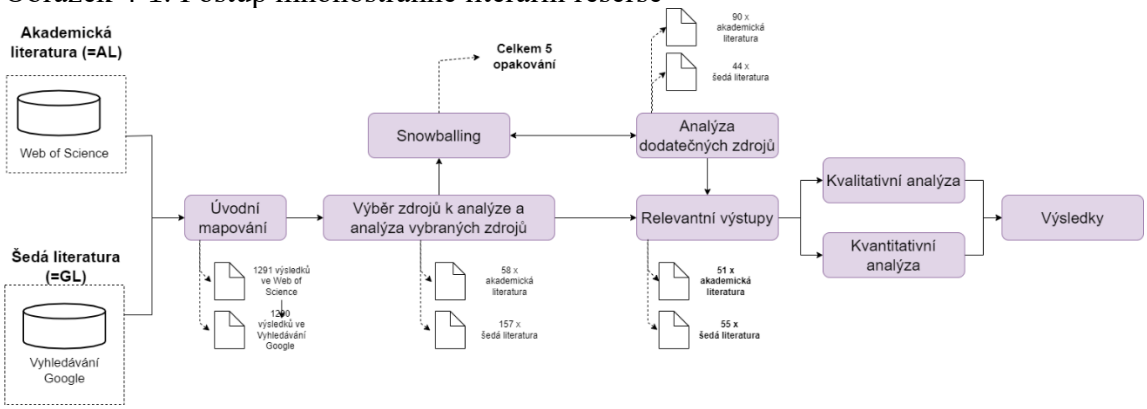
4.3 Sběr dat

Na obrázku 4-1 je znázorněn celý postup provedené mnohostranné rešerše. V úvodní fázi rešerše byly zmapování dostupné zdroje akademické i šedé literatury. Následně byl proveden výběr publikací pro bližší analýzu na základě názvu a případně také abstraktu publikace a byla provedena bližší analýza publikací.

V tomto kroku byly vzhledem k definovaným kritériím vyřazeny nerelevantní zdroje a byly zmapovány související potenciálně relevantní výsledky (více v kapitole 4.3.2),

z nichž byly následně vyřazeny zdroje nerelevantní. U celkem 107 relevantních výstupů byla následně provedena jejich kvantitativní a kvalitativní analýza. Poznatky z relevantních publikací budou následně prezentovány v kapitole „Výsledky“.

Obrázek 4-1: Postup mnohostranné literární rešerše



Zdroj: vlastní zpracování

Jednotlivé kroky literární rešerše jsou blíže popsány v následujících podkapitolách.

4.3.1 Výběr zdrojů k analýze

Na základě definovaných klíčových slov, bylo v databázi Web of Knowledge nalezeno nejprve 1291 výsledků pro výraz „GDPR“ nebo „General Data Protection Regulation“. Zadanému výrazu odpovídaly výstupy v celkem 128 různých kategoriích, které jsou definovány v databázi Web of Knowledge. Takovýto počet kategorií svědčí o tom, že přestože se jedná o výraz jednoznačně ohraničený[41], problematika GDPR má své důsledky pro velký počet vědních oborů.

V kombinaci s rozšiřujícími klíčovými slovy a dalšími nastavenými kritérii, jejímž smyslem bylo zaměřit hledání na zkoumanou problematiku, bylo nalezeno celkem **58 výsledků**, které byly následně zkoumány podrobně.

Dle nastavené metodiky výzkumu následně proběhl tentýž postup u šedé literatury, a to s využitím Vyhledávání Google. Celkem bylo zkoumáno 1200 různých výsledků (12 vyhledávaných výrazů krát 100 výsledků). I s ohledem na možné duplicity v nalezených výsledcích při opakovaném vyhledávání bylo k bližšímu zkoumání vybráno **157 výstupů**, které odpovídaly dříve zadaným kritériím.

[41] V odborných příspěvcích lze najít pouze jediné alternativní využití pro výraz „GDPR“, kdy se jedná o záměnu za jednofázový polykrystal (zkráceně označovaný jako „GdPr-123“) nebo o chemickou sloučeninu GDP-ribose (zkráceně označovanou jako „GDPR“) (Yamani & Akhavan, M., 1996; Zhanga et at., 2009). Jiné využití klíčového slova „GDPR“ známo není.

4.3.2 Snowballing

Aby byly nalezeny další relevantní podklady a byly kompenzovány možné nedostatky využitých způsobů vyhledávání relevantních zdrojů, byl jak u akademických zdrojů, tak zdrojů šedé literatury aplikován takzvaný „snowballing“ (Wohlin, 2014). Tato technika sestává ze zkoumání všech zdrojů souvisejících s dříve relevantním výstupem. V případě MLR se jedná o zdroje související s nalezenými akademickými články i šedou literaturou.

Pro potřeby této práce byl využit jak dopředný, tak zpětný snowballing:

- Zpětný (Backward snowballing) - u identifikovaných výstupů obou typů byly zkoumány zdroje, na něž tyto výstupy odkazovaly.
- Dopředný (Forward snowballing) – tento způsob bude využit pouze u akademických příspěvků. Databáze Web of Knowledge mapuje i publikace, jež vyhledaný příspěvek citovaly. V literární rešerši tedy budou zahrnuty i tyto výstupy (Wohlin, 2014).

Aby mohly být takto dohledané zdroje zařazeny do analýzy, musí splňovat kritéria, jež byla specificky definována pro oba typy zdrojů. Výjimku v případě akademické literatury tvoří výstupy, jež byly indexovány kromě databáze Web of Science i v dalších vědeckých databázích (Scopus, IEEE,…), a to vzhledem ke své relevanci vůči primárnímu zdroji. Tímto postupem, který sestával celkem z 5 iterací[42], bylo k bližší analýze vybráno dodatečných 90 akademických zdrojů a 44 zdrojů šedé literatury.

4.3.3 Vyřazení nerelevantních výstupů

Na základě předchozích dvou kroků hledání bylo celkově bližší analýze (analýza abstraktu a textu výstupu) podrobeno 349 výsledků hledání (148 akademických zdrojů, 201 šedé literatury). Během zkoumání dílčích výstupů bylo následně vyřazeno 96 výstupů akademické literatury a 144 šedé literatury.

U akademické literatury nejčastější důvodem pro vyřazení daného výsledku byla duplicita hledání[43], nezpřístupněná volná verze textu či nerelevance vůči zkoumanému tématu

[42] U každého sekundárně nalezeného zdroje byl proveden jak dopředný, tak zpětný snowballing a to až do okamžiku, kdy již nebyly žádné dodatečné zdroje identifikovány.
[43] Původní hledáním nalezená publikace byla opětovně identifikována během prováděného snowballingu.

(daný výstup neadresoval žádnou z definovaných dílčích výzkumných otázek uvedených v kapitole 4).

V případě šedé literatury byly nejčastějšími důvody vyřazení zdroje jeho nerelevance vůči definovaným výzkumným otázkám a nedůvěryhodnost zdroje projevující se například neznámým datem publikování příspěvku, neuvedených autorem nalezeného výstupu, případně publikace, které referovaly vůči GDPR platnému ve Spojeném Království[44].

V rámci mnohostranné literární rešerše tedy bylo nakonec identifikováno 106 relevantních zdrojů, 51 akademických zdrojů a 55 zdrojů šedé literatury. Kompletní seznam sesbíraných výstupů je součástí přílohy této práce (**Příloha B**).

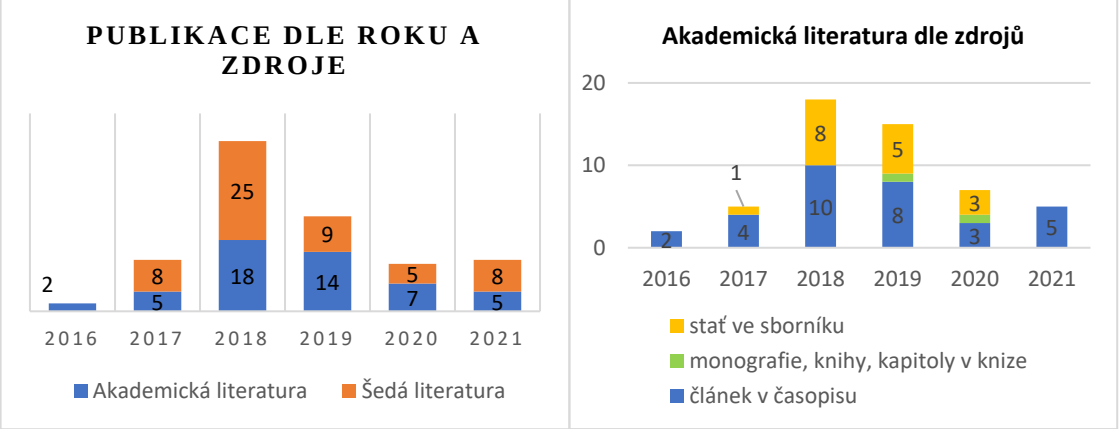
[44] Vzhledem k vystoupení Spojeného království z Evropské unie může dojít k záměně, kdy regulace platná pro toto území nese stejné označení. Také označováno jako UK GDPR. Ve výběru byly ponechány výsledky, které se zabývaly GDPR před vystoupením Velké Británie z Evropské unie (Information Commissioner´s Office, n.d.).

4.4 Kvantitativní analýza nalezených publikací

V této části jsou kvantitativně analyzovány nalezené výstupy, a to z hlediska roku vydání publikace, jejich typologického rozřazení, které je dle typu výstupu zvlášť analyzováno u literatury akademické i šedé.

Z analyzovaných výstupů na obrázku 4-2 je zřejmé, že co počtu publikací přímo zabývajících se implementací bylo nejvíce výstupů jak v akademické, tak také v mimoakademické oblasti v roce 2018, tedy v roce, kdy GDPR nabylo své účinnosti. Výrazněji je pak v roce 2018 zastoupena šedá literatura. V předchozích letech 2016, 2017 je zjevný rostoucí trend, co do počtu publikací, jež se implementací zabývaly. Jednalo se o vyšší jednotky výstupů. V letech 2019 až 2021 pak lze naopak sledovat trend sestupný.

Obrázek 4-2: Výstupy dle roku publikace



V rámci akademické literatury byly nejčastěji zastoupeny články v odborných časopisech, a to primárně rešerše literatury, druhým nejčastějším výstupem pak jsou konceptuální modely týkající se implementace GDPR. Tyto modely byly zpravidla publikovány ve sbornících z vědeckých konferencí. Dalšími významnými skupinami publikací jsou prezentované původní výzkumy, případně expertní příspěvky publikované v odborných časopisech. Absenci příspěvků z konferencí v roce 2021 lze vysvětlit dobou mezi publikací daného příspěvku či sborníku a jeho indexací v databázi Web of Science.

Tabulka 4-4: Rozdělení akademických publikací dle typu výstupu

	článek v časopisu	**stať ve sborníku**	**kniha, monografie**	**kapitola v knize**	**Celkem**
Modely	6	9	0	1	**16**
Rešerše	12	3	0	0	**15**
Původní výzkum	4	5	1	0	**10**
Expertní příspěvky	10	0	0	0	**10**
Celkem	**32**	**17**	**1**	**1**	**51**

V kontrastu s literaturou akademickou byly v rámci šedé literatury nejčastější formou výstupu návody na implementaci GDPR, které tvořily 33 z 55 všech relevantních výsledků. Zbývající část sestupně tvořily právní výklady nařízení, vlastní výzkumy, expertní příspěvky a další různé formy publikací.

Tabulka 4-5: Šedá literatura dle roku publikace

Typ publikace	**2017**	**2018**	**2019**	**2020**	**2021**	**Celkem**
e-book, e-dokument	4	9	5	1	2	**21**
článek	1	10	1	2	2	**16**
blog	2	5	2	2	3	**14**
oficiální dokument	1	1	1	0	1	**4**
Celkem	**8**	**25**	**9**	**5**	**8**	**55**

Zdroj: vlastní zpracování

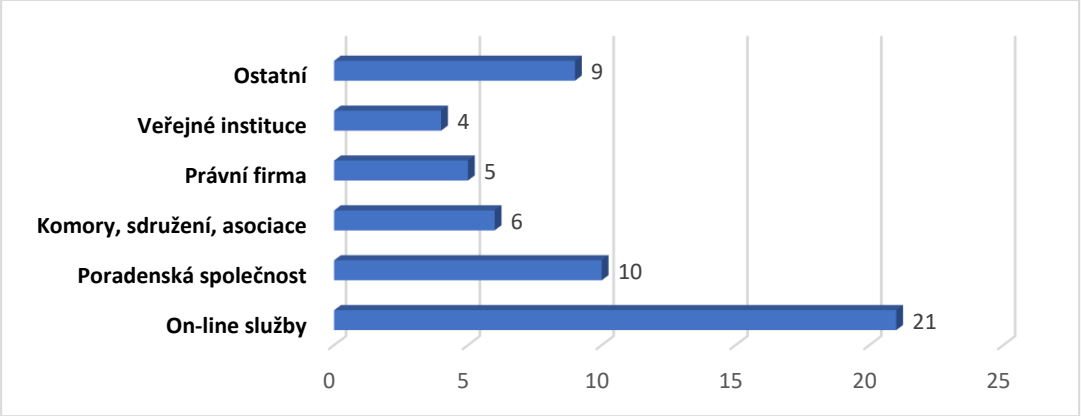
Tabulka 4-6: Šedá literatura dle typu publikace

	Návod	**Výzkum**	**Právní výklad**	**Expertní příspěvky**	**jiné**	**Celkem**
e-book, e-dokument	12	6	0	0	3	**21**
článek	12	1	2	1	0	**16**
blog	5	0	4	3	2	**14**
oficiální dokument	4	0	0	0	0	**4**
Celkem	**33**	**7**	**6**	**4**	**5**	**55**

Zdroj: vlastní zpracování

Nejčastěji zastoupenou skupinou organizací zabývající se implementací GDPR byly organizace, které poskytují různé formy on-line služeb, následované poradenskými firmami, komorami a sdružení či právnickými organizacemi.

Obrázek 4-3: Zdroje šedé literatury dle publikujících subjektů



Zdroj: vlastní zpracování

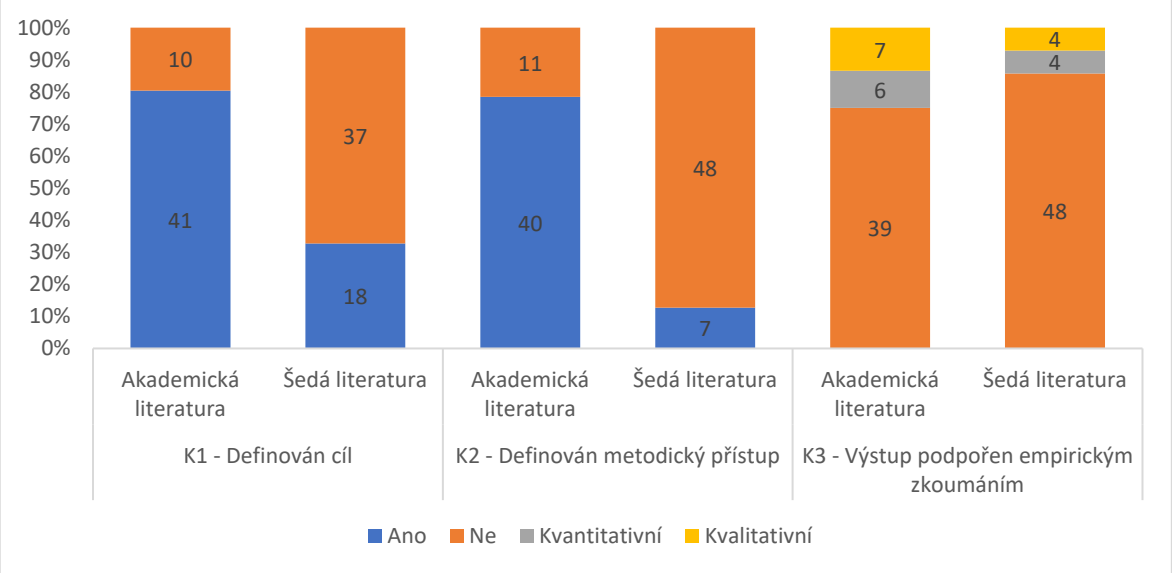
4.5 Kvalitativní analýza publikací

Každý z nalezených relevantních výstupů byl následně podroben analýze kvalitativní, a to jak z hlediska kvality výstupu samotného, tak jeho relevance v porovnání s definovanými výzkumnými otázky. V této části budou zvlášť srovnávány zdroje akademické a zdroje šedé literatury.

Pro analýzu kvality výstupu byla předem definována tato tři kritéria:

- Definice cíle výzkumu (K1) – je jednoznačně definován výzkumný cíl publikace.
- Metodický přístup (K2) – v publikaci je věnován prostor pro jednoznačnou definici metodického přístupu, jenž vede k uvedeným závěrům.
- Podpora empirických zkoumání (K3) – publikované závěry a dílčí výstupy práce jsou podpořeny vlastním empirickým zkoumáním, a to buď kvantitativní či kvalitativní povahy.

Obrázek 4-4: Kvalita relevantních publikací



Zdroj: vlastní zpracování

Z celkového počtu 107 zkoumaných publikací byl celkem u 60 z nich definován cíl publikované práce (K1), přičemž výraznou část tvoří výsledky akademické (41). V případě akademické literatury pouze 10 výstupů z celkového počtu 51 nemělo jednoznačně definovaný svůj cíl. Převážnou část takovýchto výstupů (7 výstupů) tvořily expertní posudky publikované do roku 2018, tedy do doby před nabytím či v přibližné

době nabytí účinnosti nové regulace. Na druhé straně ve zkoumané šedé literatuře mělo svůj cíl definováno pouze 18 výstupů. Důvodem může být povaha výstupů šedé literatury.

Podobně jako v případě kritéria K1 lze následně shrnout kvalitu prací s ohledem na definovaný metodický přístup. Z 11 výstupů bez definovaného metodického přístupu v akademické literatuře se v 9 případech jedná o expertní příspěvky a komentáře, v jednom případě o konceptuální modely a v jednom případě o publikované rešerše literatury. Na druhé straně pouze 7 z vybraných výstupů šedé literatury mělo explicitně definovaný metodický přístup k získání výstupu. Ve dvou případech se jednalo o výstupy poradenské společnosti Deloitte, v jednom případě o společnost Baker&McKenzie.

Obecně pouze minoritní část všech výstupů byla podpořena libovolnou formou empirického zkoumání (K3). Z celkem 19 empirických studií a výzkumů bylo u 13 využito zkoumání kvalitativní, v 8 případech pak využito zkoumání kvantitativní. Dva výstupy pak kombinovaly obě tyto formy, je tedy započítán u obou forem výstupů.

4.6 Výsledky

Věcná analýza relevantních zdrojů byla provedena s využitím software Nvivo[45], který je určen pro kvalitativní analýzu dat (QDA). U každého zdroje byly označeny pro jednotlivé výzkumné otázky relevantní pasáže. Níže jsou uvedeny výsledky strukturované v posloupnosti dle jednotlivých dílčích výzkumných otázek.

4.6.1 Implementací ovlivněné podnikové oblasti a činnosti

První částí analýzy současného poznání je vymezení všech podnikových oblastí, vůči kterým má GDPR, jakožto platný legislativní rámec, dle analyzovaných zdrojů své důsledky. Studiem celkem 106 zdrojů literatury, které svým zaměřením i kvalitou odpovídají zadaným kritériím, bylo identifikováno (analyzovanými publikacemi) celkem 13 podnikových oblastí, jež v souladu s definicemi lze označit jako podnikové procesy (Řepa, 2007; van Rosing et al., 2014) a vůči nimž má GDPR své důsledky.

Počet podnikových oblastí, jež jsou současnou literaturou považovány za ovlivněné implementací GDPR, podporuje dříve zmíněné poznatky týkající se interdisciplinarity dané problematiky i tvrzení, která toto nařízení považují pro řízení organizací za potenciálně disruptivní (Garber, 2018).

[45] NVivo je počítačový software určený pro kvalitativní analýzu dat (McNiff, 2016).

V tabulce 4-7 níže je uveden seznam identifikovaných oblastí. Ty jsou seřazeny sestupně dle počtu odkazů ve zkoumané literatuře. Vzhledem k ne vždy jasné ohraničitelnosti vybrané oblasti jsou výčtově uvedeny pro daný proces vždy i analyzovanou literaturou uváděné související výrazy či podprocesy. Za odkaz se považuje unikátní zmínění oblasti (včetně souvisejícího podprocesů) v daném zdroji[46].

Tabulka 4-7: GDPR ovlivněné podnikové oblasti dle rešerše

Podniková oblast	**Počet odkazů**	**Uváděné související činnosti/podprocesy**[47]
Řízení dat, informací a znalostí[48]	55	Řízení dat, řízení informací; řízení znalosti; Big data; Business intelligence; Analýza dat; Informační systémy; Ochrana dat; Bezpečnost dat; Uložení dat; Řízení osobních údajů
Marketing a prodej	31	Marketing; Prodej; E-mail marketing; Marketing na sociálních sítích; On-line marketing; On-line reklama; Digitální marketing; Personalizovaný marketing; Přímý marketing; **Řízení vztahu se zákazníkem**[49]
Řízení lidských zdrojů	21	Řízení vztahu se zaměstnancem
Řízení rizik	12	Posouzení rizik
Právo	8	-
Vývoj a inovace	8	Inovace; Řízení vývoje produktu
Řízení bezpečnosti	5	Bezpečnost práce
Strategické řízení	4	
Řízení dodavatelských řetězců (vstupní logistika)	4	Řízení vztahu s dodavateli; Řízení logistického řetězce
Účetnictví	2	Mzdové účetnictví
Management změn	1	-
Compliance management	1	-
Audit management	1	-

Zdroj: vlastní zpracování

Z výsledků je patrné, že nejčastěji jsou literaturou definovány dopady na oblast podnikového řízení dat, informací, okrajově také zahrnující i oblast řízení znalostí,

[46] V každém zdroji mohou být identifikovány dopady na více podnikových oblastí. Více dopadů na tutéž podnikovou oblast jedním zdrojem se uvažuje jako jeden odkaz.

[47] Struktura podnikových procesů je individuální vždy dle kontextu dané organizace, některé podprocesy mohou být součástí i jiného podnikového procesu, než výše uvedeného celku. Agenda řízení OÚ může být například vnímána také jako samostatná oblast, případně jako součást marketingu nebo HR-

[48] **Tučně jsou v uvedené tabulce zvýrazněny všechny činnosti, jež byly v rámci kapitoly 3.1.5 uvedeny jako klíčové z hlediska řízení e-shopu.**

[49] Ačkoliv byly činnost Marketing a prodej a Péče o zákazníky definovány jako samostatné činnosti, v případě provedené rešerše nebylo zpravidla možné tyto oblasti stran dopadů implementace GDPR oddělit. Pro další potřeby budou obě činnosti analyzovány, coby součást jednoho celku. Například aktivitu „e-mail marketing“ lze na jedné straně zařadit jako aktivitu, jež je součástí marketingových aktivit, na druhé ovšem také v některých případech jako aktivitu týkající se udržování a péči o vztah se zákazníkem.

a to jak z hlediska celkového počtu odkazujících zdrojů, kdy ze 75 zdrojů (implikujících alespoň jeden dopad na proces čí procesní prostředí organizace) vyvozovalo přímo či nepřímo důsledky na tuto skupinu procesů 55 zdrojů, tak i z hlediska šíře uvažovaných dopadů a ovlivněných dílčích podprocesů, kdy kromě explicitních dopadů na ochranu osobních údajů (ochrana dat, bezpečnost dat, osobní údaje) byly mimo jiné implikovány dopady i pro oblast znalostí organizace, Big data, analýzy dat (alternativně jako Business Intelligence) či obecné informační infrastruktury organizace.

Druhou nejčastěji zmiňovanou oblastí je marketing a jeho dílčí podoblasti či aktivity. Celkem v 31 případech byly vyvozeny dopady na aktivity, jež jsou prováděny s využitím internetu, případně ty aktivity, u kterých dochází ke kontaktu se zákazníkem či jeho daty.

Kromě osobních údajů zákazníků ovšem organizace zpracovávají i osobní údaje svých zaměstnanců, tato agenda je v literatuře zmiňována jako třetí v pořadí, kdy se dopady na oblast řízení lidských zdrojů zabývalo celkem 21 různých zdrojů. Další oblastí s více než 10 odkazy je dále řízení rizik, a to vzhledem ke své přímě vazbě na implementaci GDPR, konkrétně provádění analýzy rizik. Vedle toho také vzhledem k faktu, že Nařízení „rizikový přístup“ při zabezpečování osobních údajů předpokládá, jak bylo popsáno v kapitole 3.4.2.

V celém výčtů oblastí jsou publikovány dopady na právní procesy, inovační aktivity, obecné řízení bezpečnosti v organizacích, důsledky pro strategické řízení firem a management změn. V souhrnu zkoumané literatury pak vždy v jednom případě byly definovány další nejednoznačně zařaditelné interdisciplinární oblasti, a totiž compliance management (řízení směřující ke splňování regulačních norem) a audit management (řízení směřující k úspěšnému absolvování podnikových auditů).

Jak lze vidět z níže uvedené tabulky 4-8, kromě přibližně totožného zájmu o dopady na podnikové řízení dat se výstupy šedé literatury relativně častěji zabývají dopady na marketingové aktivity organizací. Naopak v akademické literatuře lze nalézt větší důraz na management rizik a inovační aktivity organizací. U zbývajících oblastí již rozdíly nejsou výrazné. Dopady na řízení změn, management auditů a compliance managementem se alespoň prozatím zabývá výhradně literatura šedá, a to zcela okrajově.

Tabulka 4-8: GDPR ovlivněné podnikové oblasti dle rešerše (dle zdroje literatury)

Související proces	Akademická literatura	Šedá literatura	Celkem
Řízení dat a informací	27	28	55
Marketing a prodej	11	20	31
Řízení lidských zdrojů	11	10	21
Řízení rizik	8	4	12
Vývoj a inovace	6	2	8
Právo	4	4	8
Řízení bezpečnosti	4	1	5
Řízení dodavatelských řetězců	0	4	4
Strategické řízení	2	2	4
Účetnictví	1	1	2
Management změn	0	1	1
Audit management	0	1	1
Compliance management	0	1	1

Zdroj: vlastní zpracování

4.6.2 Procesní změny

V předchozí části byly vymezeny oblasti, na něž má GDPR a potažmo implementace nařízení dopad. Dopadem se v tomto případě rozumí potřeba změny předchozího průběhu a nastavení dané podnikové oblasti tak, aby bylo v souladu s nařízením.

V této části budou analyzovány dopady z věcného hlediska. Vzhledem k různé povaze publikovaných příspěvků (různé cíle, metodické přístupy, používaná terminologie apod.) se analogicky odlišují i definované dopady, a to co do míry specifikace (nebo naopak obecnosti) daného dopadu, specifikace konkrétního procesu, na nějž se dopad vztahuje (obecný dopad na řízení procesů, konkrétní proces nebo podproces), případně specifikace fáze (s ohledem na implementaci GDPR), ve které je daná změna realizována.

Tabulka 4-9: Rozdělení dopadů na podnikové oblasti

	Předpoklad úspěšné implementace	Dopad během implementace GDPR	Dopad jako důsledek implementace GDPR	Bez ohledu na implementaci nebo nespecifikováno	Celkem
Akademická literatura	12	50	41	57	**160**
Šedá literatura	29	47	24	49	**149**
Celkem	**41**	**97**	**65**	**106**	**309**

Zdroj: vlastní zpracování

Tabulka 4-9 rozděluje dopady s ohledem na fázi realizace implementace. Ve zkoumané literatuře bylo identifikováno celkem 309 dopadů různé povahy na dříve vymezené oblasti. Nejpočetnější skupinou je kategorie dopadů, u nichž se důsledky na řízení

podniků neváží jednoznačně na fázi v rámci implementace GDPR (tj. skupina „*Bez ohledu na implementaci nebo nebylo autory specifikován*o“). Takovýchto dopadů bylo v jednotlivých textech identifikováno celkem 106 s převahou dopadů identifikovaných v literatuře akademické (57).

Druhou nejpočetnější kategorií dopadů jsou ty změny v řízení, které jsou důsledkem aktuálně probíhajícího procesu implementace GDPR (tj. „*Během implementace GDPR*“). Tyto dopady na vybrané oblasti jsou tedy realizovány jako součást plnění požadavků. Co do počtu opět mírně převládají dopady identifikované v akademické literatuře.

Třetí nejčastější kategorií dopadů implementace GDPR jsou ty změny, které nastávají až po dokončení implementace GDPR. Tyto dopady se převážně týkají pozitivních externalit vyplývajících z implementace, dále pak aktivit, jež je třeba realizovat, aby bylo nařízení v organizaci dodržováno dlouhodobě. Tyto dopady byly výrazně častěji definovány v literatuře akademické.

Nejméně zmiňovanou z definovaných skupin je kategorie dopadů týkajících se dopadů, které jsou předpokladem zahájení implementačního projektu. Z věcného hlediska se definované dopady prolínají s těmi, jež byly identifikovány pro fázi probíhající implementace, nicméně dle dikce vybraných textů byly tyto změny definovány jako podmínka pro zahájení implementace. Právě předpoklady pro zahájení implementace se výrazně častěji zabývala šedá literatura (29 různých dopadů).

4.6.2.1 Změny v procesním prostředí

Kromě dopadů, jež bylo možné vyvodit pouze implicitně, podstatnou část tvořily dopady, které se vázaly na celé procesní prostředí organizace, nikoliv pouze na proces konkrétní. Níže definované dopady mimo jiné odvozují procesní přístup k řízení organizace. Dominantní část dopadů se pak týká fáze, ve které dochází k postupné implementaci požadavků v organizaci. Níže v tabulce 4-10 je uveden kategorizovaný přehled všech definovaných dopadů s důsledky pro procesní řízení v organizaci, včetně popisu.

Tabulka 4-10: Dopady na procesní prostředí organizace

Formulace dopadu	**Popis**	**Fáze implementace**	**Odkazující zdroje**
Obecná revize podnikových procesů	Kontrola stávajících podnikových procesů, zda splňují požadavky vyplývající z nařízení. Dále kontrola nastavení používaných ERP systémů.	Během implementace GDPR	A04, A19, A25, A41, G04
Integrace GDPR s podnikovými procesy	Integrace požadavků vyplývajících z GDPR a přístupů Privacy by design a Privacy by design se všemi souvisejícími podnikovými procesy. Dále také různé formy změn a zlepšování procesů (redesign, reengineering procesů), aby byly požadavky naplněny.	Během implementace GDPR, V důsledku implementace GDPR	A04, A10, A34, G06, G13, G29
Praktiky k zajištění udržitelnosti GDPR v organizaci	Předpokládané zavedení praktik pro udržení a zlepšování procesů v organizaci (měření a monitoring procesů, pravidelné procesní audity, automatizace procesů, reporting procesů)	Všechny definované fáze	A03, A28, A29, A50, G06, G50,
Zavedení nových podnikových procesů	Zavedení nových stálých procesů nebo procedur pro zajištění agendy GDPR (Management auditů, Compliance management). Implementace GDPR definována jako nový podnikový proces	Předpoklad úspěšné implementace, Během implementace GDPR	G04, G13, G42, G43, G55
Racionalizace a standardizace stávajících podnikových procesů	U méně vyspělých procesů procesní mapování, standardizace úkonů, zpracování procesních návodek	Během implementace GDPR, Dopad v důsledku implementace GDPR	G22, G01, G32
Změna organizační kultury	Změna principů řízení, která je zaměřená na dodržování platné legislativy	Během implementace GDPR	A25, A29
Další dílčí dopady			
Investice do nových technologií - Procesy probíhají s využitím nových technologií, které lépe umožňují dodržovat účinné nařízení. Dále také digitalizace procesů.		Během implementace GDPR, Dopad v důsledku implementace GDPR	A02
Procesní řízení jako podpora během implementace.		Během implementace	A30
Potřeba Pověřence na ochranu osobních údajů (DPO) k integraci procesů souvisejících s agendou zpracování osobních údajů.		Předpoklad úspěšné implementace	G37
V případě nepochopení nemá GDPR vliv na podnikové procesy, požadavky nejsou zpracovávány.		Bez ohledu na implementaci nebo nespecifikováno	A12

Zdroj: vlastní zpracování

Nejčastěji zmiňované dopady vůči obecnému procesnímu prostředí organizace úzce souvisí s implementací GDPR v organizaci. Dopady se týkají především revize stávajícího nastavení procesů, zda odpovídají požadavkům vyplývajícím z obecného nařízení, a to včetně revize ERP systémů a jejich datových toků. Dalšími hlavními dopady je integrace všech požadavků GDPR do takto revidovaných procesů a zavedení takových praktik, které povedou u všech podnikových procesů k udržení stavu compliance – tedy toho, že je organizace schopná dodržovat požadavky průběžně. Dalšími dopady na procesní řízení organizace je definice nových podnikových procesů a procedur, které úzce souvisejí s GDPR.

Předpokladem a zároveň možným uvažovaným přínosem vyplývajícím z implementace GDPR je racionalizace a standardizace stávajících procesů, stejně jako s tím souvisejí digitalizace procesů. Ve dvou případech je pak zmíněna obecná změna organizační kultury, která je více zaměřená na dodržování správných zásad vůči zpracovávaným osobním údajům. V souvislosti s podnikovými procesem byla zmíněna předpokládaná role DPO, jehož úkolem by měla být právě integrace stávajících procesů, tak aby odpovídaly legislativním požadavkům. V jednom případě pak byla zmíněna možná překážka v úpravě podnikových procesů, a totiž v případě, kdy platná legislativa není dostatečně pochopena.

4.6.2.2 Řízení dat a informací

Co do počtu identifikovaných dopadů a ovlivněných oblastí je dle literatury nejvíce ovlivněnou oblastí podnikové řízení dat, informací a potažmo také znalostí. Pro tuto skupinu aktivit byla definována více než třetina všech možných dopadů (120). V tabulce 4-11 níže jsou definovány dopady pro oblast řízení dat a informací, jakožto celku. Dopady jsou do jisté míry shodné, jako dopady, jež jsou vymezeny výše pro celé procesní řízení. U méně častých dopadů (zpravidla jedna zmínka) jsou dopady definovány výčtově s ohledem na relevantní fázi implementace GDPR.

Nejčastějším dopadem implementace GDPR je dle soudobé literatury pozitivní dopad na praktiky organizace prováděné v oblasti řízení dat. Druhým nejčastějším dopadem je pak obecně revize procesu samotného. Toto již vychází i z obecných dopadů na podnikové procesy organizace.

Tabulka 4-11: Dopady GDPR na řízení dat a informací dle rešerše

Formulace dopadu	**Popis**	**Fáze implementace**	**Odkazující zdroje**
Zlepšení praktik a změna přístupu v oblasti řízení dat	Koordinace řízení aktivit zpracování dat; zachycování a hodnocení rizikových zpracování; poskytování informací jednotlivcům i institucím.	Důsledek implementace GDPR	A04, A08, A23, A26, A33, G40, A46, A35
	U méně vyspělých praktik pak zmíněná disrupce celého procesu		G35, G05
Revize procesu	Kontrola stávajících praktik v oblasti řízení dat a jejich kontrola, zda splňují požadavky vyplývající z nařízení.	Během implementace GDPR	A27, A48, G43
Další přínosy vyplývající z implementace GDPR (odděleno čárkou):			
Racionalizace procesu a souvisejících podprocesů, Zvýšení konzistence dat, Zapojení DPO do procesu, lepší praktiky v hodnocení dat, Systém pro průběžnou kontrolu postupů, snížení nákladů na proces, nastavení systému založeného na odpovědnostním přístupu (accountability).			
Předpoklady úspěšné implementace s dopadem na danou oblast:			
Potřeba již historických dat, potřeba zpracovaných procesních návodů.			
Dopady při během implementace:			
Alokace zdrojů - finančních a lidských, minimalizace zpracovávaných dat.			

Zdroj: vlastní zpracování

Vedle obecných dopadů na podnikovou oblast jako celek byly identifikovány různé dopady i pro podoblasti (podprocesy). Vzhledem k vysokému počtu identifikovaných dopadů bude pro každý z výše uvedených procesů uveden pouze výčet všech specifických dopadů.

Tabulka 4-12: Dopady GDPR na oblasti řízení dat dle rešerše

Podproces:	**Formulace dopadu (odděleno čárkou):**	**Zdroje:**
Ochrana dat	Dopady na cloud computing, investice prostředků, Minimalizace zpracovávaných dat, nastavení metrik procesu, nastavení bezpečnostních metrik v procesu, pravidelný audit procesu, monitoring procesu, řízení informačních rizik, zvýšení bezpečnosti, stanovení zodpovědnosti za proces, zabezpečení databází	A03, A04, A07, A08, A19, A20, A22, A23, A24, A31, A34, A39, A42, G53, G01, G03, G04, G11, G12, G13, G25, G29, G30, G38, G40, G42, G45
Zpracování osobních údajů	Minimalizace rozsahu zpracování, nové datové toky, nové podprocesy (Personal data Security management), změna přístupu, procesní modely pro řízení osobních údajů, zvýšení etičnosti zpracování, aplikace best-practices	A01, A04, A23, A35, G50, A42, A48, G22, G24, G26, G31, G32, G36, G38
Uložení dat	Revize archivovaných dat, revizi přístupu řízení životního cyklu dat, snížení nákladů na aktivity	A23, A34, A41, A48, G04, G24, G43
Big data	Zvýšení etičnosti zpracování, změna náhledu na oblast (GDPR v kontradikci s přístupy v oblasti Big data), racionalizace procesu	A02, A22, A27, A28, A39
Analýza dat (business intelligence)	Revize procesu, zlepšení datové analýzy organizace v důsledky lepší praktik řízení dat, rozšíření podnikových znalostí	A04, A23, A26, G38
Informační systémy	Změna informační infrastruktury	A04, G13
Propojení s externími službami	Omezení v oblasti propojených služeb a zpracování dat třetí stranami, omezení předávání dat do třetích zemí	A27, A23, G41, G34

Kromě nejčastěji uvažovaných podprocesů, tj. ochrany dat a zpracování osobních údajů, byly dále uvažovány dopady na praktiky, jež se týkají uchovávání dat, analýzy dat, problematiky Big data, informační infrastruktury a datového propojení s externími službami.

4.6.2.3 Marketing a prodej

Druhou výrazně ovlivněnou oblastí dle literatury je oblast marketingu a prodeje. Na rozdíl od předchozího procesu řízení dat nemají definované dopady souvislost pouze s přímým zapracováním legislativy, nýbrž i v důsledku změny spotřebitelského chování v souvislosti s přijatou legislativou a analogickým zvýšením o této problematice v běžné populaci. Přehled všech dopadů je zobrazen v následující tabulce:

Tabulka 4-13: Dopady GDPR na marketing a prodej dle rešerše

Podproces	**Formulace dopadu (odděleno čárkou):**	**Zdroj:**
Marketing a prodej jako celek	Změny v akvizici nových zákazníků, rozsáhlé změny procesu, investice do nových technologií, zlepšení vztahu se zákazníkem (v důsledku implementace), změny ve spotřebitelských postojích, riziko ztráty důvěryhodnosti vůči zákazníkovi	A03, A05, A07, G05, G09, G13, G15, G21, G22, G24, G26, G31, G32, G34, G37, G45, A26, A34, A36, G51
E-mail marketing	Potřeba návodů	G13
Marketing na sociálních sítích	Snížení kvality dat X zlepšení výsledků kampaní	A39, G34, G41
On-line marketing	Efekt na engagement zákazníka, omezení reklam třetích stran, snížení efektivnosti reklamy	A05, A27, G33
Personalizovaný marketing	Automatizace zpracovávaných dat, zvýšení etičnosti zpracování, zlepšení výsledků, zlepšení vztahu se zákazníkem, změny ve spotřebitelském chování, nový proces (Consent management)	A05, A23, A27, A35, G51, A48, G08, G21, G33, G35, G38, G41, G44
Přímý marketing	Negativní vliv na oblast, potřebě vzdělání v oblasti osobních údajů, snížení tržeb, potřeba obnovení souhlasů se zpracováváním	G13, G37, G35, G21, G44
Péče o zákazníka	Potřeba návodů pro vedení databází	G13

Zdroj: vlastní zpracování

Na rozdíl od předchozích oblastí lze u oblasti marketingu dojít k protichůdně definovaným dopadům na tuto podnikovou oblast. Negativní důsledky jsou primárně směřovány na období před implementací GDPR. Tato fáze je spojena se sníženou dostupností zákaznických osobních údajů ve více podoblastech. V tomto důsledku je tedy předpokládaná nižší efektivita realizovaných marketingových a snížení tržeb, a to i s ohledem na změnu spotřebitelského chování. Na druhé straně úspěšná implementace dle některých zdrojů může vést k celé řadě přínosů v porovnání s obdobím před účinností GDPR. Jmenovitě se jedná o nastavení

zlepšeného vztahu se zákazníkem, zlepšení výsledků kampaní v důsledku zvýšené kvality zpracovávaných dat, snížení nákladů na marketing. V jednom případě pak dochází i k hodnocení adekvátnosti implementace, kdy je rozsah změn považován za nepřiměřený.

4.6.2.4 Řízení lidských zdrojů

Třetím významnou oblastí, jež je implementací GDPR ovlivněna, je řízení lidských zdrojů. Na tuto oblast odkazovala přibližně pětina zkoumaných zdrojů (21), přičemž bylo definováno 29 v různé míře specifikovaných dopadů. Přičemž téměř všechny tyto dopady mají svůj vztah k případně probíhající implementaci regulace.

Dopady lze kategorizovat do několika hlavních oblastí. Tou první a nejčastěji zmiňovanou je nutnost investic do vzdělávaní a tréninku pracovníků, zaměřených na nastavení správných praktik při zpracování osobních údajů a obecně nakládání s nimi, které jsou předpokladem dodržení regulace. Předpokládaný dopad se v tomto případě neomezuje pouze po čas zavádění normy, ale také je předpokladem udržení stavu compliance po zavedení této regulace. Tento dopad tedy předpokládá kontinuálně probíhajícího školení v oblasti řízení lidských zdrojů. V této souvislosti byla dále zmíněna potřeba zpracování návodů, co se zpracování osobních údajů týče.

Druhým nejčastější dopadem je potřeba kvalifikovaných pracovníků pro oblast soukromí a osobních údajů. V tomto případě se jedná o nové pracovníci síly s požadovanou kvalifikací a kompetencemi, stejně jako vzdělávání již stávajících zaměstnanců (viz první dopad). U získávání nových pracovníků se jedná primárně o profesionály v oblasti ochrany dat a cybersecurity. Zdroje uvádějící tento dopad se váží s obdobím probíhajícího procesu implementace regulace nebo obdobím před jeho zahájení. V této souvislosti byla ještě zmíněna potřeba sestavit interní tým, který se bude implementací zabývat.

Zbývající dílčí zmiňované dopady jsou potřeba komunikovat agendy GDPR napříč organizací, potřeba revize procesů a změny ve zpracování údajů se zaměstnanci, potažmo přenastavení vztahu mezi zaměstnancem a organizací.

4.6.2.5 Řízení rizik

Speciální pozornost je v této práci věnována dopadům implementace GDPR na oblast řízení rizik. Řízení rizik a jeho podprocesy jsou regulací explicitně zmíněny[50]. Kromě toho nařízení definuje přístup založený na riziku při zpracování osobních údajů (EP & EUC, 2016).

Nakonec i 12 zdrojů, které tuto oblast zmiňují, v tomto duchu dopady na RM zmiňuje. Celkem 9 zdrojů proces řízení rizik považuje za nutnou podporu pro implementaci GDPR. V případě již zavedené podnikové metodiky pro řízení rizik se předpokládá, že její prvky budou i přeneseny na oblast implementace nařízení v organizaci. Zmíněna je dále především metodika pro analýzu rizik.

U skupiny organizací bez zavedené metodiky pro řízení rizik se z druhé strany očekává, že některé prvky managementu rizik budou při implementaci využity. V tomto případě ovšem není zmíněna nutnost definování řízení rizik jakožto nového procesu. Při využití metodik pro hodnocení vyspělosti managementu rizik lze tedy tento proces charakterizovat jako neúplný (Chrissis et al., 2013).

Pro obě výše uvedené skupiny je pak předpokládáno rozšíření dosud uvažovaných rizik o rizika související se zpracováním informací a dat, specificky pak související se zpracováním osobních údajů. Další skupinou nově identifikovaných rizik jsou rizika reputační.

[50] Odkaz na aktivity týkající se řízení a minimalizace rizika se najde například v odůvodnění 71,75,76,77 a v článcích 25, odst. 1; 32 nebo 35 a v dalších částech textu nařízení.

4.6.2.6 Další ovlivněné podnikové oblasti

Vzhledem k relativně nižšímu počtu zmínek bude u zbývajících oblasti uveden pouze výčet uvažovaných dopadů na vybrané procesy. Dopady jsou zobrazeny v následující tabulce:

Tabulka 4-14: Dopady GDPR na ostatní podnikové oblasti dle rešerše

Oblast	Formulace dopadu	Upřesnění dopadu	Zdroje
Vývoj a inovace	Negativní vliv na inovace v některých odvětvích	V důsledku omezeného přístupu k datům a externím službám, jež se zabývají zpracováním dat. Explicitně zmíněny oblast vývoje umělé inteligence a internetu věcí.	A35, A41, A05, A40, A34, A40,
	Revize procesu	Změny v přístupu k dílčím praktikám v rámci procesu. U méně vyspělých praktik racionalizace procesu. Změny ve zpracování dat	A02, A05, G09
	Datově podložené inovace	V důsledku implementace a změn přístupu pro zpracování dat a racionalizace praktik	G25
	Zvýšení investic do inovací	V důsledku zvýšení povědomí.	A02
	Tlak na etičnost zpracování údajů		A02
	Dopad na dílčí praktiky		A34
Právo	Adaptace a definice nových zásad pro zpracování		A27, G37, A26
	Alokace dodatečných zdrojů na proces		G01
Řízení bezpečnosti	Revize bezpečnostních zásad		G04
	Zastřešení implementace, nová agenda		A45, A09, A42
	Změna přístupů při zajištění bezpečnosti práce		A03
Řízení dodavatelských řetězců	Revize a racionalizace procesu a praktik. U méně vyspělých procesů jejich racionalizace		G09, G37
	Zabezpečení dodavatelských řetězců v oblasti předávání dat		G03
	Negativní vliv na současné praktiky		G03
Strategické řízení	Integrace oblasti ochrany dat a kyberbezpečnosti do podnikové strategie		A19, G25, G50
	Využití zpřesněných dat pro strategické účely		A27
Účetnictví	Agenda mzdového účetnictví		A15, G24
Management změn	Změna organizační kultury		G38
Audit management	Nový specializovaný proces		G42
Compliance management	Nový specializovaný proces		G42

Zdroj: vlastní zpracování

Z výše uvedených jsou v největší míře definovány dopady na inovační aktivity organizací. Pro tuto oblasti jsou definovány negativní dopady vůči současným praktikám, a to jak v některých dílčích činnostech, tak specificky i v některých, s osobními údaji souvisejících, odvětvích. V tomto ohledu jsou dále definovány nutnost revize stávajícího procesu, zvýšený tlak na etičnost prováděných aktivit a zvýšení investic do tohoto procesu. Naopak možným přínosem implementace je zlepšení inovačních aktivit, které jsou založeny na kvalitnějších datech.

V oblasti práva se jedná primárně o adaptaci na novou regulaci, která předpokládá, že právní procesy slouží k „přeložení" novely v nové politiky a zásady v organizaci. V tomto ohledu je právní oblast uvažována i jako spolupracující na implementaci. Změny v zásadách se týkají se obecného řízení bezpečnosti v organizaci, a to i při zajišťování bezpečnosti práce. V oblasti řízení dodavatelských řetězcům pak byly definovány změny týkající se změn v procesu s ohledem na předávaná data.

4.6.3 Teoretické přístupy k implementaci GDPR

Vzhledem k tomu, že v rámci nařízení není vymezen konkrétní postup a teoretický podklad, na jehož základě má být norma v organizacích implementována, je cílem této výzkumné otázky vymezit doposud známé postupy a přístupy k implementaci GDPR a identifikovat, jaký je pro existující postupy využívaný teoretický rámec.

Z 59 publikací, které se zabývají postupy pro implementaci GDPR, z nichž převážnou část tvoří výstupy šedé literatury (31 publikací), častěji konkretizovaný teoretický základ pro implementaci definují naopak výstupy z akademické literatury. Obecně lze v analyzované literatuře nalézt doporučení týkající se využití odvětvových standardů a frameworků, které zahrnují nejlepší praktiky.

Explicitně jsou za možný základ, na jichž základě jsou i definovány konkrétní postupy pro implementaci GDPR, zmiňovány:

- **Business Process Management**

Řízení podnikových procesů (BPM) zahrnuje, to jak podniky studují, identifikují, mění a monitorují podnikové procesy, jejich modelování a simulaci, aby zajistily jejich efektivní provoz a zároveň tyto procesy v průběhu času zlepšovaly (van Rosing et al., 2014).

Řízení podnikových procesů, jakožto samostatná disciplína, je zmiňováno v publikacích zabývajících se nebo poskytujícími postupy pro implementaci GDPR z několika perspektiv. Náhled na organizaci z pohledu podnikových procesů umožňuje dle analyzovaných publikací mapovat a dokumentovat jednotlivé podnikové aktivity, pracovní postupy a datové toky a porovnat je s požadavky vyplývajícími z nařízení. Business Process Management dále umožňuje upravené praktiky standardizovat a nadále zlepšovat. V této souvislosti je na implementaci GDPR nahlíženo spíše než jako na projekt jako na proces, který je třeba průběžně zlepšovat.

Jako nástroj pro integraci GDPR do podnikových procesů, mapování současných datových toků, analýzy nedostatků v implementaci a nástroj odhalování možných rizik vyplývajících z nedosažené implementace, je vícekrát zmiňováno BPMN[51]. A to především v souvislosti s faktem, že je mapování podnikových procesů (nebo také zpracování záznamů o činnostech zpracování[52]) považováno za jeden z předpokladů implementace GDPR.

Tato grafická notace je v této souvislosti rovněž zmiňována i jako nástroj, který umožňuje prokazovat implementaci GDPR v organizaci a transparentnost ve zpracování osobních údajů. Za limit tohoto nástroje je zmiňována problematika modelování jednotlivých právních požadavků do podnikových procesů.

Druhým zmiňovaným nástrojem je UML[53]. Využití tohoto nástroje je zmiňováno jako úvodní krok pro vývoj automatizovaných metod implementace GDPR. Dále je využití tohoto nástroje zmiňováno jako nástroj pro identifikaci a modelování datových toků.

- **Risk management**

Risk management, jakožto jedna z manažerských oblastí, byl již popsán výše v této práci (kapitoly 3.2, 3.3.3 a 3.4.2), kde byla definována i přímá vazba na obecné nařízení. Kromě principů managementu rizik, které jsou v textu nařízení zakotveny, je tato oblast využívána i jako základ pro postupy vedoucích k implementaci GDPR v organizacích

[51] Business Process Model and Notation (BPMN) je grafická notace (soubor grafických objektů a pravidel, podle nichž jsou mezi sebou spojovány) sloužící k modelování podnikových procesů pomocí procesních diagramů. (Řepa, 2007; International Organization for Standardization [ISO]; 2013)
[52] Činnosti, v jejímž rámci dochází ke zpracování osobních údajů (ÚOOÚ, 2017).
[53] Unified Modeling Language [UML] je grafický jazyk pro vizualizaci, specifikaci, navrhování a dokumentaci programových systémů a procesů. UML podporuje objektově orientovaný přístup k analýze, návrhu a popisu programových systémů (Booch et al., 2005).

nebo je jejich předpokladem. Dle publikovaných výzkumů toto očekávají i samotné organizace.

Využití metod managementu rizik se očekává dle publikovaných příspěvků při posouzení vlivu na ochranu osobních údajů (DPIA), v jehož rámci se očekává, že bude provedena analýza rizik, a to včetně opatření vůči těmto rizikům. Aby byl tento krok úspěšný, je předpokládaný širší přístup k řízení rizik v organizaci.

Ukotvený systém pro řízení je pak předpokladem pro řadu činností během implementace GDPR. Je zmiňován rizikový přístup k mazání dat, je předpokládán management rizik během implementace v rámci cloud computingu, hodnocení dodavatelských rizik, širší podnikové koncepce řízení soukromí (Privacy engineering) nebo systému řízení ochrany dat.

Zmiňován je i standard ISO 31000:2018 Risk management.

- **Standardy ISO 27000**

Řada ISO/IEC 27000 je rodina mezinárodní standardů týkajících se řízení informační bezpečnosti v organizacích (ISO, 2018). V případě analyzovaných publikací se jedná o možný základ pro implementaci GDPR v organizacích.

Nejčastěji jsou v tomto směru zmiňovány standardy ISO 27001 a ISO 27002 vzhledem k tomu, že umožňují organizacím stanovit dostatečné bezpečnostní metriky k ochraně informací, umožňují zapojení nejlepších praktik do procedur. Metriky týkající se bezpečnosti informací, které definuji technická i organizační opatření, jsou předpokladem implementace GDPR, Dle publikovaných příspěvků je dalším společným rysem fakt, že jak GDPR, tak normy ISO uvažují tři aspekty zabezpečení, a to lidi, procesy a technologie, což znamená, že společnosti mohou chránit své podnikání nejen před riziky založenými na technologiích, ale také před dalšími a běžnějšími hrozbami, jako jsou špatně informovaní zaměstnanci nebo neefektivní postupy.

ISO 27001 je zmiňována vzhledem k tomu, že poskytuje dobré praktiky a schémata pro řízení informační bezpečnosti a managementu rizik[54]. Předpokladem aplikace tohoto standardu neustálé zlepšování. ISO 27001 vyžaduje, aby procesy byly neustále

[54] I normy ISO 27000 předpokládají systematický přístup k řízení rizik

aktualizovány, monitorovány a revidovány, což znamená, že se tento systém vyvíjí v souladu s vývojem podnikání. Tento předpoklad je shodný s požadavky GDPR.

Standardy ISO 27000 nemusí být pouhým základem pro postup, předchozí implementace a certifikace těchto norem je po doplněních možné aplikovat i na GDPR. Certifikací ISO lze dle publikací prokazovat implementaci GDPR.

- **Doprovodné metodiky při využití ISO 27000**

Další zmiňovanou metodikou, kterou je vhodné využít pro implementaci GDPR, je standard ISO 9000. ISO 9000 je mezinárodní standard týkající se managementu jakosti. Ten byl v publikovaných implementačních modelech zmíněn v jednom případě, a to ve fázi implementace GDPR jako metodický podklad za souběžného využití výše zmiňovaných standardů ISO 31000 (jako mechanismus pro kompletaci jednotlivých fází implementace) a ISO 27000 jakožto nástroje prokazování shody s nařízením.

Další zmiňovanou metodikou je COBIT vytvořený mezinárodní asociací ISACA pro správu a řízení informatiky (IT Governance). Jedná se o soubor praktik, které by měly umožnit dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik. Opět je doporučováno využití společně se standardem ISO 27001. Využití COBIT 5 je uvažováno pro hodnocení informačních aktiv.

- **Enterprisse Architecture Management**

EAM je strategicky řízená manažerská disciplína, jejímž cílem je podporovat rozvoj a vývoj infrastruktury organizace, která je potřebná k dosažení strategických cílů (Kehrer et al. 2016a; Lagerström et al. 2011; Simon et al. 2014). Důraz je kladen na různé komponenty, které tvoří tuto infrastrukturu, jejich vzájemné vztahy a jejich vztahy k prostředí, odtud pochází pojem organizační nebo podniková architektura.

Jako vhodný základ je tato disciplína jmenována i pro implementaci GDPR, a to vzhledem k tomu, že pokud je podnik vnímán jako systém, lze sledovat vztahy mezi jednotlivými prvky, které jsou relevantní pro řešenou oblast (tj. oblast osobních údajů). Implementace GDPR vyžaduje posouzení klíčových prvků v organizaci (lidé a jejich role, data a procesy). Použitím EAM lze rozšířit tyto interakce na další organizační subjekty (SW aplikace, úložiště, další legislativa).

Další zmiňovaným důvodem pro využití tohoto přístupu je fakt, že vzhledem k holistickému pojetí poskytuje platformu pro zapracování požadavky vyplývajících z plnění požadavků GDPR. Dalším předpokladem vhodnosti je dále zmiňována transparentnost integrace informací v celé organizaci.

Naopak za problematickou sránku tohoto přístupu je fakt, že se jedná o obecný základ, který neumožňuje aplikaci detailních ujednání v rámci GDPR (zmiňována problematika uchovávání dat).

- **ISO 27552**

Tento standard je nový rámec, který je rozšířením ISO/IEC 27001:2013 a řeší DPR a zejména požadavky GDPR. Vzhledem k tomu, že se jedná o nový rámec, je nyní k dispozici pouze jako koncept. Tento standard byl vyvinut v souladu s GDPR

4.6.4 Činnosti implementace GDPR

Má-li být vymezeno současné poznání v oblasti implementace GDPR v případě malých podniků, je cílem této části identifikovat všechny balíky činností i konkrétní aktivity, jež jsou nutné pro splnění požadavků vyplývajících z nařízení, tj. kroků k implementaci GDPR v organizacích.

Ze všech zkoumaných publikací v akademické i šedé literatuře celkem 47 z nich definovalo konkrétní činnosti implementace, a to s ohledem na různé formy výstupů, úroveň podrobnosti návodu na implementace i zaměření publikací dle vybraných podnikatelských oblastí, kde má být GDPR implementováno, případně se navržené postupy týkaly konkrétní části implementace (napři. Posouzení rizik, DPIA, mapových datových toků apod.). Většinu z publikací relevantních pro tuto oblast tvoří zdroje šedé literatury, a to v přibližném poměru 2:1 vůči literatuře pocházející z oblasti akademické (16 publikací v akademické, 31 publikací šedé literatuře). Z uvedených 47 výstupů bylo identifikováno celkem 55 postupů implementace, kdy byl v některých případech ve zkoumaných zdrojích uveden více než jeden možný postup. Zpravidla se jednalo o výstupy rešeršní povahy.

Tabulka 4-15: Činnosti v rámci implementace GDPR (seznam)

Činnost	Popis činnosti, případně dílčí aktivity
Seznámení se a pochopení GDPR	
Zvýšení povědomí o problematice v organizaci	
Posouzení vlivu GDPR na organizaci	Cost/benefit posouzení dopadů, vyhodnocení možných sankcí, sestavení týmu a hodnocení připravenosti na GDPR, určení rozsah dopadů GDPR, rozhodnutí o území, kde budou zpracovávány osobní údaje, analýza trhu
Plán projektu implementace	Jmenované osoby odpovědné za implementaci, vyčlenění týmu pro implementaci, plánování a alokace zdrojů, vytvoření plánu implementace, definice priorit implementace, definice klíčových aktivit, revize plánu, nastavení realistických lhůt na realizace, nastavení auditního systému, řízení organizačního programu, systém hodnocení výkonnosti programu
Management rizik (posouzení rizik zpracování)	Identifikace rizik, analýza rizik, hodnocení rizik, navržení opatření, monitoring rizik, zavedení procesu řízení rizik, vyhodnocení rizik třetích stran
DPIA	Rozhodnutí o realizaci DPIA, identifikace oblastí, které jsou klíčové pro DPIA, posouzení rizik v rámci DPIA, provedení DPIA,
Analýza současného stavu + GAP analýza (obecně)	Revize reportingu a současných kontrolních mechanismů, audit procesů a kontroly, analýza a vyhodnocení současných praktik, analýza současného stavu informační bezpečnosti a implementace GDPR, sestavení současného modelu organizace, GAP analýza, identifikace požadavků, jež je třeba implementovat
Mapování datových toků a zpracování	Mapování informačních aktiv, datových toků a osobních údajů, mapování digitálního dodavatelského řetězce, revize metodiky a rozsahu zpracování osobních údajů, audit dat s ohledem na zpracovávané osobní údaje, identifikace rizik zpracování, posouzení aktiv, analýza sekundárních informačních aktiv, mapování a ochrana datových toků do třetích zemí, analýza ukládání a uchovávání dat
Záznamy o zpracování osobních údajů	Registr zpracování
Definice strategie zpracování dat v organizaci	Definice politik, Identifikace zainteresovaných stran, Propojení dat s procesy, Data protection board, Založte globální agenturu, která se bude zabývat nařízeními a standardy ochrany dat a soukromí, Specifikace datových potřeb a využití, Master data Management
Úniky dat a incidenty	Příprava na úniky dat, identifikace možných úniků, vytvoření postupů pro vyšetření úniků osobních údajů, vytvoření postupů pro reportování autoritám, systém pro upozornění a hlášení o narušení dat, učení se z úniků a jejich vyhodnocování, sanační plány
Zajištění zákonnosti, férovosti a transparentnosti zpracování	Čištění dat a zajištění jejich přesnosti, výmaz dat, identifikace a zabezpečení adekvátních právních základů, spojení právního základu s konkrétním zpracováním, dokumentace, agenda správy souhlasů (evidence souhlasů, demonstrace souhlasů, revize nastavení získávání souhlasů, kontrola a aktualizace zásad, oznámení a souhlasů pro veřejnost, získání souhlasů subjektů, návrh stránek souvisejících se získáváním souhlasů, služby pro sběr souhlasů)
Agenda DPO	Rozhodnutí o jmenování DPO, jmenování DPO
Trénink personálu a školení	Vzdělání a trénink v oblasti hlášení úniků, prevence incidentů, vzdělávání dodavatelů, revize zaměstnaneckých kontraktů, zvýšení dovedností v oblasti ochrany dat
Zajištění principu odpovědnosti	Nastavení zodpovědností, nastavení rolí, úprava přístupů ke sběru dat, vytvoření schémat pro zaznamenávání přístupů
Zajištění práv subjektů	Audity záznamů o přístupech k osobním údajům, zavedení procesu pro zajištění práv subjektů práv, vytvoření nebo změna postupů, audit procesů, posouzení práv subjektů dat, automatizace zpracování požadavků, portál pro žádosti subjektů práv, umožnění přenositelnosti dat, zpracování námitek a stížností vůči zpracování,

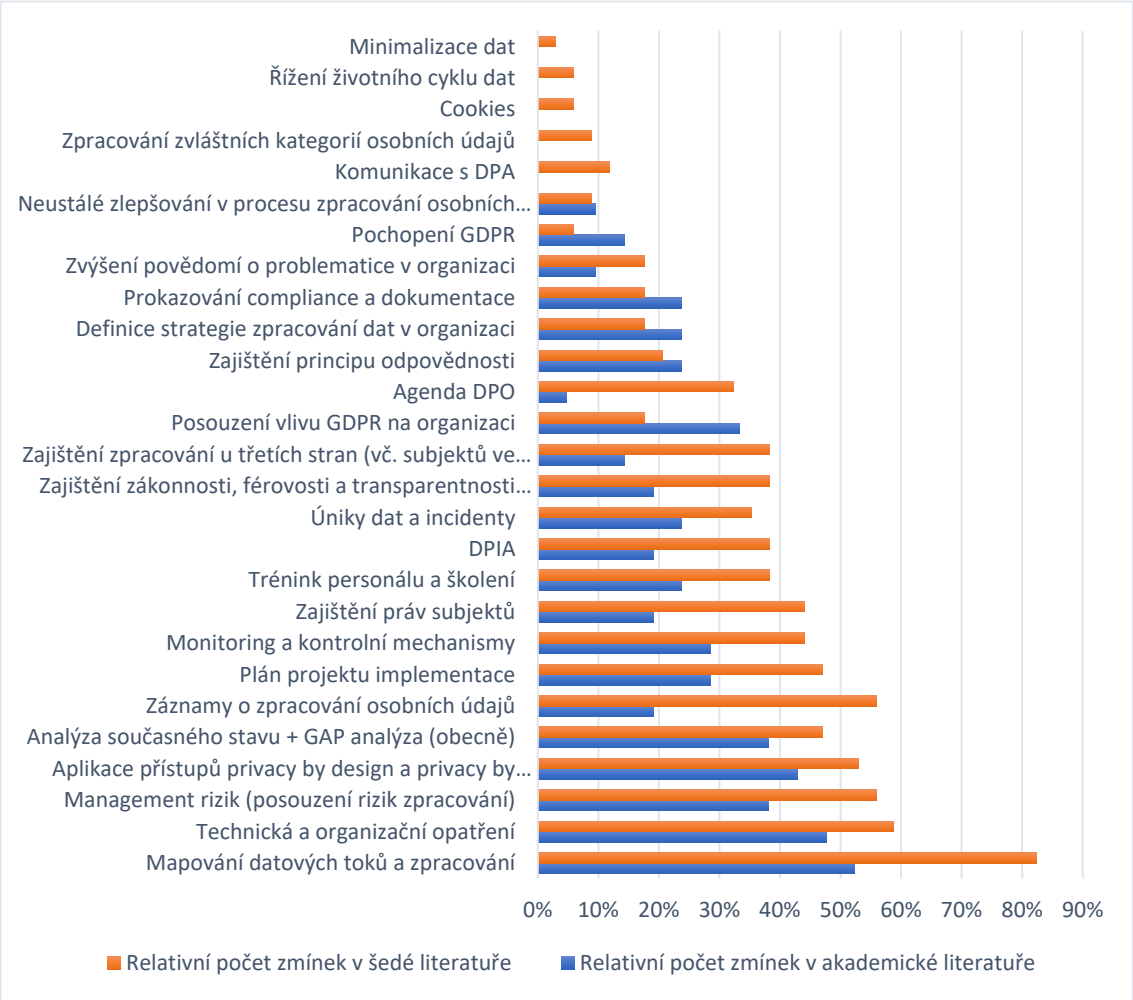
	Aktualizace zásad zpracování, Zajištění práva jednotlivců být zapomenut, průběžná kontrola zajišťování práv uživatelů
Komunikace s DPA	Nalezení příslušného DPA, Kontaktování DPA, Reakce a komunikace s DPA, Zapracování dodatečných požadavků národních autorit
Zajištění zpracování u třetích stran (vč. subjektů ve třetích zemích)	Analýza rizik u dodavatelů, audit poskytovatelů služeb, evidence zpracovatelů, hodnocení řízení ze strany správce a zpracovatele, revize procesu výběru zpracovatele, mapování digitálního dodavatelského řetězce, předávání dat do třetích zemí, zvažování podmínek pro zpracování dat v mezinárodním kontextu, Mapování a ochrana přenosu dat do třetích zemí a přezkoumání postupů
Technická a organizační opatření	Identifikace a zavedení opatření k ochraně osobních údajů (nebo dat obecně), plán pro zavedení opatření, rozhodnutí o opatřeních, Zabezpečení komunikace, Posílení fyzického a environmentálního zabezpečení, revize bezpečnostních přístupů, Dokumentace bezpečnostního programu, šifrování a pseudonymizace, design a návrh podpůrných technologií, změny informačních systémů (v případě potřeby), demonstrace bezpečnostních a organizačních opatření
Monitoring a kontrolní mechanismy	Revize metrik, kontrol a opatření v průběhu času, Tvorba workflow pro neustálý monitoring, Monitoring, Monitoring nejlepších praktik, Monitoring trendů v oblasti bezpečnosti, odvětvových standardů, Monitoring přístupů a procesů, Monitoring a detekce hrozeb, Audit a monitoring, Kontrola účinnosti implementovaných metrik, Definice mechanismů pro identifikace nových rizik v oblasti soukromí, Nastavení systému pro hlášení, Sledování regulačních postojů a aktivit
Neustálé zlepšování v procesu zpracování osobních údajů	Zlepšování a adaptace, Automatizace, Průběžná kontrola
Prokazování compliance a dokumentace	Databáze aplikovaných nařízení a regulací, Evidence a aktualizace, Prokázat efektivitu postupů nakládání s osobními údaji. Distribuovat aktualizované zásady ochrany údajů a oznámení o ochraně osobních údajů,
Aplikace přístupů privacy by design a privacy by default v podnikových procesech	Nový proces zabývající se zpracováním osobních údajů, zavedení nových metrik procesů ve vazbě na ochranu osobních údajů, změny postupů v procesech s ohledem na ochranu osobních údajů a jejich popis, tvorba referenční architektury zajišťování ochrany osobních údajů, Změny v procesech a systémech, implementace upravených procesů a jejich validace, vytvoření obecné infrastruktury pro zajištění soukromí, dokumentace procesů
Zpracování zvláštních kategorií osobních údajů	
Minimalizace dat	
Cookies	
Řízení životního cyklu dat	

Zdroj: vlastní zpracování

Ve výše uvedené tabulce 4-15 bylo v analyzovaných výstupech definováno 23 (+4) balíků činností, které sdružují jednotlivé konkrétní aktivity při implementaci a které byly definovány jako kroky pro implementaci potřebné. Obecně lze tyto skupiny činností rozdělit do dvou kategorií, a to činnosti, které se hledí na implementaci GDPR jako na projekt, a ty činnosti, které se specificky zabývají činnostmi implementace konkrétních požadavků, jež přímo vyplývají z Nařízení. Tato druhá skupina pak výrazně převažuje, co do počtu, tak i počtem publikací, jež danou činnost jako součást

implementace GDPR definují. Z analyzovaných publikací lze dále soudit, že postupy pro implementaci se šedá literatura zabývá častěji jak absolutně (více výstupů zabývajících se implementací), tak relativně, kdy i z počtu relevantních zdrojů jsou konkrétní činnosti častěji definované v literatuře šedé.

Obrázek 4-5: Činnosti implementace (relativní četnost v literatuře)



Zdroj: vlastní zpracování

Z výše uvedeného grafu (Obrázek 4-5) vyplývá, že mezi činnosti implementace GDPR jsou nejčastěji zmiňovány aktivy týkající se mapování datových toků (71 %), jejichž cílem je získání přehledu o zpracovávaných osobních údajů v organizaci (v obecném náhledu pak všech dat). Druhou nejčastěji zmiňovanou aktivitou je posouzení rizik, které se zpracovávaných osobních údajů týkají. Mezi další nejčastější činnosti patří analýza současného stavu (do této fáze by bylo mj. možné zařadit i mapování datových toků) a plán projektu implementace. Zbývající část aktivit se týká zajištění zavedení konkrétních ustanovení v nařízení, přičemž je zjevné, že těmito aktivitami se výrazně častěji zabývá literaturu šedá. Výjimku tvoří obecně méně často definované oblasti,

jako je posouzení vlivu GDPR na organizaci, průběžné prokazování compliance a vedení dokumentace či seznámení se a pochopení regulace.

4.6.5 Specifika implementace GDPR u malých podniků

Smyslem této výzkumné otázky je identifikovat hlavní odlišnosti implemetace GDPR v prostředí malých organizací v porovnání s organizacemi středními a velkými. Odlišnosti mezi těmito oběma skupinami vychází z charakteristik MSP, které byly dříve identifikovány v kapitole 3.1.5. Právě charakteristiky MSP determinují, jako povahu budou mít implementační projekty v této skupině organizací. Tato část je rozdělena na mapování konkrétních bariér implementace v případě MSP, dále specifickým požadavkům na implementaci u této skupiny, specifickým potřebám, které se týkají samotného postupu implementace a nakonec posouzení nákladnosti implementačních projektů u této skupiny organizací.

Specifiky implementace v prostředí malých nebo malých a středních podniků se ze zmapovaných zdrojů věnuje celkem 32 různých publikací při shodném počtu zdrojů akademické i šedé literatury. V tabulce níže jsou tyto výstupy kategorizovány na výstupy rešeršní povahy, expertní názory či návody na implementace a provedenými výzkumy (šetřeními, případovými studiemi či strukturovanými rozhovory).

Tabulka 4-16: Implementace GDPR u MSP (přehled publikací)

	Rešerše	**Expertní názor nebo návod**	**Empirický výsledek**	**Celkem**
Akademická literatura	7	3	6	**16**
Šedá literatura	2	11	3	**16**
Celkem	**9**	**14**	**9**	**32**

Zdroj: vlastní zpracování

Na téma implementace GDPR v MSP bylo nalezeno celkem 9 rešerší (tento typ výstupu převládá u akademické literatury), 14 expertních názorů s výrazným zastoupením výstupů šedé literatury. U 9 výstupů pak byla dílčí specifika podpořena i vlastním empirickým zkoumáním. Takovýchto výstupů bylo identifikováno celkem 9 s převahou zdrojů akademické literatury. V tabulce 4-17 níže jsou uvedeny základní charakteristiky těchto empirických výzkumů.

Tabulka 4-17: Implementace GDPR u MSP (empirické výsledky)

Kód zdroje	Typ zkoumání	Zkoumaný vzorek
A12	dotazníkové šetření	512 různých organizací v ČR
A14	dotazníkové šetření	223 podnikatelských subjektů v ČR
A15	případová studie	malý výrobní podnik v ČR
A24	strukturované interview	nebylo nespecifikováno
A31	strukturované interview	12 respondentů, specialisté v oblasti zajišťování soukromí
A40	strukturované interview	zástupci 15 start-upů (mimo ČR)
G12	dotazníkové šetření	716 zástupců malých firem ve Španělsku
G13	dotazníkové šetření	60 respondentů ze zemí EU (bez ČR)
G43	dotazníkové šetření	specialisté v oblasti zajišťování soukromí z různých odvětví a různé velikosti firem (16% respondentů zástupci podniků s méně než 1000 zaměstnanci)

Zdroj: vlastní zpracování

4.6.5.1 Bariéry implementace u MSP

První částí mapování specifik implementace u malých podniků je identifikace možných bariér pro implementaci GDPR i identifikace potenciálních příležitostí pro tuto skupinu organizací. U identifikovaných zcela převládají existující bariéry, přičemž byla identifikována pouze jedna příležitost u MSP, a totiž vyšší flexibilita této skupiny firem v reakci na nová legislativní opatření.

Nejčastěji zmiňovanou bariérou je obecná bariéra týkající se obecné nedostatečností zdrojů, znalostí a dovednosti. Vzhledem k tomu, že nebylo autory publikací blíže specifikováno, o jakou konkrétní nedostatečnost se jedná, byla tato barréra vymezena takto obecně. U celkem 12 publikací byl bez bližší specifikace uveden tento typ. Druhou nejčastěji zmiňovanou a také již specifičtěji zmiňovanou bariérou implementace GDPR u malých podniků je zmiňována finanční náročnost celého projektu. Část autorů zmiňuje danou bariéru tako jako nedostatek prostředků k financování implementace.

Dalšími často zmiňovanými bariérami je „balík“ do jisté míry spolu souvisejících bariér implementace, kterými jsou nepochopením textu regulace, a to s ohledem na:

- vnímanou vágnost ze strany malých firem,
- nízké povědomí o regulaci v organizaci,
- podcenění rozsahu implementace,
- nedostatek znalostí pro implementaci potřebných požadavků,
- obecné nedostatky odborníků v této oblasti.

Všechny tyto jednotlivé oblasti úzce souvisejí se schopností sestavit a zabezpečit tým (či jednotlivce), který by byl schopný v prostředí organizace implementaci zajistit. Ve dvou případech je jako bariéra implementace definována její časová náročnosti. Pozornost dále byla věnována také možné externí podpoře (především ze strany autorit), která by výše uvedené bariéry mohla do jisté míry kompenzovat. I v tomto případě ovšem MSP vnímají obecný nedostatek, a to buď v absenci možnosti poradenství při implementaci, případně v její pozdnosti (vzhledem k termínu účinnosti). Pomoc ze strany centrálních autorit byla v případě MSP preferována také vzhledem k jejich obecné nedůvěře vůči externím konzultačním či právním službám a jejich nákladnosti. Tato bariéra implementace byla zmíněna ve dvou případech.

Mezi možnými bariérami byla okrajově zmíněna problematika menší schopnosti MSP ovlivnit legislativní proces, a to do takové formy, která by umožnila implementaci těmito organizacemi realizovat.

Všechny výše zmíněné a v tabulce v **Příloze C** zobrazené bariéry mají pro malé a střední podniky celou řadu negativních důsledných efektů:

- **Nechopnost GDPR v organizaci implementovat**

Jako nejvýznamnější důsledek existujících bariér je zmiňována neschopnost GDPR v organizaci implementovat. Publikace upozorňují na nízký stav implementace u této skupiny firem před i po nabytí účinnosti. Zmiňována je připravenost této skupiny mezi 20-30 % z existujících firem (A07, A36, A35). Dle některých dalších průzkumů (např. G13) pak v této skupině firem až 50 % organizací neučinilo žádnou akci vedoucí k implementaci nebo obecně vykazuje malou připravenost (G51). A42 pak uvádí, že mezi touto skupinou firem převládá falešný pocit jistoty a nečinnost a pocit, že je

GDPR implementováno (G13). Možných dalším důsledkem neimplementované regulace jsou potenciální spory s vlastními zaměstnanci (A12).

- **Nákladnost a nedostatky v dílčích aktivitách v rámci implementace**

Především vzhledem k omezeným finančních zdrojům jsou některé aktivity úzce spjaté z implementací GDPR pro tuto skupinu firem považovány za nákladné. Jedná se především o nákladnost jmenovat a mít pověřence na ochranu osobních údajů (G13), revizi současných praktik v oblasti zpracování dat (G13), nákladnost provedení interního školení (G13, A31) či provedení DPIA (G25). Za nedostatečné pak lze jmenovat aktivity týkající se kvality zpracování informací (G47,G04), neschopnost zmapovat vlastní datové toky (A31), neschopnost řešit případné incidenty a úniky dat (G04, G03), chybějící systém pro posuzování rizik (G47), případně systém pro plánování nových technologií (G47). Další skupina důsledků se týká podinvestování jednotlivých přidružených a souvisejících procesů, jako jsou inovace (G35) a bezpečnost (A42).

- **Externí konzultace u komerčních subjektů**

Část negativních důsledků se týká problematiky spolupráce s externími subjekty, kde je zmiňována nedostupnost konzultací pro MSP (G21), a to i vzhledem k nákladnosti na tyto služby, případně jejich vysokou cenu, která se projeví na nákladnosti implementačního projektu (A04, G110, G12, A40). Specifická oblast je pak věnována zranitelnosti této části organizací vůči možným podvodným praktikám ze strany konzultačních firem (A31), které se opět mohou projevit na vysoké ceně za implementaci. I vzhledem k tomuto malé a střední firmy méně často během implementace spolupracují s externími subjekty (SBA1-A10), což se mimo jiné může projevit i na menším úspěchu implementačních snah.

- **Vyšší potřeba konzultací s autoritami (DPA) a zároveň jejich nedostupnost**

Část MSP směřuje vedle komerčních subjektů své snahy také vůči centrálním autoritám v oblasti zpracování dat (v ČR ÚOOÚ) (G13,A40). Zároveň je ovšem zmiňována jejich omezená dostupnost, nebo (v období před účinností) již jen malý efekt z případné konzultace (G08).

- **Zvýšený důraz na technickou stránku implementace**

Jedním z dalších negativních důsledků je v důsledku nižší expertízy této skupiny firem vyšší důraz na pouze softwarová, nikoliv i organizační řešení (A15)

4.6.5.2 Specifika implementace u MSP

Pozornost je v této části věnována specifikům samotných postupů v případě malých a středních firem. V této části budou bodově zmíněna tvrzení zabývající se implementací GDPR v prostředí malých firem:

- Součástí implementace GDPR u MSP není požadováno jmenovat DPO (G40,A05,GL28).
- Není vyžadováno posouzení DPIA, DPIA je pro MSP překážkou implementace (G50, A05).
- Pro implementaci u malých podniků se předpokládá konzultace s externími subjekty (G13).
- Povědomí o GDPR je důležitým prvním krokem implementace GDPR v organizaci (G13).
- Proběhlé implementace zahrnují/uvažují 60 % možných rizikových scénářů (G13)
- Pro implementaci v prostředí malých podniků je běžné široké využití běžných (kancelářských) aplikací, jako jsou Microsoft Word, Microsoft Excel či Microsoft PowerPoint, iCloud, Dropbox, Reddit (G13, G12).
- Případné nedostatky v implementaci mají, co se důvěryhodnosti týče, vyšší negativní dopad na skupinu malých podniků (A05).
- Implementace předpokládá nastavení auditního systému a provedení auditu aktuálních praktik (G07).
- Malé podniky nejsou povinny zpracovávat registr pro zpracování osobních údajů, pokud zpracování není doprovázeno vysokým rizikem (G51). Zároveň ale je registr při implementaci předpokládán (G40,G09,G08). 88 % registr zpracovalo (G43).

Některá dostupná šetření dále vyčíslují náklady potřebné pro implementaci u malých a středních podniků. Výsledky studií jsou znázorněny v tabulce níže:

Tabulka 4-18: Implementace GDPR u MSP (náklady implementace)

Zdroj	**G12**	**A14**	**G43**
Vyčíslené náklady	10 % - žádné náklady 22 % - do 999 Eur 27 % - do 9999 Eur 24 % - do 49999 Eur 10 % do 99 999 Eur 8 % více než 99 999 Eur	v 50 % případů náklady nepřevýšily 10 000 Kč, v 80 % případů náklady nepřevýšily 50 000 Kč	39 % bez investice

Zdroj: vlastní zpracování

4.6.6 Shrnutí výsledků a východiska pro další výzkumná šetření

Hlavním cílem provedené literární rešerše bylo vymezit současné poznání v oblasti implementace GDPR a jejich dopadů na řízení podnikových činností. Vzhledem ke specifičnosti skupiny malých e-shopů a možnému nedostatku dostupné literatury, byla rešerše zaměřena na skupinu malých podniků. Pro zmapování současného poznání pak byly rovnocenně využity zdroje jak akademické, tak komerční. Získané poznatky lze rozdělit do třech základních skupin, a totiž na implementací ovlivněné činnosti a oblasti a dopady na ně, postupy pro implementaci a specifika implementace v prostředí malých podniků.

Dopady implementace na klíčové činnosti a podnikové oblasti

Dle literární rešerše má implementace GDPR svůj dopad až na třináct oblastí činností podniku. Zpravidla se jedná o ty aktivity, v jejichž rámci dochází dle předpokladu ke zpracování osobních údajů. I proto nejčastěji zmiňovanou je oblast řízení dat, informací a znalostí v organizaci a jejich aspektů. Dalšími významně zmiňovanými oblastmi jsou marketing a prodej, řízení lidských zdrojů či řízení rizik. U zbývajících 9 identifikovaných oblastí byla četnost jejich zmínek v literatuře nižší než 10 procent. V rámci následující případové studie budou ovšem tyto činnosti rovněž zkoumány.

Z hlediska konkrétních dopadů bylo identifikováno celkem 309 různých dopadu jak na výše uvedené činnosti, tak také procesní řízení organizace jako celku, kdy nejčastějším dopadem implementace je zmiňována obecná revize procesů v organizaci, jejich integrace s požadavky GDPR, případně jejich racionalizace či standardizace.

Postupy implementace

Literární rešerší byly mapovány i postupy, které se provádějí pro implementaci GDPR v organizaci. Zmapované postupy lze rozdělit na dvě základní skupiny, a totiž ty, které postup implementace definují na podkladu širšího teoretického rámce a ty, které vychází z expertních postojů. Jako teoretický podklad pro definici postupu implementace byly zmiňovány metodiky BPM (**Business Process Management**), řízení rizik a s touto problematikou spojené standardy, Enterprise Architecture Management a dále pakstandardy ISO – 27000 a jeho podskupiny a ISO 27552.

Dle provedené rešerše lze dále kategorizovat **27 činností a oblastí**, jimiž se lze v rámci implementace GDPR zabývat. Platí-li, že způsob implementace vychází z kontextu organizace (Mali, n.d.), nelze těchto 27 činností nutně považovat za povinné. Část z těchto činností se například týkala obecného přístupu k implementaci bez přímé vazby na požadavky nařízení (plánování projektu implementace, zvyšování povědomí o problematice v organizaci apod.). Některé činnosti jsou pak povinné pouze v konkrétním kontextu (například zpracování DPIA, jmenování DPO, agenda zvláštních kategorií osobních údajů, problematika cookies se týká pouze podniků provozujících webové stránky atd.).

V navazující části výzkumu bude ověřeno, nakolik jsou takto vymezené aktivity realizovány během implementace v prostředí malých e-shopů a nakolik jsou tyto aktivity pro tuto skupinu relevantní.

Specifika implementace v prostředí malých podniků

Část zmapovaných zdrojů se věnovala specificky problematice implementace ve skupině malých podniků (dle terminologie zahrnující potenciálně i skupinu podniků středních), kdy byla definována řada možných bariér, které mohou případnou implementaci znemožnit. I v souladu s obecnými charakteristikami této skupiny podniků byly jako nejčastější bariéry implementace definovány **nedostatečné schopnosti** k tomu implementaci provést, **nákladnost implementace**, **omezené možnosti při implementaci konzultovat s externími subjekty** a **omezené technické schopnosti pro implementaci**. V navazující části výzkumu (kapitola 5) je věnována pozornost bližšímu popisu a analýze těchto bariér ve vazbě na kontext skupiny malých e-shopů.

4.6.7 Limity literární rešerše

Navzdory rozsahu provedené literární rešerše má provedené šetření několik limitů, které vycházejí převážně z kritérií pro výběr relevantních publikací, kdy bylo pro každý typ literatury (akademické a šedé) omezeno vždy pouze na jednu databázi (Web of Knowledge a Vyhledávač Google). Ačkoliv pouze okrajově byly využity další databáze vědeckých publikací (Scopus, Google Scholar apod.), vzhledem k počtu publikací v databázi Web of Science a rozsahu hledání by měly nalezené zdroje dostatečně mapovat současné poznání. Stejně tak pro hledání šedé literatury byl zvolen pouze Vyhledávač Google, kdy možné nedostatky této databáze byly kompenzovány

rozsahem hledání. Obecným limitem šetření pak je fakt, že byly zkoumány pouze zdroje, které byly v čase hledání zveřejněné. K tomuto datu je provedená rešerše aktuální.

Druhým omezením rešerše je její omezení na hledání dopadů GDPR na podnikové činnosti a oblasti v literatuře dostupné on-line, a to pro podniky obecně bez ohledu na jejich možné klíčové charakteristiky (odvětví, počet zaměstnanců, rozsah a kontext zpracování OÚ apod.). Sledovány dále nebyly další charakteristiky identifikovaných dopadů (například finanční nebo časové hledisko dopadů apod.).

Další část výzkumu je proto designována s cílem ověřit, nakolik jsou poznatky relevantní specificky pro skupinu malých e-shopů působících v České republice.

5 Implementace GDPR v prostředí malého e-shopu

Druhým definovaným dílčím cílem disertační práce je **popsání a ověření možných přístupů vedoucích k implementaci GDPR v malých e-shopech s uvážením kritických faktorů**. Tento cíl kombinuje jak úkoly teoretické, tak i empirické.

Na základě definovaného cíle této části práce je níže v tabulce 5-1 nejprve definovaná výzkumná otázka, která je následně dekomponovaná ve specifické výzkumné otázky.

Tabulka 5-1: Výzkumné a specifické výzkumné otázky (cíl 2)

Dílčí cíl 2:
Popsat a ověřit možné přístupy vedoucí k implementaci GDPR v malých e-shopech s uvážením kritických faktorů.
Výzkumná otázka 2:
Jaké přístupy vedou k implementaci GDPR v prostředí malého e-shopu? (VO2)
Specifické výzkumné otázky:
Jak malé e-shopy prezentují problematiku zajišťování soukromí vůči zákazníkovi? (SVO2.1.)
Jak malé e-shopy implementují GDPR? (SVO2.2)
Jaké kritické faktory ovlivňují přístup k implementaci GDPR v prostředí malého e-shopu? (SVO2.3)
Jaké jsou důsledky implementace GDPR na klíčové činnosti malého e-shopu[55]? (SVO2.4)

Zdroj: vlastní zpracování

Definovanou výzkumnou otázkou v této části je: „*Jaké přístupy vedou k implementaci GDPR v prostředí malého e-shopu*?“, k jejímuž dostatečnému zodpovězení byly rovněž definovány otázky specifické. Zodpovězení výše definovaných otázek bude vycházet z poznatků získaných dříve provedenou rešerší a také empirickými poznatky, které budou získány v rámci provedené vícenásobné případové studie. Design studie je představen v následujícím textu.

5.1 Metodika vícenásobné případové studie

Pro bližší zkoumání implementace GDPR v podniku bude provedena vícenásobná případová studie. Případové studie jsou dle Yina (2014) doporučovány v případech, kdy nejsou jednoznačně vymezeny hranice mezi zkoumaným fenoménem (GDPR a jeho implementace a problematika zajišťování soukromí) a kontextem reálného prostředí (podnikání na internetu, realita malých a středních podnikatelských subjektů).

[55] Zkoumány budou ty činnosti, jež byly shodně identifikovány u skupiny e-shopů (kapitola 3.1.5) a lze vůči nim identifikovat dopad v důsledku implementace GDPR (kapitola 4.6.1).

Spolehlivost případové studie je pak zvýšena v případě sestavení vícenásobné případové studie (Yin, 2014).

Vícenásobná případová studie bude provedena na základě doporučeného postupu, kdy sledované subjekty budou zkoumány krátkodobě. Zároveň se jedná o vloženou vícenásobnou studii, kdy je každá organizace zkoumána zvlášť (Yin, 2014). V kontextu s cílem šetření se jedná o výzkum deskriptivní (Eger & Egerová, 2014).

5.2 Výběr subjektů, kritéria výběru

Výběr subjektů vhodných pro případovou studii byl proveden dle doporučení (Yin, 2014), seznam kritérií byl sestaven tak, aby bylo možné zodpovědět výzkumné otázky.

Podmínkou pro zařazení e-shop je splnění následujících kritérií:

- Subjekt odpovídá kritériím dle definice malého e-shopu uvedené v kapitole 3.1.6.
- Subjekt implementoval Nařízení GDPR.
- Subjekt a účastníci výzkumu souhlasí s poskytováním informací.

Zástupci subjektů, kteří odpovídaly zadaným kritériím, byli následně osloveni s cílem získání dodatečných informací. Vícenásobná studie byla provedena **na příkladu 3 vybraných subjektů**.

5.3 Výzkumné metody

K zodpovězení výzkumných otázek byla dle doporučení využita jak kvalitativní, tak kvantitativní data. Dle Woodside (2010) či Yin (2014) použití více metod ve výzkumu případových studií přispívá ke zvýšení přesnosti a komplexnosti studie. Sběr dat je vzhledem k tomu, že se jedná o studii pilotní, rozsáhlejší v porovnání se zamýšlenou vícenásobnou studií (Yin, 2014). S ohledem na definované výzkumné otázky jsou následně využity tyto výzkumné metody:

Zúčastněné pozorování a pozorování

V případě případové studie provedené ve společnosti Dům a zahrada Ježek s.r.o. bude využita metoda takzvaného zúčastněného pozorování (Eger & Egerová, 2014; Hendl, 2005), kterou bylo možné aplikovat vzhledem k faktu, že autor textu byl zároveň zaměstnancem sledovaného subjektu.

I protože tuto metodu nelze využít v externím prostředí (firem, kde autor textu nepracuje), design vícenásobné studie zároveň předpokládá nahrazení zúčastněného pozorování pozorováním prostým, konkrétně strukturované pozorování z pozice úplného

pozorovatele. Dle Hendla (2005) je výhodou tohoto pozorování, že není ovlivněno chování sledované skupiny.

Yin (2014) tuto metodu řadí mezi šest možných zdrojů důkazů případové studie. Tato metoda může být hlavní metodou výzkumného šetření, pokud se jedná o výzkum deskriptivní (Hendl, 2005). S ohledem na definované specifické otázky bude tato metoda využita k analýze webové prezentace či profilů na sociálních sítích vybraných subjektů a bude aplikována na všechny výzkumné otázky, a to především za účelem hlubšího pochopení kontextu organizace.

Stejnou metodu zisku informací při realizaci případové studie v prostředí organizací aplikovali například Mahura & Birollo (2021) nebo Fernandes et al. (2021).

Dokumentace a záznamy

Analýza dostupné dokumentace je relevantní zdroj informací každé případové studie (Yin, 2014; Woodside, 2010). Analyzovány budou jak dokumenty dostupné on-line, tak poskytnuté interní dokumenty organizace. Využití této metody je tedy částečně podmíněno i přístupností požadovaných údajů. S ohledem na výzkumnou oblast se jedná o návody a záznamy týkající se zpracování osobních údajů, stejně jako dokumentaci vytvořenou během samotného procesu zkoumání. Analyzované dokumenty dále slouží jako podklad pro vedení následných rozhovorů.

Nestrukturovaný rozhovor

Dle Eger & Egerová (2014) umožňuje rozhovor zachytit nejenom data, ale i hlouběji proniknout do motivů respondentů. Součástí sběru dat k případové studii je neformální rozhovor s otevřenými otázkami. Smyslem těchto rozhovorů je konfrontovat získané poznatky se zkušenostmi a postoji zástupců organizace za účelem komplexního náhledu na dílčí aspekty případové studie.

Strukturovaný rozhovor

Alternativou vůči rozhovoru nestrukturovanému je rozhovor strukturovaný (Eger & Egerová, 2014). Ten dle Hendla (2005) sestává z řady předem formulovaných otázek. Nevýhodou tohoto přístupu je nižší pružnost. Naopak výhodou je fakt, že se redukuje pravděpodobnost, že se data získaná v jednotlivých případových studiích budou výrazně lišit. Poznatky z případových studií tak bude možné tímto přístupem účelně srovnávat. Zároveň je tento případ vhodný, pokud neexistuje možnost rozhovor

opakovat a existuje relativně malý časový prostor pro práci s respondentem. To může být i příklad níže uvedených případových studií (Hendl, 2005).

Dle povahy výzkumu i potenciálních respondentů může být dále využita i metoda polostrukturovaného rozhovoru s předem danými okruhy otázek (Eger & Egerová, 2014; Hendl, 2005).

5.4 Crystalis s.r.o.

Společnost Crystalis s.r.o. byla založena roku 1993. Firma se zabývá zásobováním právnických osob, podnikajících fyzických osob i fyzických osob pramenitou vodou. Do portfolia produktů se řadí výdejníky na barelovou vodu, výdejníky s připojením na vodovodní řad a nakonec samotná barelová voda. V případě barelové vody je společnost v pozici výrobce, firma vlastní svůj vlastní pramen v kraji Vysočina.

Dle výsledků hospodaření z roku 2020 činil obrat společnosti 35,8 mil. Kč, kdy většinu z těchto tržeb tvořil prodej vlastních výrobků a služeb. Dle údajů z roku 2019 činil průměrný přepočtený počet zaměstnanců 36 lidí. Dle kategorizace Evropské komise (2019a) tak společnost spadá do kategorie malých podniků. Z hlediska struktury je až 90 % veškerého obratu v České republice tvořeno zákazníky v síti B2B, kdy blíže nespecifikovanou podstatnou část z této skupiny zákazníků tvoří podnikající fyzické osoby, zbývající část pak tvoří podnikající právnické osoby. Zbývající přibližné 10 % obratu tvoří zákazníci v kategorii B2C. Vzhledem k tomu, že v rámci podnikání společnosti dochází ke zpracování osobních údajů, vztahuje se na společnost povinnost GDPR implementovat.

Z hlediska prodejních kanálů je 50 % objednávek tvořeno telefonicky, a to jak formou přímého prodeje, tak příjmem zakázek na telefonní lince. 20 % objednávek probíhá na základě e-mailové komunikace, opět současně aktivní i pasivní formou. 3 % objednávek je tvořeno příjmem skrz webové stránky organizace – e-shopem či komunikační okno, tzv. webchat. Zbývající část přibližně 17 % objednávek tvoří nasmlouvané pravidelné závozy k zákazníkům.

5.4.1 Průběh implementace v organizaci

Implementace GDPR ve společnosti Crystalis je popsána na základě vícero důkazů, kdy nejprve bylo provedeno pozorování a zúčastněné pozorování na e-shopových stránkách organizace (test funkcionalit webových stránek), byla provedena analýza dokumentace

prezentované na webových stránkách (stránky související s problematikou zpracování osobních údajů). Získané poznatky z této fáze byly následně i s ohledem na definovaný cíl šetření konfrontovány se zástupci organizace při polotrukturovaném telefonickém rozhovoru. Konkrétně s jednatelem společnosti a manažerem marketingu, který byl za implementaci GDPR zodpovědný.

Dle rozhovoru došlo k implementaci na jaře roku 2018, to je před nabytím účinnosti regulace GDPR. Obecně se organizace zpracováním osobních údajů věnuje v mezích zákonných povinností. Z pohledu konkrétních kroků implementace došlo nejprve ze strany zodpovědné osoby k studiu základních informací o regulaci, které se opíralo o informace volně dostupné na internetu, především pak na stránkách komerčních subjektů. Respondent poukazuje na nedostatek podkladů pro implementaci ze strany veřejných subjektů. Na základě vlastní rešerše zodpovědné osoby byly definovány konkrétní kroky implementace, kdy v rámci dalšího postupu byl osloven externí právník, který zpracoval aktualizované obchodní podmínky společnosti tak, aby byly v souladu s požadavky vyplývajícími z GDPR.

V dalším kroku pak externí administrátor stránek provedl nezbytné úpravy webových stránek e-shopu tak, aby rovněž odpovídaly proklamovaným zásadám zpracování osobních údajů[56]. Posledním krokem implementace GDPR bylo školení personálu k dodržení správných zásad zpracování osobních údajů (více o této problematice v následující podkapitole).

Implementace byla dle obou respondentů zcela dokončena před nabytím účinnosti nové regulace. Společností kalkulované celkové náklady na implementaci se pohybují v řádu nižších desítek tisíc Kč složené na jedné straně z pracovních nákladů vyplývajících z časové náročnosti na straně zodpovědné osoby a na druhé straně náklady na externí služby (aktualizace obchodních podmínek a úpravy na webových stránkách).

Respondent zodpovědný za implementaci byl dále dotazován na bariéry, se kterými se společnost v průběhu implementace potýkala. První proklamovanou bariérou je již výše zmíněná nedostupnost veřejně dostupných informací, na základě kterých by mohla jednoznačně společnost během implementace postupovat. S čímž souvisí i

[56] Ke stejnému kroku pak došlo v druhé polovině roku 2021 v souladu s nabytím účinnosti regulace, jež se vztahuje specificky na oblasti elektronického podnikání.

finanční nákladnost implementace, kdy k provedení nutných kroků implementace bylo zapotřebí externích komerčních služeb.

Za druhou bariéru pak respondent považuje nepřiměřenou nákladnost jednotlivých činností a také negativně orientovaný marketing konzultačních společností.

5.4.2 Dopady na činnosti

- Řízení dat a informací

V oblasti zpracování dat došlo ke změnám především ve zpracování zákaznických údajů. Byly nastaveny přístupy zaměstnanců do jednotlivých databází. Každý zaměstnanec, který má přístup k osobním údajům zaměstnanců, byl zároveň řádně proškolen. Školením nastavené praktiky pak byly stvrzeny podpisy jednotlivých zaměstnanců.

Další významnou změnou v oblasti řízení dat byly provedené úpravy na webových stránkách, kdy byla nastavena takzvaná cookies lišta a bylo provedeno další nastavení, aby byla zajištěna zákonnost zpracování.

- Marketing a prodej

Dle analýzy dokumentů i rozhovorů se zástupci společnosti se firma ve velké míře opírá o přímý marketing, který je jedním z hlavních nástrojů pro zisk nových objednávek.

V souvislosti s účinností GDPR došlo především v této oblasti k několika změnám, kdy byla provedena opatření především v oblasti předchozího zajištění souhlasu se zpracováním osobních údajů. V případě telefonického navolávání potenciálních zákazníků se společnost opírá o nakoupenou databázi firem a podnikajících fyzických osob. Dle proklamací dodavatele této databáze byl zajištěn předchozí souhlas s poskytnutím osobních údajů subjektů údajů třetím stranám k účelu přímého marketingu. Dle vyjádření zástupce společnosti ovšem neměla firma možnost si tuto skutečnost ověřit. Investice do databáze kontaktů se pohybovala v řádu nižších desítek tisíc korun. Každý zaměstnanec, který má do této databáze přístup, byl zároveň proškolen o zásadách o zpracování. O tomto školení je dostupný záznam.

Druhou oblastí marketingu je rozesílka obchodních sdělení. Právním základem pro toto zpracování je udáván oprávněný zájem (uvedeno rovněž v Obchodních podmínkách). Zároveň u obou zmíněných kanálů dochází k pasivnímu příjmu, kdy iniciátorem komunikace je subjekt údajů. V tomto případě se jedná opět o zpracování na základě oprávněného zájmu.

V rámci webových stránek došlo k jejich úpravě tak, aby odpovídaly právním normám. V této souvislosti došlo k úpravě tzv. cookies lišty, která umožňuje nastavení záznamu o chování uživatele webových stránek. Toto nastavení proběhlo v souvislosti s platností regulace o elektronické komerci.

V souvislosti s regulací GDPR (a regulaci o elektronické komerci) dále manažer marketingu zmiňuje snížení výkonnosti některých kanálů v oblasti personalizované propagace (ÚOOU, 2021b). Poukazuje především na horší výsledky reklamních kampaní, které se opírají o osobní údaje uživatelů. V tomto důsledku vzhledem k nerentabilitě společnost omezila svou činnost v oblasti e-mailového marketingu a propagaci na sociálních sítích.

- Řízení rizik

Náhledem na management rizik z pohledu vyspělosti lze tento proces v organizaci charakterizovat nejnižším stupněm, kdy není předem definován přístup k vyhodnocování rizik. Rizika jsou organizací vyhodnocována, nicméně žádnou standardizovanou formou.

Vzhledem k odvětví, ve kterém společnost působí, je pozornost věnována regulatorním rizikům. V tomto ohledu společnost přistupovala k implementaci GDPR, kdy si firma byla vědoma především rizika možného postihu a negativního vlivu na reputaci organizace především před jejími dlouhodobými zákazníky i dodavateli.

V rozporu s některými výzkumnými předpoklady nevedla doposud implementace GDPR k přehodnocení přístupu v řízení rizik, nedošlo k adopci systému řízení rizik

- Řízení lidských zdrojů

Vzhledem k tomu, že se jedná o obchodní společnost, je příjem a vyřizování zákaznických objednávek jednou z klíčových činností organizace. V souvislosti s agendou zpracování osobních údajů byl každý ze zaměstnanců, jenž má přístup k osobním údajům zákazníků, proškolen k zásadám o správném zpracování osobních údajů. To se v rámci společnosti týká jak pracovníků na objednávkovém oddělení, tak zaměstnanců, kteří zásilky zaváží.

- Právo & Compliance management

Dle vyjádření marketingového manažera je plnění zákonných a právních povinností pro společnost jednou z priorit. Na druhé straně se s ohledem na velikost společnosti nejedná o činnost, které by bylo dedikováno vlastní oddělení. Dopady na tuto činnost tak

lze charakterizovat coby krátkodobé, a to v podobě dodatečných nákladů na právní služby, a to konkrétně zpracování nových obchodních podmínek. Implementace GDPR neměla důsledné dlouhodobé dopady na činnosti v oblasti práva. Aktivity směřující k plnění všech zákonných požadavků jsou prováděny rovněž bez dlouhodobých úprav.

Další analyzované činnosti e-shopu:

- Vývoj a inovace – bez zjevného dopadu
- Strategické řízení – bez zjevného dopadu
- Řízení dodavatelských řetězců – bez zjevného dopadu
- Účetnictví – bez zjevného dopadu

5.5 Dům a zahrada Ježek s.r.o.

Dům a zahrada Ježek, s.r.o působí na českém trhu od léta 2017. Společnost se sídlem v Ledcích u Plzně se zaměřuje především na prodej zahradního vybavení. Dle klasifikace dle Kunešové (2017) se jedná o kvazielektronický obchod. Aktuálně společnost kromě České republiky působí rovněž na Slovensku (od roku 2021) a v Maďarsku (od 2022).

Dle výsledků hospodaření společnosti za rok 2021 dosahuje obrat společnosti 61 milionů Kč bez DPH, který tvoří primárně tržby z prodeje zboží. Částečně se na obratu podílí i prodej služeb. Dle interních údajů organizace je přibližně 93 % obchodů sjednáváno prostřednictvím objednávek na webových stránkách, 5 % pak fyzickým prodejem na pobočce v Plzni. Minoritně jsou pak obchody sjednávány prostřednictvím e-mailové či telefonické komunikace, využitím webchatu, případně na základě komunikace na sociálních sítích, kde organizace spravuje své profily na platformách Facebook, Instagram a LinkedIn. Společnost se orientuje na prodej v segmentu B2C. I vzhledem k této obchodní orientaci se na společnost vztahuje povinnost splňovat požadavky vyplývající z Nařízení na ochranu osobních údajů.

K začátku září 2022 organizace zaměstnává 8 pracovníků na hlavní pracovní poměr. Dle charakteristik podle obratu či počtu zaměstnanců se jedná o malý podnik.

5.5.1 Průběh implementace v organizaci

Případová studie z prostředí organizace je popisována na základě vícero důkazů, na jejíchž sestavení se podílí autor[57] a dva interní respondenti, konkrétně jednatel společnosti (respondent A) a provozní manažer (respondent B). Se zástupci společnostmi

[57] V době sestavování případové studie autor této práce se společností aktivně spolupracuje.

byly, co se týče problematiky implementace GDPR, vedeny opakované nestrukturované rozhovory. Dále jako podklad pro sestavení studie slouží analýza interní dokumentace a webových stránek.

Úkony nutné k implementaci GDPR ve společnosti byly zahájeny na jaře roku 2018 před nabytím účinnosti nové regulace. Po úvodní analýze ze strany jednatele byl implementací pověřen autor tohoto textu.

Základním informačním zdrojem pro postup implementace byly veřejně dostupné zdroje a na tomto podkladě byly naplánovány dílčí kroky. Vzhledem k možné nákladnosti probíhala implementace bez konzultace s externími odborníky.

Prvním a zásadním krokem byla zevrubná analýza organizace, a to z pohledu struktury a návaznosti jednotlivých dat, kdy byly fakticky zmapovány všechny datové toky a jejich úložiště. Z perspektivy vybrané organizace se toto mapování aktivně týkalo primárně fyzické dokumentace organizace a základního mapování toků v rámci vlastních informačních systémů. Ačkoliv bylo mapování datových toků organizací provedeno, není o tomto dostupný žádný záznam, a to vzhledem k tomu, že v době implementace neměla organizace k dispozici žádný podklad, na jehož základě by bylo možné formální dokument, který by odpovídal právním nárokům, sestavit.

Další krokem implementace byla i s ohledem na obecná doporučení analýza rizik, návrh opatření a jejich provedení. Organizace pro tyto kroky nevyužila žádnou dostupnou metodiku analýzy rizik, soustředila se pouze na realizaci opatření vůči možným rizikům byla organizačního charakteru, a to úpravou přístupových práv, decentralizací přístupových hesel a bezpečnému uložení a zálohování fyzické dokumentace s fyzickým omezením přístupu. Z hlediska technologických opatření u využívaných aplikací byla jejich realizace ponechána na dodavatelích těchto služeb, kdy společnost nedisponovala potřebnými dovednosti opatření provést.

Vlastní reálné úpravy při zpracování pak fakticky dle zkušenosti autora provedli všichni dodavatelé externích služeb. Dle provozního manažera provedly vlastní opatření jak dodavatelé aplikace v rámci zasílání e-mailingu, tak i jednotliví poskytovatelé sociálních sítí. V souvislosti s tímto došlo následně i k podpisu nových zpracovatelských smluv, jež vyhovění GDPR předpokládaly.

Následným krokem implementace GDPR ve společnosti byly v závěru provedeny nutné úpravy webových stránek pro odpovídající zajišťování souhlasů se zpracováním k marketingovým účelům a byly přidány Podmínky zpracování osobních údajů (Dům a zahrada Ježek, s.r.o., 2018), které byly sestaveny dle předlohy poskytované APEK. Tyto podmínky byly dále upraveny na jaře 2022 v souladu s novou evropskou regulací (ÚOOU, 2021b).

Posledním krokem implementace bylo zajištění udržitelnosti nových procesů a dodržování nových požadavků (Gabriela et al., 2018). V tomto ohledu byl tento stav v organizaci zajištěn pouze po neformální stránce. Organizace nezpracovala žádnou dokumentaci, jež by toto zajištění prokázala. Monitoring možných nových rizik pak probíhá pouze ad hoc, stejně jako případná opatření.

V době implementace neproběhlo ani žádné interní školení zaměstnanců, společnost v roce 2018 sestávala ze tří stálých pracovníků a tří externích spolupracovníků, s nimiž byly podepsány zpracovatelské smlouvy, pokud někteří takto spolupracující pracovníci byli ve styku s osobními údaji zákazníků.

Dle zkušeností z vybraného subjektu lze jednoznačně na vybraném případu potvrdit již dříve identifikované bariéry, které úspěšnosti implementace v kontextu organizace bránily. Rozsah celého implementačního projektu a jeho následného udržení se odvíjely od prioritizace daného tématu v organizaci, znalostí v oblasti řízení osobních údajů a množství finančních prostředků. V době implementace neexistoval dle zástupců organizace (včetně autora) žádný veřejný zdroj informací k tomu, jak z praktického hlediska GDPR „krok za krokem“ implementovat. Vzhledem k omezenosti finančních zdrojů (organizace v době implementace působila na trhu méně než jeden rok) ani nebylo možné zajištění implementace externí cestou – ani externím školením ani implementací externím subjektem. V tomto ohledu tedy organizace spoléhala na implementaci na základě dostupných zdrojů a informací. I proto byla implementace provedena těsně před nabytím účinnosti regulace (e-mail s výzvou o opětovné získání souhlasů pak dokonce několik měsíců po nabytí účinnosti).

Kromě implementace v České republice bylo dále nutné požadavky, které vyplývají z regulace, zapracovat i v případě Slovenska a Maďarska. V obou těchto zemích jsou aplikovány přístupy ke zpracování stejné jako v případě České republiky. Za dodatečné aktivity v rámci implementace lze považovat přeložení podmínek zpracování do cizího

jazyka. Z hlediska nákladů v tomto případě probíhá další implementace jen s minimálními dodatečnými náklady. Respondent A v tomto ohledu zmiňuje zjednodušení vstupu podniku na další zahraniční trhy z perspektivy adaptace na místní právní prostředí, kdy se jinak dle respondenta některé další legislativní požadavky v oblasti elektronického podnikání liší.

5.5.2 Dopad na činnosti

- Řízení dat a informací

V oblasti řízení dat došlo i v souvislosti s účinností GDPR k celé řadě změn technického i organizačního charakteru. Již zmiňovanou oblastí je změna politiky v oblasti bezpečnosti dat, kdy došlo jednak ke změnám především v oblasti přístupových práv, dáletaké v oblasti zabezpečení exportů dat, které jsou zasílány třetím stranám (aplikacím).

Další změnou v přímé návaznosti na agendu zpracování osobních údajů je zpracování zákaznických dat, která jsou před analýzou zcela a jednostranně anonymizována. Dále je tato oblast negativně ovlivněna sníženou kvalitou v poskytováním analytických dat ze strany používaných aplikací (například Google Analytics).

Technické změny ve zpracování jsou realizovány především poskytovateli služeb (aplikací). Ačkoliv se projevují na aktivitách ve společnosti, společnost sama na ně nemá přímý vliv.

- Marketing a prodej

Výrazně ovlivněnou oblastí je marketing organizace, kdy došlo k celé řadě změn a omezení. Ty fakticky kopírují změny v procesech uvedené v případě předchozí případové studie. Dle provozního manažera se omezení nejvýrazněji dotkla e-mailingových kampaní, kdy došlo k restrikcím na straně poskytovatele aplikace, což se projevilo na ztížení pravidelné rozesílky.

Další ovlivněnou oblastí je oblast výkonnostního marketingu, kde došlo (ale až v návaznosti na směrnici z roku 2022) k výraznému snížení kvality poskytovaných dat ze strany on-line reklamních služeb. I v této souvislosti tak došlo k přehodnocení marketingové strategie organizace.

- Řízení rizik

V oblasti řízení rizik nedošlo k výrazným změnám. Vyspělost organizace v oblasti řízení rizik lze i nadále charakterizovat nejnižším, „iniciačním“ stupněm vyspělosti, kdy k vyhodnocování rizik dochází ad hoc způsobem, na kterém se primárně podílí seniorní manažerský tým. Nicméně je v oblasti rizik pokládán větší důraz na možná regulatorní rizika, a to nejen v oblasti zpracování dat.

- Řízení lidských zdrojů

Minimálními změnami prochází agenda lidských zdrojů, a to i s ohledem na nízký počet zaměstnanců. Ta je zajišťována jediným pracovníkem. Přístupová práva týkající se informací o zaměstnancích byla nastavena již před implementací GDPR. Přístup k údajům má kromě pověřeného zaměstnace také jednatel a externí účetní (pro potřeby mzdového účetnictví).

- Právo & compliance management

Tuto agendu spravuje jednatel společnosti samostatně. Záležitosti týkající se právní agendy jsou zpravidla řešeny ad hoc externími službami. Ve vztahu k implementace GDPR nejsou sledovány žádné změny v této činnosti – externí služby nebyly v rámci implementace GDPR poptávány.

Další analyzované činnosti e-shopu:

- Vývoj a inovace – činnost podniku v této oblasti je zcela minimální bez výrazné inovace procesní či produktové a bez zjevného dopadu GDPR
- Strategické řízení – bez zjevného dopadu
- Řízení dodavatelských řetězců – bez zjevného dopadu, případné úpravy podmínek se týkají dodavatelů externích služeb
- Účetnictví – bez zjevného dopadu

5.6 Firma A

Následující případová studie se zabývá společností, jejíž zástupci si přejí, aby název společnosti zůstal v anonymitě. Pro potřeby této práce bude společnost uváděna pod smyšleným název „Firma A“.

Sledovaná společnost byla založena roku 2013 a zabývá se prodejem zboží a s tím souvisejících služeb v odvětví stavebnictví. Obrat společnosti v roce 2020 činil 130 mil. Kč, z toho přibližně 60 % tvoří tržby za prodej zboží, zbývajících 40 % pak prodej vlastních výrobků a služeb. Prodej zboží společnost realizuje primárně prostřednictvím e-shopu, zatímco prodej služeb je realizován primárně prostřednictvím obchodních zástupců. Společnost vedle e-shopu realizuje prodej i na čtyřech pobočkách v České republice a jedné na Slovensku. Na Slovensku rovněž probíhá prodej přes internetový obchod. Společnost obsluhuje zákazníky v segmentech B2B, B2C i B2G s převažující skupinou B2C. V současnosti společnost zaměstnává 35 zaměstnanců, řadí se tedy do kategorie malých podniků.

5.6.1 Implementace GDPR v organizaci

Případová studie je zpracována na základě kombinace několika zjištění. Hlavním zdrojem informací jsou provedený nestrukturovaný a následně i strukturovaný rozhovor s marketingovým manažerem společnosti. Druhým zdrojem informací je provedené pozorování, kdy byly ověřeny poskytnuté informace na základě analýzy webových stránek e-shopu společnosti.

Dle rozhovoru se zástupcem organizace byly kroky vedoucí k implementaci GDPR zahájeny s předstihem (před nabytím účinnosti) na konci roku 2017. Implementací byl vedením společnosti pověřen marketingový manažer (respondent rozhovoru), který byl rovněž jedinou osobou, která se v organizaci na implementaci podílela. Dle vyjádření respondenta byl obecný zájem o implementaci ve společnosti mizivý.

V úvodních fázích došlo ke studiu problematiky, a to na základě volně dostupných materiálů na internetu (videa s odborníky na právo v e-commerce, články týkající se GDPR apod.). Dle vyjádření respondenta nebyly dostupné ucelené informace o implementaci a bylo nutné využít vícero zdrojů pro pochopení problematiky. Zároveň se jevil výklad zákona respondentovi, jakožto právnímu laikovi, zmatečný a nejednoznačný.

Podstatnou se respondentovi jevila opakující se informace o formě implementace, kdy měl být kladen důraz na „jednoduchost a pochopitelnost vůči zákazníkovi bez nutnosti zpracovávat obsáhlý právní dokument“. Během celé implementace nedošlo ke konzultaci s externím specialistou, neboť vedení společnosti nebylo ochotno na toto poskytnout peněžní prostředky.

Z pohledu manažera marketingu byla implementace rozdělena na tři základní kroky, a to přípravu informační architektury na webových stránkách, technická opatření a organizační opatření. V případě úpravy informací byla na webových stránkách vytvořena sekce stránek zabývající se problematikou GDPR, byly aktualizovány obchodní podmínky v souladu s novelou. Rovněž byla aktualizována stránka popisující podmínky zpracování osobních údajů.

Do skupiny úkolů, která se týká technické implementace, řadí respondent kontrolu dodavatelů služeb, zda budou z jejich strany provedeny požadované změny. Společností nebylo realizováno mapování datových toků s cílem analýzy zpracování osobních údajů. Nedošlo ani k úpravě principů zpracování osobních údajů (nedošlo k jejich omezení či změně). S organizací dále spolupracuje externí IT specialista, který byl pověřen realizací opatření, jež se týkala primárně bezpečnosti dat.

Poslední skupinou úkolů bylo organizační opatření, které primárně sestávalo z vytvoření tištěných materiálů týkajících se GDPR pro fyzické uložení ve firmě a instruování vlastních zaměstnanců. Primární motivací pro vytvoření tištěných materiálů byla příprava pro případnou inspekci. Neproběhla dodatečná revize praktik v oblasti udělování přístupových práv apod.

Z časového hlediska trvala probíhala implementace ve společnosti po dobu několika týdnů s pracností v řádu nižších desítek jednotek hodin, kdy majoritní část tvořilo prostudování problematiky, nižší počet jednotek hodin pak samotné úpravy a tvorba výstupů. Vzhledem k tomu, že respondent byl jedinou osobou, která se na implementaci podílela bez jakékoliv externí konzultace, je si respondent vědom možností nedostatků implementace, jejichž náprava by potenciálně mohla trvat „výrazně delší dobu“.

Dle respondenta (manažer marketingu) byly všechny kroky implementace realizovány postupně s dostatečným předstihem, a v době nabytí účinnosti byly již všechny požadavky splněny, a to i s ohledem na fakt, že třetí strany (poskytovatel e-shopového

řešení, e-mailingová služba a další využívané externí aplikace) zavedly nutné změny „až na poslední chvíli“. Změny se týkaly například vytvoření checkboxu pro zaškrtnutí souhlasu se zpracováním osobních údajů a tak dále.Co se nákladů na implementaci týče, ty jsou počítány v řádu vyšších jednotek tisíc korun a sestávají výhradně ze mzdy pověřeného pracovníka.

5.6.2 Dopady na činnosti

V souvislosti s platností GDPR nedošlo ve společnosti k výrazným změnám v oblasti řízení procesů. Implementace se týkala fakticky pouze marketingových procesů a oblasti lidských zdrojů, k širším změnám v organizaci nedošlo. Nebyly zavedeny praktiky vedoucí ke zlepšení procesního řízení ani nebyly zavedeny nové procesy, jež se mají zpracováním osobních údajů zabývat.

- Řízení dat a informací

Dle vyjádření v oblastech řízení informací a dat dochází k neustálým změnám, v souvislosti s implementací GDPR došlo pouze k některým dílčím úpravám. Nelze jednotlivé změny v praktikách přiřknout GDPR.

Subjektivně důležitým tématem je v organizaci bezpečnost dat, a to ne pouze dat osobních. Ačkoliv praktiky v této oblasti nejsou zcela standardizovány, existují opatření, jejichž cílem je snížit riziko jejich úniku či ztráty. Zaměstnanci mají přístup pouze k relevantním databázím, možnosti exportu většího objemu dat jsou omezené zcela na minimum. Dle respondenta případové studie je rizikem v této oblasti samotný přístup jednotlivých zaměstnanců.

V oblasti zpracování osobních údajů dochází k minimalizaci doby uchování těchto údajů s cílem minimalizovat možné úniky. Data jsou po této době z úložišť mazána. V oblasti propojení s externími službami nedošlo ze strany organizace ke změnám. Ani z důvodu nedostatečného zabezpečení nebyla ukončena spolupráce s žádným z těchto subjektů. Dle vyjádření manažera marketingu implementovali všichni dodavatelé služeb GDPR bez výhrad, a to na základě jeho ověření.

- Marketing a prodej

Za výrazně dotčenou je považována oblast on-line marketingu. Pro každé zpracování je explicitně definován právní základ zpracování. Za výrazné změny jsou považovány úpravy v oblasti zpracování cookies na vlastních webových stránkách (ÚOOU, 2021b).

Využívané služby v této oblasti byly dle vyjádření adaptovány bez jakéhokoliv omezení. Pouze došlo ke změnám v přístupu ke měření a ukládání dat.
V oblasti přímého marketingu nedošlo ke změnám i vzhledem k faktu, že s ohledem na poskytované produkty a služby se společnost jen v omezené míře věnuje retenčnímu marketingu. Data získaná prostřednictvím přihlášení do newsletteru jsou po půl roce vymazávána. Údaje o registraci jsou uchovávána v databázi používané platformy.
Problematiku soukromí společnost vůči svým zákazníkům komunikuje výhradně prostřednictvím dedikovaných webových stránek. Transparentnost v této oblasti společnost považuje za svou konkurenční výhodu, na druhé straně se organizace nedomnívá, že se mělo jednat o rozhodující faktor při koupi.

- Řízení rizik

V oblasti řízení rizik nedošlo k výrazným změnám. Vyspělost organizace v oblasti řízení rizik lze i nadále charakterizovat nejnižších „iniciačním“ stupněm vyspělosti, kdy k vyhodnocování rizik dochází ad hoc způsobem, na kterém se primárně podílí vedení společnosti, případně manažeři na úrovni jednotlivých procesů.

- Řízení lidských zdrojů

V oblasti práce se zaměstnanci nedošlo fakticky k žádným změnám. Investice do vzdělání a tréninku v oblasti zpracování osobních údajů společnost nerealizuje, ačkoliv dle vyjádření zástupce organizace je toto jednou ze slabých stránek implementace GDPR v organizaci. Školení v této oblasti má na starosti za implementaci zodpovědný pracovník, k jejímu průběžnému opakování už ovšem nedochází.

- Právo & Compliance management

Právní oblast je omezena na miniální zákonné požadavky, která je spravována jednatelem společnosti. V této oblasti nejsou sledovány žádné krátkodobé ani dlouhodobé změny či dopady v provádění činnosti.

Další analyzované činnosti:

- Vývoj a inovace – společnost se inovacemi systematicky nezabývá.
- Strategické řízení – bez zjevného dopadu.
- Řízení dodavatelského řetězce – bez přímého vliv implementace GDPR
- Účetnictví – bez zjevného dopadu

5.7 Shrnutí výsledků a diskuse

Podkladem pro shrnutí této časti jsou výsledky třech provedených případových studií, jejichž souhrnné výsledky jsou zobrazeny v níže uvedených tabulkách 5-2 (implementace GDPR) a 5-3 (dopady na činnosti). Shrnutí výsledků je provedeno na základě odpovědí na položené dílčí výzkumné otázky.

Tabulka 5-2: Shrnutí výsledků případové studie (část „implementace GDPR“)

Průběh implementace GDPR	**Crystalis s.r.o.**	**Dům a zahrada Ježek s.r.o.**	**Firma A**
Zahájení	Jaro 2018	Jaro 2018	Konec roku 2017
Dokončení	Před květnem 2018	V květnu 2018	Před květnem 2018
Trvání implementace	< 3 měsíce	< 1 měsíc	< 1 měsíc
Náklady	10 - 50 tisíc Kč	< 10 tisíc Kč	< 10 tisíc Kč
Nákladové položky implementace	zaměstnanec zodpovědný za implementaci + náklady na externí služby (právní a IT)	zaměstnanec zodpovědný za implementaci	zaměstnanec zodpovědný za implementaci
Bariéry implementace	Nedostatek informací (podklady a návody)	Nedostatek informací (podklady a návody)	Nedostatek informací (neucelenost a nejednoznačnost)
	Nepřiměřené finanční výdaje	Znalosti potřebné pro implementaci	Znalosti potřebné pro implementaci
	Negativně zaměřený marketing konzultačních společností	Nedostatek finančních prostředků	Nízká podpora v organizaci
			Limitované finanční prostředky
Kroky implementace	Pověření odpovědného pracovníka	Pověření odpovědného pracovníka	Pověření odpovědného pracovníka
	Rešerše dostupných informací	Rešerše dostupných informací	Rešerše dostupných informací
	Úprava podmínek a dokumentů na webových stránkách	Analýza zpracování dat v organizaci (datové toky)	Příprava opatření
	Úpravy nastavení webových stránek	Organizační opatření	Tvorba požadované dokumentace
	Školení personálu	Úprava podmínek a dokumentů na webových stránkách	Úprava podmínek a dokumentů na webových stránkách
		Úpravy nastavení webových stránek	Změny nastavení webových stránek
		Kontrola externích služeb	Tvorba interních dokumentů
		Přeložení dokumentů do dalších jazyků	Školení personálu
Externí služby	Ano	Ne	Ne

Zdroj: vlastní zpracování

Tabulka 5-3: Shrnutí výsledků případové studie (část „dopady na činnosti e-shopu“)

Dopady	**Crystalis s.r.o.**	**Dům a zahrada Ježek s.r.o.**	**Firma A**
Řízení dat a informací	Změna přístupu ke zpracování zákaznických údajů	Zabezpečení dat (Politika přístupových práv, zálohování)	Zabezpečení dat (Politika přístupových práv)
	Úprava zpracování dat na stránkách e-shopu	Nižší dostupnost informací, které poskytují aplikace	Minimalizace doby uchování dat
Marketing a prodej	Zajišťováni souhlasu se zpracovaním osobních údajů (externí služby)	Restrikce v oblasti přímého marketingu (e-mailing)	Zvýšení transparentnosti v oblasti zpracování osobních údajů
	Snížení výkonnosti kampaní	Snížení výkonnosti reklamních kampaní	Omezení v oblasti retenčního marketingu
		Přehodnocení on-line marketingové strategie	
Řízení rizik	Orientace na regulatorní a reputační rizika	Orientace na regulatorni rizika	Bez zřejmých změn
HR	školení v oblasti zpracování osobních údajů	bez dopadu	školení v oblasti zpracování osobních udajů
Právo & Compliance management	Krátkodobé vyšší náklady na činnost (zpracování obchodních podmínek)	Bez zjevného dopadu	Bez zjevného dopadu
Vývoj a inovace	Bez zjevného dopadu		
Strategické řízení	Bez zjevného dopadu		
Řízení dodavatelského řetězce	Bez zjevného dopadu		
Účetnictví	Bez zjevného dopadu		

Zdroj: vlastní zpracování

- **Jak malé a střední e-shopy prezentují problematiku zajišťování soukromí vůči zákazníkovi?**

V rozporu s předchozími poznatky v oblasti vnímání zajištění soukromí ze strany zákazníků (kapitola 3.2.2), jakožto jednoho z faktorů při výběru obchodníka, všechny tři zkoumané subjekty se věnují oblasti prezentace problematiky soukromí vůči zákazníkovi pouze v minimální legislativou dané míře. Faktor zajištění soukromí vůči zákazníkovi není vybranými malými e-shopy vnímán jako potenciální konkurenční výhoda.

Vliv na tento postoj dle respondentů případové studie nemají ani potenciálně limitující faktory (nedostatek finančních prostředků či schopnosti možné úpravy zavést).

- **Jak malé e-shopy implementují GDPR?**

Přístupy ani postupy k implementaci se v případě třech zkoumaných subjektů výrazně neliší v jejich základních charakteristikách. Ve všech třech případech došlo k implementaci před nabytím účinnosti v květnu 2018. Co se týče času potřebného pro implementaci, byla zapotřebí v případě malého e-shopu doba v rozmezí od několika týdnu po tři měsíce, přičemž ještě menší rozdíly mezi subjekty jsou v pracnosti implementace. Z hlediska nákladů si pak implementace vyžádala investici v rozpětí od řádu vyšších jednotek tisíc (v případě zcela interně prováděné implementace) do nižších desítek tisíc (v případě spolupráce s externími subjekty). Poznatky z hlediska času a nákladů podporují již dříve získané poznatky ve zkoumané oblasti (Faifr & Januška, 2021; Hospodářská komora ČR, 2018) i výsledky systematické literární rešerše. Co se týče nákladových položek, pak implementaci zpravidla v prostředí malých e-shopů zajišťoval vedením společnosti pověřený pracovník. V jednom případě pak byly investovány peněžní prostředky na externí právní či IT služby, což neodpovídá předpokladům dle literární rešerše (G13).

Z hlediska konkrétních postupů vybrané subjekty nenásledovaly žádné strukturované teoretické přístupy k implementaci. Jimi stanovený postup ve všech případech vycházel z podkladů a návodů volně dostupných v internetových zdrojích.

Oproti v této práci dříve uvedenému rozsahu aktivit vedoucích k implementaci (kapitola 4.6.4), je rozsah aktivit vedoucích k implementaci v prostředí malých společností o poznání užší. Ve všech případech implementace sestávala z pověření odpovědného

pracovníka, rešerše dostupných informací (rozšíření znalostí potřebných pro implementaci), následného zavádění organizačních a technických opatření. Ta zpravidla byla prováděná jen v omezeném rozsahu a soustředila se pouze na některé klíčové oblasti (například udělování přístupových práv, aktualizaci smluvních podmínek či tvorbu dokumentů). Ve dvou ze třech případů pak byla implementace zakončena školením personálu. V oblasti monitoringu či udržení stavu compliance jsou aktivity v případě zkoumaných subjektů minimální.

- **Jaké kritické faktory ovlivňují přístup k implementaci GDPR?**

Na přístupech všech zkoumaných společnosti se projevily jak obecné charakteristiky těchto společností, tak specifika týkající se implementace GDPR u této skupiny firem (tj. malých podniků).

Nejvýznamnějšími faktory, které určily povahu implementace GDPR ve společnosti, byly podnikové znalosti a kompotence společnosti v kontextu volných peněžních prostředků, kdy se na jedné straně všechny zmíněné subjekty potýkaly s minimálními znalostmi dané problematiky a schopnostmi GDPR implementovat. Na druhé straně byla i klíčovými faktory nemožnost či neochota do implementace GDPR investovat.

I proto byly přístupy ve všech případech velmi podobné, implementací byla pověřena jedna interní osoba, jež následně prováděla jednotlivé úkony na základě samostudia informací na internetu. V jednom případě byly do implementace GDPR zapojeny externí subjekty, ale pouze v rozsahu poskytnutí dílčích výstupů (zpracování obchodních podmínek e-shopu).

Především výše zmíněné faktory pak determinovaly i rozsah implementačních projektů, které byly oproti identifikovaným postupům jen velmi omezené. Technické limity v provádění opatření byly kompenzovány poskytovateli externích on-line služeb.

Poznatky provedené případové studie v tomto ohledu potvrzují platnost poznatků získaných literární rešerší, které se týkaly bariér implementace GDPR u MSP, i pro skupinu malých e-shopů. Nad to se u sledované skupiny projevuje obecný postoj k problematice ochrany osobních údajů, kdy je GDPR vnímano jako další administrativní zátěž.

- **Jaké jsou důsledky implementace na činnosti e-shopu?**

Obecně lze shrnout dopady na vybrané podnikové činnosti jako minimální. Oproti výčtu potenciálních dopadů, které byly identifikovány výše v této práci (kapitoly 4.6.1 a 4.6.2), se u vybraného vzorku společností objevují pouze dílčí změny v praktikách. Dle zjištění doprovodným efektem implementace není v rozporu s poznatky z provedené rešerše obecný rozvoj procesního prostředí v organizaci, a to i s ohledem na rozsah implementačních projektů, které toto nepředpokládaly.

Na druhé straně identifikované změny ve vybraných podnikových procesech odpovídají definovaným změnám, přičemž jsou vnímány primárně s negativní konotací.

V oblasti **klíčových činností**, které byly definovány v kapitole 3.1.5 se dopady týkají činností marketingu & prodeje a péče o zákazníka. Všechny sledované podniky vnímaly tyto činnosti jako součást jednoho celku. Mezi vnímané dopady pro tuto oblast činností vnímají zkoumané e-shopy shodně restrikce v oblasti přímého marketingu i souvisejícího snížení výkonnosti on-line kampaní. To v konečném důsledku vede k relativnímu zdražení marketingových aktivit společností.

V oblasti „příchozí“ či „odchozí“ logistiky nebyly sledovány v kontextu implementace GDPR specifické dopady a opatření. Předávání osobních údajů zákazníků přepravcům při doručování zásilek je řešeno standardně dle informační povinnosti prodejce (kapitola 3.1.4) aktualizovanými obchodními podmínkami a na základě přepravci aktualizovanými zpracovatelskými smlouvami. V důsledku implementace GDPR také nebyly zaznamenány změny v oblasti běžné operativy a v rámci vyřizování požadavků zákazníků.

Změny lze ovšem sledovat v části **podpůrných činností**. V oblasti řízení dat a informaci ve dvou ze třech případů dochází i v důsledku implementace GDPR k vyšší akcentaci problematiky zabezpečení dat a bezpečnosti obecně. V případě společnosti Crystalis s.r.o. vzhledem k jejímu charakteru došlo k úpravám v oblasti zpracování osobních údajů. Zbývající změny, a to zhoršená dostupnost a kvalita zpracovávaných informací či minimalizace doby pro uchování dat, jsou oslovenými společnostmi vnímány spíše negativně.

V oblasti řízení rizik nedošlo k výrazným změnám. Vyšší pozornost je věnována identifikaci rizik regulatorního a reputačního charakteru. Ovšem bez dopadu na ostatní

aktivity RM dle vymezení v kapitole 3.2.1. Nejsou rovněž sledovány přímé důsledky pro RM dle kapitoly 3.2.2. Nakolik lze tyto poznatky zobecnit na skupin malých e-shopu bude předmětem zkoumání následujícího dotazníkové šetření (kapitola 6).

Primárním důsledkem v oblasti lidských zdrojů je nutnost školení zaměstnanců v této oblast, školení a trénink byl ovšem zpravidla jednorázový. V jednom případě pak nebylo školení provedeno vůbec.

5.8 Limity výzkumného šetření

Limity provedených případových studií vychází již z jejich designu a účelu, kdy se jedná o vícenásobnou kvalitativní případovou studii z prostředí třech podniků. Ačkoliv se pro výzkum jedná o reprezentativní subjekty, výsledky šetření nelze zobecnit na celou zkoumanou skupinu podniků. Na druhou stranu výsledky tohoto šetření doplňují a rozšiřují dřívější zjištění o specifika podnikání malých subjektů na internetu. Tato studie dále podrobně popisuje současný stav implementace v dané skupině podniků, dokresluje jejich kontext a umožňuje upřesnit design dále prováděných šetření.

Další limitem provedeného šetření je fakt, že byly zkoumány dopady pouze na omezený výčet podnikových činnosti, a to konkrétně těch, které byly identifkovány jako relevantní pro zkoumanou skupinu malých e-shopů (dle kapitoly 3.1.5) a zároveň byl v rešerši u těchto činností identifikován možný dopad na danou činnost (kapitola 4.6.1).

6 Management rizik v souvislosti s implementací GDPR

Zatímco první dvě šetření popisují postup implementace nařízení GDPR, respektive dopady implementace na klíčové činnosti malých e-shopů, třetím definovaným dílčím cílem výzkumu je **popsat a zhodnotit souvislosti mezi implementací GDPR a oblastí řízení rizik se zaměřením malé e-shopy v ČR**. Na základě předchozích poznatků i dostupné teorií jde o zjištění, *do jaké míry souvisí implementace GDPR s praktikami v oblasti managementu rizik malých e-shopů?* I s ozhledem na povahu výzkumu, který probíhá po nabytí účinnosti nařízení, není zkoumán kauzální vztah mezi oběma výše uvedenými proměnnými. Výše položená výzkumná otázka pro tento cíl výzkumu je níže v Tabulka 6-1 rozložena na specifické výzkumné otázky:

Tabulka 6-1: Výzkumné a specifické výzkumné otázky (cíl 3)

Dílčí cíl 3:
Popsat a zhodnotit souvislosti mezi implementací GDPR a oblastí řízení rizik se zaměřením na malé e-shopy v České republice.
Výzkumná otázka 3:
Do jaké míry souvisí implementace GDPR s praktikami managementu rizik malých e-shopů?
Specifické výzkumné otázky:
Jaké existují souvislosti mezi managementem rizik a implementací GDPR v organizacích? (SVO3.1)
Jak lze hodnotit systém řízení rizik? (SVO3.2)
Jaká existují kritéria hodnocení managementu rizik? (SVO3.3)
Jaký existuje vztah mezi implementací GDPR a vyspělostí managementu rizik organizací? (SVO3.4)
Jaké faktory mají na případný vztah mezi implementací GDPR a vyspělostí managementu rizik vliv? (SVO3.5)

Zdroj: vlastní zpracování

S ohledem na návaznost této části výzkumu na předchozí části disertační práce a zároveň znění položených specifických otázek, je součástí designu dotazníkového šetření rovněž kvantitativní zhodnocení implementace GDPR u malých e-shopů, a to především ze dvou důvodů:

- Kvantitativní doplnění informací týkajících se specifických výzkumných otázek SVO2.2. až SVO2.4. (definovány v kapitole 5) a tím naplnění dílčího výzkumného cíle 2 (dle uvedení v kapitole 1).
- Jako prostředek srovnání mezi implementací GDPR u malých e-shopů a jejich současným řízením rizik (SVO3.1., SVO3.4., SVO3.5.).

6.1 Metodika dotazníkového šetření

Vzhledem k definovanému dílčímu cíli se jedná o šetření deskriptivní, kdy k jeho vyhodnocení jsou využity metody kvantitativního výzkumu a statistické analýzy (Hendl, 2015).

Kvantitativní výzkum je proveden **dotazníkovým šetřením on-line** (CASI[58]). S ohledem na design výzkumu této disertační práce je toto šetření provedeno coby závěrečné, kdy jsou v této části uvažovány poznatky vyplývající z předchozích částí práce, a to provedené systematické literární rešerše a případových studií. Metoda dotazníkového šetření byla vybrána i coby nástroj pro verifikaci získaných předchozích poznatků na větším počtu zástupců zkoumané skupiny (Creswell, 2013). V souladu s tématem disertační práce šetření byly osloveny právnické osoby odpovídající následujícím kritériím:

- Jedná se o malý e-shop dle definice uvedené v kapitole 3.1.6.1.[59]
- Jedná se o maloobchodní společnost - skupina 47 dle CZ-NACE (ČSÚ, 2023)
- Subjekt implementoval GDPR
- Subjekt a účastníci výzkumu souhlasí s poskytováním informací

Předmětem výzkumu je v tomto případě implementace GDPR vybraných subjektů, kdy na základě literární rešerše budou v následující části definovány hypotézy i dílčí proměnné. Vzhledem k různé povaze sledovaných proměnných bude pro testování každé hypotézy využito různých statistických metod a testů.

6.1.1 Hypotézy

V rámci kvantitativních studií jsou vedle výzkumných otázek definovány i hypotézy (Creswell, 2013; Gray, 2009), a to jako věcná tvrzení o souvislosti mezi uvažovanými proměnnými. Ty se neshodují se statistickými hypotézami, které budou uvedeny pro zkoumání platnosti níže uvedených hypotéz (Eger & Egerová, 2014). Věcné hypotézy jsou definovány následovně[60]:

[58] Computer Assisted Self Interviewing je metoda internetového dotazování, kdy respondent obdrží pozvánku k výzkumu elektronickou formou a následně vstupuje do dotazovacího prostředí, kde zaznamenává svoje odpovědi na otázky (STEM/MARK, 2023).
[59] Šetření nebylo prováděno na podnikajících fyzických osobách, a to s ohledem na možné restrikce týkající se zpracování osobních údajů a také s ohledem na charakteristiky těchto subjektů v kontextu výzkumu.
[60] Definice těchto hypotéz není totožná s nulovými hypotézami, jež budou definovány pro provedení statistických testů (Gray, 2009).

H1. Průměrná úroveň praktik managementu rizik u malých e-shopů pozitivně koreluje s počtem činností, jež byly v rámci implementace GDPR prováděny.

Tato hypotéza uvažuje vazbu mezi úrovní dílčích praktik managementu rizik, k čemuž je využit užívaný aparát pro hodnocení managementu rizik v organizaci, a činnostmi implementace GDPR, jež byly zmapovány v kapitole 4 a doplněny v kapitole 5.

V tomto případě jsou uvažovány dílčí praktiky v rámci podnikového řízení rizik, jež bez ohledu na celkové hodnocení vyspělosti managementu rizik organizace aplikují. To může být dáno dílčími kroky implementace GDPR, které se částečně shodují nebo navazují na jednotlivé praktiky managementu rizik (viz například kapitola 3.4.5).

Tento předpoklad je podpořen i dřívějšími poznatky, kdy adopce systému managementu rizik je podporována platností nových regulatorních opatření (Lam, 2017). Dále je podporován předpokladem, že regulatorní opatření a jejich plnění (a specificky i GDPR) má své důsledky pro management rizik organizací (Lam, 2017; Hubbard, 2020; Girling, 2013). Na druhé straně na základě zjištění vícenásobné případové studie nelze tyto předpoklady prozatím potvrdit.

H2. Organizační kontext a chararakteristiky malých e-shopů mají vliv na počet činností, jež jsou během implementace GDPR uvažovány

S ohledem na poznatky Faifra & Janušky (2021) je smyslem této hypotézy ověřit vliv identifikovaných charakteristik malých e-shopů na počet činností implementace GDPR, jež jsou v rámci implementace prováděny. Které konkrétní faktory budou v rámci dotazníkového šetření sledovány, je upřesněno v následující podkapitole 6.1.2.

H3. V případě certifikace standardy ISO se zvyšuje i úroveň implementace GDPR v organizaci.

V návaznosti na kapitolu 3.3.3.2 existuje pozitivní vztah mezi certifikací ISO 27000 a implementací GDPR. Smyslem této hypotézy je tento vztah ověřit i v prostředí malých e-shopů v České republice, a to i s ohledem na další možné formy standardizace a certifikace. Výčet uvažovaných standardů je uveden v následující podkapitole 6.1.2.

6.1.2 Definice proměnných

V této části jsou rámcově definovány proměnné, jež jsou v rámci šetření uvažovány. Zároveň je v této fázi popsána vazba na konstrukci jednotlivých otázek dotazníku:

- **Úroveň dílčích praktik managementu rizik**

Podkladem pro definici nejlepších praktik managementu rizik byla využita metodika hodnocení vyspělosti, konkrétně modelu vyspělosti PMMM (Crawford, 2014; Faifr, 2020). Na základě předchozích zjištění (Faifr, 2020) tento model vzhledem k definici praktik managementu rizik i hodnocení vyspělosti odpovídá potřebám výzkumu. Byl vybrán i vzhledem ke snadnosti využití v rámci šetření.

Vybraný model PMMM je formální nástroj vyvinutý společností PM Solutions k měření zralosti projektového řízení organizace (Crawford, 2014). Cílem metodiky PMMM je stejně jako u ostatních modelů vyspělosti umožnit jakékoli organizaci systematicky a efektivně rozvíjet své schopnosti projektového řízení (Ferreira de Souza, 2015).

Stejně jako v případě jiných modelů (například OPM3) je řízení rizik u tohoto modelu rozděleno na šest klíčových komponent (praktik), přičemž je dále uvažován i systém dokumentace při řízení rizik. Na základě sebeevaluace lze posoudit jak úroveň konkrétní praktiky, tak hodnocení managementu rizik jako celku. Metodika je založena na sebehodnocení a je tedy možné ji využít v rámci prováděného dotazníkového šetření.

Tabulka 5-2 zobrazuje přehled uvažovaných dílčích praktik managementu rizik dle modelu PMMM, který odpovídá i definicím v kapitole 3.2.1. Dále jsou v tabulce definovány i jednotlivé úrovně každé dílčí praktiky. Ve třetím sloupci je pak k dané úrovni přiřazeno i vzestupné skóre. Hodnoty kategoriálních proměnných jsou využity pro statistické vyhodnocení úrovně jednotlivých praktik.

Tabulka 6-2: Praktiky managementu rizik, úroveň praktik a jejich skóre

Definované praktiky	**Úroveň praktik**	**Hodnota kategoriální proměnné**
Plánování řízení rizik	Iniciační fáze	1
Identifikace rizik	Standardizovaný proces	2
Kvalitativní analýza rizik	Institucionalizované procesy	3
Kvantitativní analýza rizik	Řízené procesy	4
Plánování opatření vůči rizikům	Optimalizované procesy	5
Monitoring a controlling rizik		
Dokumentace rizik		

Zdroj: vlastní zpracování na základě Faifr (2020)

V rámci dotazníku byly otázky vedoucí k zhodnocení úroveň definovány následujícím způsobem:

> „Charakterizujte <DEFINOVANÁ PRAKTIKA>[61] ve vaší organizaci. <KRÁTKÉ VYSVĚTLENÍ DANÉ PRAKTKY>. Vyberte jednu z možností“

Následné uzavřené otázky budou obsahovat vždy celkem šest odpovědí. Pro každou oblast je zvoleno vždy 5 možností dle popisu dané praktiky v **Příloze A**. A to pro zhodnocení úrovně dané praktiky. Šestou možností je pak možnost „Nedokážu posoudit“.

Oproti metodice vzhledem k podobnosti obou praktik jsou sloučeny praktiky „*Kvalitativní analýza rizik*“ a „*Kvantitativní analýza rizik*“ jako jedna praktika „*Analýza rizik*“. Tak jak například uvádí Hassel & Cedergren (2021) nebo ISO (2018b).

Otázky dotazníku včetně možností odpovědi jsou uvedeny v **Příloze E**.

- **Průměrná vyspělost managementu rizik**

Oproti metodice PMMM nebude využit aparát pro zhodnocení úrovně vyspělosti managementu rizik, která je daná úrovní praktiky s nejnižším hodnocením (Crawford, 2014). Pro evaluaci bude využit aritmetický průměr hodnocení jednotlivých praktik. Důvodem výběru této proměnné je také předpokladané neparametrické testování, kdy by mohl být výsledek testování v případě většího počtu shodných hodnot v souboru zkreslen (Hendl, 2015).

- **Činnosti implementace GDPR**

Na základě předchozí části výzkumu (výzkumný cíl 1 a výzkumný cíl 2 uvedené v kapitole 1) jsou definovány konkrétní aktivity, jež mohou být součástí implementace GDPR v případě malého e-shopu.

Tato proměnná je daná součtem provedených kroků implementace, kdy hodnota každého dílčího kroku je definována binárně následujícím způsobem:

- 1 – tato činnost byla v rámci implementace GDPR realizována,
- 0 – tato činnost nebyla v rámci implementace GDPR realizována.

[61] Z tabulky 6-2

Celkový výčet činností v rámci implementace pro potřeby provedeného dotazníkového šetření čítá **30 různých činností**. Seznam vychází ze seznamu 27 činností uvedených v Tabulka 4-15, který byl na základě provedených případových studií (kapitola 5), rozšířen o dvě další identifikované aktivity, a to „*Nastavení zodpovědnosti za implementaci GDPR*“ a „*Zpracování Podmínek pro zpracování OÚ na webových stránkách*“[62]. V kontextu poznatků vyplývajících z provedené případové studie byla dále upravena aktivita „*Technická a organizační opatření*“, která byla rozdělena na aktivitu „*Technická opatření*“ a „*Organizační opatření*“.

- **Charakteristiky a kontext malých e-shopů**

Pro potřeby provedeného šetření byly definovány kategoriální vzájemně výlučné proměnné, které indikují konkrétní charakteristiku zkoumaného e-shopu. S ohledem na možný vliv na podobu implementace GDPR či vyspělost RM byly zkoumány následující faktory:

- **oblast podnikání** v rámci maloobchodu[63]
- kromě e-shopu v ČR také **provoz e-shopu v zahraničí** (binární proměnná + rozdělení do jednotlivých kategorií dle zemí působnosti)
- **standardizace ISO** – standardy uváděné v kapitole 4.6.3, každá forma standardizace má povahu binární proměnné (standardizace ano/ne)
- **jiné formy certifikace**[64] - binární proměnná
- **přístup k implementaci** z perspektivy zapojení jiných než pouze interních zdrojů v návaznosti na předchozí shrnutí v kapitolách 4.6.6, 5.7 či Faifr & Januška (2021) – kategoriální proměnná
- zpracování **zvláštních kategorií osobních údajů** dle Faifr & Januška (2021)

6.1.3 Přehled statistických metod

Pro testování definovaných proměnných a výše uvedených hypotéz v kapitole 6.1.2 jsou kromě základního statistického aparátu (absolutní četnost, relativní četnost, průměr, medián) využity různé typy metod statistického testování. Jejich přehled je s ohledem na konkrétní hypotézy a proměnné uveden v následující tabulce 6-3.

[62] V souladu se Zákonem č. 110/2019 Sb. o ochraně osobních údajů (viz kapitola 3.1.4).
[63] Vychází z klasifikace ekonomických činnosti CZ-NACE (ČSÚ, 2023). Konkrétně se jedná o skupinu „47 Maloobchod, kromě motorových vozidel“ (ČSÚ, 2023).
[64] Formou obecné otázky, konkrétní certifikace se může lišit dle oblasti podnikání.

Tabulka 6-3: Přehled použitých statistický metod

Název testu	**Obecný účel využití**	**Využití v šetření (hypotézy, proměnné..)**
Pearsonův chi-kvadrát test (χ^2 test)	Test existence statisticky významné asociace mezi dvěma kategoriálními proměnnými (Hendl, 2015)	Struktura respondentů, Vliv charakteristik e-shopů
Shapiro-Wilkův W test (S-W test)	Ověření normality dat u náhodné veličiny (Hendl, 2015).	Počet činností implementace, Průměrná vyspělost RM
Kruskal-Wallisův H test (K-W test)	Test o shodě distribučních funkcí dvou a více nezávislých proměnných bez předpokladu normality dat v souboru (Hendl, 2015).	Hypotéza H2, Hypotéza H3
Spearmanův koeficient pořadové korelace ρ	Statistická závislost mezi dvěma veličinami (Hendl, 2015).	Hypotéza H1, Činnosti ve fázích implementace, Rozdíly mezi charakteristikami
t-test o nulové korelaci dvou náhodných veličin	Vyloučení nulové korelace mezi dvěma proměnnými (Pavlík, n.d.).	Hypotéza H1
Dunnův test	Post-hoc analýza Kruskal-Wallisova testu s Bonferroniho korekcí k určení rozdílů mezi jednotlivými výběry (Dinno, 2015).	Hypotéza H2, Hypotéza H3
Fisherova Z-transformace	Zhodnocení statistické významnosti rozdílu dvou korelací (Taraldsen, 2021).	Hypotéza H1

Zdroj: vlastní zpracování

Schéma využití výše uvedených statistických metod v kontextu definovaných hypotéz a průběhu testování je uvedeno v **Příloze D**.

6.1.4 Zkoumaná skupina e-shopů

Dle Creswell (2013) je před provedením dotazníkového šetření třeba jednoznačně identifikovat zkoumanou skupinu respondentů. Výzkumné šetření bylo provedeno na předem stanoveném vzorku respondentů. Kritéria vhodnosti podnikatelského subjektu pro zařazení do šetření byla definována v kapitole 6.1.

Odhad počtu e-shopů působících v České republice vychází z poznatků v kapitole 3.1.6. Informace o počtu e-shopů, které jsou provozovány právnickou osobou, která zároveň odpovídá definici malého podnikání, v současnosti nejsou známy. Prováděné průzkumy se soustředí na e-shopem dosahovanou výši ročního obratu, nikoliv na provozovatele jako takového a jeho další charakteristiky. Na základě tohoto kritéria a odhadů vyplývá,

že co do výše obratu, odpovídá malému podnikání mezi 45000 až 51000 subjekty[65] (APEK, 2023a; CzechCrunch s.r.o., 2023). Oba zmíněné odhady ovšem nerozlišují mezi právnickými a fyzickými osobami.

Pro odhad celkového počtu malých e-shopů provozovaných právnickou osobou byly využity statistiky databáze Orbis (Bureau Van Dijk, 2023), a to konkrétně statistiky ve skupině „*Malých podnikatelských subjektů*" podnikajících v České republice (skupina 47 dle NACE). Z celkově nalezených 106 tisích malých maloobchodních subjektů přibližně 21 % subjektů tvořily osoby právnické[66] (Bureau Van Dijk, 2023). Zbývající část subjektů byla provozována osobami samostatně výdělečně činnými.

Pro potřeby tohoto šetření je tedy odhadováno, že zkoumaná skupina čítá mezi přibližně 9500 a 10700 subjekty (21 % ze 45000 – 51000 malých e-shopů). S ohledem na možnou nepřesnost odhadu bude v další části této práce uvažováno s odhadem **10000 subjektů**.

Pro sběr kontaktů vhodných subjektů byla využita databáze Orbis. Subjekty zde byly vybrány na základě kritérií odpovídajících zkoumané skupině včetně uvedeného e-mailového kontaktu a webových stránek.[67]

Po smazání pro dotazníkové šetření nerelevantních subjektů v exportovaném souboru činil počet kontaktů z této databáze 6802 kontaktů. Ten byl následně doplněn o dalších 1194 unikátních kontaktů sbíraných z dalších volně dostupných databází (členové APEK[68] a subjekty prodávající své zboží na srovnávači Heuréka.cz[69]). Celková nestratifikovaná databáze relevantních subjektů tedy zahrnovala **7996 kontaktů**.

6.1.5 Sběr dat

Dotazník vytvořený v software Google Forms byl nejprve pilotně distribuován mezi 500 respondentů. S ohledem na získanou zpětnou vazbu od vyplňujících respondentů byl tento software následně změněn na software od společnosti Survio s.r.o., byla upravena formulace některých otázek a byly opraveny chyby v nastavení. Celé znění dotazníku je uvedeno v **Příloze E**.

[65] Zaokrouhleno na celé tisíce
[66] Údaje zaokrouhleny na celé tisíce a celá procenta
[67] Pro ověření, že daná společnost skutečně provozuje e-shop.
[68] Dle dostupných údajů (k 12.10.2023) je v této asociaci aktuálně sdruženo 685 členů, z nichž významnou část tvoří právě e-shopy (APEK, 2023c).
[69] Dle dostupných šetření je na tomto srovnávači dle dat z roku 2022 přítomno 73,41 % všech českých e-shopů (Bizmachine, 2023).

Postupná distribuce dotazníků, včetně doprovodného představení obsahu a účelu, mezi kontakty v databázi probíhala následně od 30. srpna do 27. září 2023, a to ve dvou kolech[70]. Celkem bylo v této fázi získáno 211 odpovědí.

Z tohoto vzorku byly následně vyřazeny nerelevantní odpovědi, a to z následujících důvodů:

- Nerelevantní respondent – odpovídající se nezúčastnil implementace GDPR v organizaci a zároveň není zodpovědný za tuto problematiku v organizaci
- Duplicitní odpovědi – dotazník byl vyplněn více než jednou osobou v organizaci nebo byl vyplněn opakovaně
- Vyplněný dotazník nebyl kompletní – například nebyla vyplněna část hodnotící management rizik v organizaci
- Subjekt v současnosti neprovozuje e-shop
- Nerelevantní odpovědi – například zaškrnutí vždy všech možností odpovědi nebo zaškrtnutí vždy první odpovědi v otázce a podobně

Pro analýzu bylo po vyřazení nerelevantních odpovědí zahrnuto celkem **146 odpovědí malých e-shopů**.

Při uvažované a ve výzkumech nejčastěji využívané 95% hladině spolehlivosti (Creswell, 2013; Hendl, 2015), činí při odhadovaném celkovém počtu zkoumané skupiny statistická chyba zaokrouhleně 8,1 %. Za přijatelnou míru chyb se považuje interval chybovosti od 4 do 8 % (Pollfish, 2020). Některé výzkumy v oblasti společenských věd a výzkumu organizací však pracují i s mírou statistické chyby na úrovni až 10 % (Schwambach et al., 2022; Sanchez-Ruiz & Blanco, 2019; Dillman et al. 2009).

6.1.6 Struktura respondentů

Tato podkapitola je rozdělena do dvou částí. Tou první jsou informace o osobách, jež za danou organizaci dotazník vyplnily. V druhé části je pak analyzována struktura respondentů z hlediska zkoumaných charakteristik organizací.

Jak je uvedeno v následující Tabulka 6-4, ze 146 relevantně zodpovězených dotazníků, tvořily nadpoloviční část (55,5 %) odpovědi vyplňované zástupci vedení daných společností. Vzhledem k možnému přesahu mezi funkcemi ve vedení společnosti (majitel může být současně jednatelem, CEO může být současně majitelem apod.), není tato část

[70] Subjektu, který v 1. kole rozeslání dotazník nevyplnil, byl s časovým odstupem dotazník zaslán podruhé.

dále strukturována. Na 41 odpovědí pochází od respondentů (zainteresovaných v implementaci GDPR či zajišťování ochrany osobních údajů), kteří působí v managementu společnosti, nejčastěji bez blíže specifikované oblasti řízení. Nejčastěji zmiňovanými oblastmi řízení u vyplňujících je marketing, provoz či obchod a prodej.

Tabulka 6-4: Respondenti šetření - dle pracovní pozice

Řidicí úroveň (počet respondentů)	**Pracovní pozice**	**Počet respondentů**
Vedení společnosti (81)	Ředitel/jednatel/CEO/majitel/prokurista	81
Management společnosti (41)	Bez bližšího upřesnění	12
	Marketing	9
	Provoz	7
	Obchod a prodej	7
	ICT	2
	Projektový manažer	2
	Finance	1
	HR	1
Neexekutivní pozice (24)	Administrativní pracovník	15
	Správce e-shopu/administrátor webových stránek	5
	Asistent jednatele/ředitele	2
	Hlavní účetní	1
	Právník	1

Zdroj: vlastní zpracování

Minorititní část respondentů (24 odpovědí) pak tvoří neexekutivní zaměstnanci organizací. Nejčastěji zmiňovanými pozicemi jsou v tomto případně blíže nespecifikovaný „*Administrativní pracovník*“, případně „*Správce e-shopu/administrátor webových stránek*“.

Další perspektivou získaných odpovědí je vazba odpovídajícího vůči zkoumanému tématu[71]. To zobrazuje Tabulka 6-5. Každý z respondentů mohl zaškrtnout více než jednu možnost. Ze 146 osob, které vyplnily dotazník, bylo 88 z nich přímo zodpovědných za implementaci GDPR ve společnosti. 80 je v současné době osobami, které jsou zodpovědné za ochranu osobních údajů v organizaci (zahrnující i problematiku GDPR). 57 respondentů pak bylo členem týmu majícího za úkol v organizaci GDPR implementovat (mezi těmito respondenty jsou i osoby, které byly za tento tým zodpovědny viz první možnost).

[71] V předchozí kapitole bylo uvedeno, že odpovědi těch respondentů, kteří nezaškrtnuli žádnou z následujících možností, byly z vyhodnocení vyřazeni.

Tabulka 6-5: Respondenti šetření - dle role v rámci ochrany OÚ

Role v organizaci	Počet respondentů
Zodpovědný za implementaci GDPR	88
V současnosti zodpovědný za zajišťování ochrany osobních údajů	80
Člen týmu pro implementaci GDPR	57

Zdroj: vlastní zpracování

Ze získaných 88 odpovědí osob zodpovědných za implementaci GDPR vyplývá, že v případě malých e-shopů se nejčastěji implementace ujímali zástupci vedení společnosti či jejich majitelé (59 odpovědí z 88). Implicitně pouze 27 % zástupců vedení společnosti (22 z 81) pověřilo implementací osobu jinou než sebe. Přehled implementujících osob dle pracovní pozice je uveden v následujícím výčtu:

- Ředitel/jednatel/CEO/majitel/prokurista – 59 odpovědí
- Management organizace – 19 odpovědí
- Neexekutivní pozice – 10 odpovědí

Druhou perspektivou struktury respondentů jsou informace o samotných společnostech. První perspektivou je odvětví, ve které e-shop působí. Přehled Tabulka 6-6 vychází z kategorizace dle NACE. Mezi odpověďmi se nejčastěji vyskytují nespecializované e-shopy. Ze specializovaných maloobchodů se nejčastěji jedná o obchody se zbožím pro domácnost, kulturní rozhled či rekreaci a ostatní jinak nespecifikované zboží.

Tabulka 6-6: Struktura e-shopů - odvětví dle NACE

Kód	Název	Počet respondentů
472	Potraviny, nápoje a tabákové výrobky ve specializovaných prodejnách	5
474	Počítačová a komunikační zařízení ve specializovaných prodejnách	13
475	Ostatní výrobky převážně pro domácnost ve specializovaných prodejnách	25
476	Výrobky pro kulturní rozhled a rekreaci ve specializovaných prodejnách	20
477	Ostatní zboží ve specializovaných prodejnách	23
4791	Maloobchod prostřednictvím internetu nebo zásilkové služby	60

Zdroj: vlastní zpracování

S ohledem na téma práce je dále v následující tabulce 6-7 uvedena informace o případném působení e-shopu na zahraničnch trzích.

Tabulka 6-7: Struktura e-shopů - prodej v zahraničí

Země působnosti	**Počet**	**Podíl z respondentů (v %)**
Česká republika	146	100 %
Slovenská republika	64	44 %
Ostatní země EU (kromě Slovenska)	32	22 %
Země EU celkem (včetně Slovenska)	69	47 %
Evropské země mimo EU	10	7 %
Neevropské země	8	5 %
E-shopy působící pouze v ČR	**75**	**51 %**
E-shop působící alespoň na 1 zahraničním trhu	**71**	**49 %**

Zdroj: vlastní zpracování

Ze vzorku odpovídajících téměř polovina e-shopů (71 ze 146) prodává své zboží prostřednictvím e-shopu na alespoň jednom zahraničních trhu. Přičemž ve výrazné většině těchto e-shopů se jedná o prodej ve Slovenské republice (64 společností). Dalších 32 e-shopů uvedlo, že bez uvažovaného Slovenska, působí v některé z jiných zemí EU. V 10 případech pak e-shop nabízí své zboží v některé evropské zemi, která není členskou zemí EU. 8 e-shopů pak prodává své zboží i mimo prostor Evropy.

Pro testování hypotéz je rovněž podstatným faktorem případná certifikace organizace některým ze souvisejících standardů ISO, případně některou z jiných certifikací. To zobrazuje Tabulka 6-8. Ze 146 sesbíraných odpovědí, pouze 22,6 % všech e-shopů je certifikováno, případně je přidruženo k některé z komor či asociací.

Tabulka 6-8: Struktura e-shopů - certifikace

Certifikace	**Počet**	**Podíl certifikovaných**
ISO 9000	16	11,0 %
ISO 31000	0	0,0 %
ISO 27000	0	0,0 %
ISO 27552 - Správa osobních údajů	0	0,0 %
Společnost certifikována jinou autoritou (členství v komorách atd.)	17	11,6 %
Certifikované firmy	**33**	**22,6 %**
Firmy bez certifikace	**113**	**77,4 %**

Zdroj: vlastní zpracování

17 respondentů uvedlo, že je certifikováno jinou certifikací než ISO, případně je členem přidružených komor a asociací (například Hospodářská komora, APEK a podobně). V případě certifikace standardy ISO se ve všech 16 případech jedná o standard ISO 9000

týkajícího se systému řízení kvality. Naopak žádná z oslovených firem neuvedla, že je certifikována standardem ISO 31000 (Řízení rizik), ISO 27000 (Bezpečnost dat) či ISO 27552 (Správa osobních údajů). **V tomto důsledku nemůže být součástí zkoumaní tohoto šetření vztah mezi zmíněnými standardy, vyspělostí managementu rizik a implementací GDPR v dané organizaci.**

Faktory, které dle předchozího zjištění autora (Faifr & Januška, 2021) mají vliv na implementaci GDPR v organizaci, je přístup zvolený k implementaci a případné zpracovávání zvláštních kategorií osobních údajů. Dle předchozího zjištění mají tyto dva faktory vliv na celkové náklady implementace GDPR[72]. I proto jsou tyto dva faktory součástí tohoto šetření.

Tabulka 6-9: Struktura e-shopů – externí spolupráce během implementace GDPR

Přístup k implementace	**Počet firem**	**Podíl respondentů**
Interní implementace (bez externí spolupráce)	82	56,2 %
Kombinace aktivit prováděných interně či externě	38	26,0 %
Implementací byl pověřen externí subjekt (Externí služba)	26	17,8 %

Zdroj: vlastní zpracování

Převážná část e-shopů (56,2 %) implementovala dle informací uvedených v tabulce 6-9 výše bez využití kterékoliv externí spolupráce výhradně vlastními prostředky a s využitím pouze vlastních znalostí a dovedností. 38 z 146 pak uvedlo, že část implementace byla provedena interně a část pak externí společností (například jako je to uvedeno v kapitole 5.4.1). Nejmenší část 17 % všech respondentů pak implementaci delegovala zcela na externí subjekt. Rozložení odpovídá obecným specifikům implementace GDPR v kapitole 4.6.5.

Tabulka 6-10: Struktura e-shopů - zvláštní kategorie osobních údajů

Zpracování zvláštních kategorií osobních údajů	**Počet firem**
Ne	124
Ano	22[73]

Zdroj: vlastní zpracování

[72] Mezi zkoumanými faktory ve zmíněné práci byly i velikost organizace a typ organizace (veřejný nebo soukromý subjekt). Byly zjištěny rozdíly v implementaci mezi malými, středními a velkými podniky. Nebyly ovšem potvrzeny rozdíly mezi skupinou malých a mikropodniků. Kromě možnosti ověření a přesného zařazení je i toto důvodem, proč jsou obě skupiny těchto e-shopů zkoumány současně. (Faifr & Januška, 2021).

[73] Skupinu zpracovávajících OÚ ve zvláštních kategoriích tvořily v klasifikaci dle NACE nespecializované e-shopy (11 e-shopů), dále pak byly zastoupeny e-shopy prodávající zdravotnické či farmaceutické výrobky, případně doplňky stravy (7 e-shopů).

Faktory odvětví působnosti e-shopu, zahraniční působnost e-shopu, certifikace standardy a jiné certifikace, vliv externí spolupráce během implementace a zpracovávání zvláštních kategorií osobních údajů byly dále v této práci zkoumány z pohledu jejich vlivu na podobu implementace GDPR v prostředí malých e-shopů. Aby se předešlo možnému zkreslení výsledků vzhledem k těmto charakteristikám shromážděného vzorku, byly pro testování možných asociací mezi uvedenými kategoriálními proměnnými v souladu s doporučeními provedeny dílčí Pearsonovy chí-kvadrát testy (Creswell, 2013; Hendl, 2015)[74]

Výsledky provedených testů jsou uvedeny v níže uvedené tabulce 6-11. S ohledem na nároky testu byly před provedením testů některé proměnné upraveny.[75]

Tabulka 6-11: Struktura e-shopů - Pearsonův chí-kvadrát test

Faktor	**Zahraničí ano/ne**	**Certifikace**	**Externí spolupráce**	**Zvláštní kategorie OÚ**
NACE****	0,577	Četnost <2	**0,274	Četnost <2
Zahraničí ano/ne		0,434	0,412	0,287
Slovensko		0,469	0,439	0,272
Země EU (bez SK)		Četnost <5	0,738	0,223
Země EU (s SK)		0,404	0,309	0,228
Evropské země (mimo EU)		***0,032	**0,684	Četnost <5
Mimoevropské země		Četnost <2	Četnost <2	0,419
Certifikace			*0,087	0,079
Externí spolupráce				0,118

** Spojeny údaje o certifikaci (ISO 9000 + ostatní certifikace) + spojeny údaje o externí spolupráci (externí + kombinovaný přístup)*
*** Spojeny údaje o externí spolupráci (externí + kombinovaný přístup)*
**** Spojeny údaje o certifikaci (ISO 9000 + ostatní certifikace)*
***** Vzhledem k nízkému počtu vyřazena skupina 472*

Zdroj: vlastní zpracování

Na základě naměřených p-hodnot nelze odmítnout nulové hypotézy o shodách v kontingenčních tabulkách na hladině významnost $\alpha = 0,05$. Nelze tedy konstatovat, že by docházelo ke zkreslení výsledku v důsledku provázaného působení dvou různých dále testovaných faktorů. Výjimku tvoří vztah mezi proměnnou týkající se **certifikace**

[74] Pearsonův chi-kvadrát test (Chi-square test) je statistická metoda, která se používá k určení, zda existuje statisticky významná asociace mezi dvěma kategoriálními proměnnými v datasetu. Tato metoda se používá k porovnání pozorovaných frekvencí (četností) s očekávanými frekvencemi a může být použita pro různé statistické analýzy, včetně testu nezávislosti a testu dobré shody (Hendl, 2015).
[75] Chí kvadrát test lze použít, pokud nejmenší očekávaná četnost v 2x2 tabulce je alespoň 5, u ostatní není menší než 2. Pokud je tato hodnota nižší, je potřeba údaje v tabulce upravit a počet kategorii zredukovat (Maths and Stats Support Centre, n.d.). Případně zredukování a sloučení skupin je uvedeno v Tabulka 6-11.

ISO či jinou certifikací a situací, kdy e-shop působí v evropské zemi mimo EU. Na základě p-hodnoty (0,032) lze soudit, že mezi těmito proměnnými může existovat příčinná souvislost. Toto možné zkreslení bude při vyhodnocování uvažováno. V Tabulka 6-11 jsou dále uvedeny případy, kdy nebylo možné s ohledem na výskyt znaků v kategorií test provést. Popsáno jako „*Četnost < 5*“ případně „*Četnost < 2*“ dle rozsahu kontingenční tabulky.

6.2 Výsledky dotazníkového šetření

Níže v této kapitoly jsou uvedeny a analyzovány výsledky provedeného dotazníkového šetření.

6.2.1 Činnosti implementace

Činnosti implementace lze rozdělit do 3 základních skupin, a totiž na aktivity, které jsou spojeny s předimplementační fází, kdy nejsou zapracovávany žádné povinnosti z nařízení vyplývající. Jedná se především o činnosti, jež mají nastavit přístup k prováděné implementaci (v tabulce 6-12 označeno jako A.), druhou skupinu činností tvoří aktivity, jejichž výstupy jsou podklady, které slouží k rozhodování o parametrech budoucí implementace, jejich cílem je primárně zanalyzovat současný stav společnosti s ohledem na požadavky a na jejichž podkladě bude následně implemenetace provedena. Třetí skupinu aktivit pak tvoří naplnění jednotlivých náležitostí implementací ve formě konkrétních aktivit mající za cíl zvýšit úroveň ochrany osobních údajů ve společnosti a vyhovět požadavkům GDPR (s ohledem na zpracované podklady).

Šetřením získané výsledky navazují na dříve provedené výzkumy nastiňující menší připravenost v oblasti implementace GDPR u malých firem, kdy vzorek malých e-shopů v České republice v tomto není výjimkou (Faifr & Januška, 2018; Garber, 2018; Perry, 2019). Výsledky tohoto šetření dále nepřímo doplňují předchozí výzkum autora (Faifr & Januška, 2021) analyzující výši investic do implementace GDPR, kdy lze dát počet vykonaných činností během implementace GDPR do souvislosti s náklady na implementaci.

Na podkladu předchozích zjištění této disertační práce lze tuto situaci obecně vysvětlit třeti hlavními faktory – finančním, znalostním a prioritou v organizaci. Nízká priorita ze strany vedení v důsledku specifik stran implementace GDPR u této skupiny podniků (nízké povědomí či pochopení GDPR, vyšší potřeba konzultovat – viz kapitoly 4.6.5 nebo 5.7) a v tomto důsledku či objektivně nízký rozpočet na implementaci

(viz případové studie 5.4.1 nebo 5.6.1) vede častěji k implementaci bez využití externích služeb (viz Tabulka 6-9), kdy jsou za implementaci zodpovědní pracovnící či vedoucí pracovníci s omezenou znalostí problematiky ochrany osobních údajů. Kombinace a interakce zmíněných faktorů pak může vést k menšímu rozsahu implementačního projektu. Tento předpoklad ovšem prozatím nelze na základě výsledků v Tabulka 6-12 jednoznačně bez zkoumání dílčích faktorů a charakteristik potvrdit.

Žádná z pro implementaci relevantních činností nebyla e-shopy prováděna **ve více než 80 % případů**. V případě předimplementační fáze je nejčastější aktivitou „*Seznámení se s textem nařízení*“, kterou dle výsledků realizovalo 74,7 % (95 % spolehlivosti mezi 62,8 – 86,5 %). Žádná z dalších činností v tomto bloku úkolů nepřesahuje hranici 50 % realizujících e-shopů. To znamená, že pouze minoritní část e-shopů se v rámci implementace zabývá obecným nastavením a plánováním implementačního projektu.

Ještě menší podíl firem lze sledovat v části pro implementaci podkladových dokumentů, které jsou následně využity pro realizaci konkrétních opatření a ošetření dílčích problematických (v souladu s GDPR nevyhovujících) aspektů. Posouzením rizik spojených se zpracováním osobních údajů se zabývalo 43,2 % e-shopů. Mapováním současných datových toku a osobních údajů pak méně než jedna třetina respondentů.

Tabulka 6-12: Činnosti implementace GDPR malými e-shopy

ČINNOST IMPLEMENTACE GDPR	POČET	RELATIVNÍ ČETNOST
A. Předimplementační fáze (řízení projektu)		
Seznámení se s textem nařízení	109	74,7 %
Posouzení vlivu GDPR na organizaci (nakolik se nařízení společnosti týká)	63	43,2 %
Aktivní zvýšení povědomí o GDPR v organizaci	53	36,3 %
Nastavení zodpovědnosti za implementaci GDPR	44	30,1 %
Zpracování plánu projektu implementace	37	25,3 %
B. Dokumenty a vstupní analýzy		
Posouzení rizik zpracování (vyhodnocení rizik spojených se zpracováním osobních údajů)	63	43,2 %
Mapování datových toků a zpracování osobních údajů	42	28,8 %
Analýza současného stavu ochrany osobních údajů + GAP analýza	20	13,7 %
DPIA - zpracování Posouzení vlivu na ochranu osobních údajů	19	13,0 %
Definice strategie zpracování dat v organizaci	16	11,0 %
C. Projektové aktivity (Realizace aktivit)		
Zpracování tzv. "Záznamů o zpracování osobních údajů"	101	69,2 %
Zajištění zákonnosti, férovosti a transparentnosti zpracování (čištění dat, výmaz dat, agenda správy souhlasů, zajištění adekvátních právních základů pro zpracování)	99	67,8 %
Problematika cookies	89	61,0 %
Zpracování Podmínek pro zpracování OÚ na webových stránkách	82	56,2 %
Zajištění práv subjektů (zapracování práv vyplývajících z Nařízení)	61	41,8 %
Trénink personálu a školení	50	34,2 %
Vytvoření postupů pro případ úniku dat a jiných bezpečnostních incidentů	48	32,9 %
Provedení opatření organizačního charakteru (přístupová práva apod.)	48	32,9 %
Provedení technických opatření (např. šifrování, pseudonymizace dat, zavedené nových bezpečnostních systémů apod.)	45	30,8 %
Nastavení zodpovědností za ochranu osobních údajů v organizaci	43	29,5 %
Zajištění zpracování u třetích stran (analýza rizik dodavatelů, pravidla pro předávání údajů třetím stranám apod.)	43	29,5 %
Dokumentace GDPR a prokazování plnění požadavků	40	27,4 %
Minimalizace dat	37	25,3 %
Řízení životního cyklu dat	29	19,9 %
Problematika zpracování zvláštních kategorií osobních údajů (citlivých údajů)	28	19,2 %
DPO - jmenování "Pověřence pro ochranu osobních údajů"	23	15,8 %
Neustálé zlepšování procesu ochrany osobních údajů	23	15,8 %
Komunikace s ÚOOÚ	9	6,2 %
Monitoring a kontrolní mechanismy (systém pro monitoring ochrany osobních údajů)	8	5,5 %
Aplikace přístupů privacy by design a privacy by default v podnikových procesech	3	2,1 %

Zdroj: vlastní zpracování

Největším blokem činností jsou již na základě předchozích analýz konkrétní aktivity vedoucí k vyhovění požadavků GDPR. U žádné z činností nebyl změřen podíl větší než 70 % e-shopů, které se danou aktivitou zabývaly. Z toho lze vyvodit, že podstatná část malých e-shopů alespoň v části předepsaných aktivit nevyhovuje platnému nařízení. Ze seznamu 20 činností v této části 93 % respondentů realizovalo méně než 15 činností, 78 % respondentů realizovalo méně než 10 činností, 47 % respondentů pak realizovalo méně než 5 činností z celkového výčtu.

6.2.2 Korelační vztah mezi fázemi implementace

Kromě samotného měření četnosti prováděných činností bylo zkoumáno, nakolik se jednotlivé fáze mezi sebou ovlivňují. Tento vztah byl měřen na základě koeficientu korelace. Vzhledem k tomu, že naměřené hodnoty nevykazují dle Shapiro-Wilkova testu[76] parametrů normálního rozdělení ($p<0,001$), byla síla vztahu v souladu s doporučeními mezi jednotlivými veličinami měřena na základě Spearmanova koeficientu pořadové korelace ρ (Hendl, 2015), a to s využitím software TIBCO Statistica® 14.1.0 (TIBCO Software Inc., 2023).

Tabulka 6-13: Činnosti implementace GDPR (Spearmanův korelační koeficient ρ)

Fáze implementace GDPR	Předimplementační fáze	Dokumenty a analýzy	Realizace aktivit
Předimplementační fáze	1	0,396	0,616
Dokumenty a analýzy	0,396	1	0,364
Realizace aktivit	0,616	0,364	1

Zdroj: vlastní zpracování

Výsledky v tabulce 6-13 nastiňují, že existuje pozitivní korelační vztah mezi jednotlivými částmi implementace (vyšší počet aktivit v jedné části souvisí s vyšším počtem aktivit v části další). Na hladině $\alpha=0,05$ jsou naměřené vztahy statisticky významné.

Nejsilnější vztah lze sledovat mezi předimplementační fází a realizací konkrétních aktivit, který dle Hall (2020) nebo Statutor (n.d.) lze charakterizovat jako „*střední*“ až „*silný*“. Rozsah aktivit ve fázi příprav na implementaci tak determinuje počet činností, které v rámci realizace budou následně provedeny. U zbývajících dvou testů byla naměřena pozitivní korelace na pomezí „*slabé*“ až „*střední*“ úrovně. Jednotlivé fáze se tak vzájemně ovlivňují, působících faktorů, které ovšem mají vliv na rozsah činností implementace, je více.

[76] Shapiro-Wilkův W test slouží k ověření, že naměřená náhodná proměnná má normální rozdělení. (Hendl, 2015).

6.2.3 Faktory ovlivňující rozsah implementace GDPR

V předchozí části byly představeny obecné výsledky týkající se implementace GDPR v případě malých e-shopů. Nicméně, jak je z kapitoly 6.1.6 zjevné, existují mezi touto skupinu podniků rozdíly, co se týče:

- odvětví, ve kterém působí,
- prodeje v zahraničí,
- certifikace e-shopu,
- přístupu k implementaci,
- specifik zpracování OÚ.

Pro ověření vlivu výše uvedených charakteristik byly za tímto účelem provedeny dílčí statistické testy. Dle Shapiro-Wilkova W testu náhodná veličina neodpovídá normálnímu rozdělení ($p<0,001$). Pro testování vlivu zmíněných charakteristik bude v souladu s doporučeními prováděn neparametrický test, které nevyžadují povědomí o rozdělení zkoumaných veličin[77] (Hendl, 2015). Konkrétně byl proveden Kruskal-Wallisův test (Hendl, 2015). Test je založen na ordinálních hodnotách, kdy nulové hypotézy předpokládají, že měření ve dvou a více nezávislých skupinách mají stejné mediány (Hendl, 2015). Výsledky testovaných charakteristik jsou uvedeny souhrnně v Tabulka 6-14.

Tabulka 6-14: Faktory ovlivňující implementaci GDPR (K-W test)

Charakteristika e-shopu	K–W H test	Počet stupňů volnosti	$\chi 2$ rozdělení	p-hodnota	H_0
Odvětví dle NACE	6,058	5	11,070	0,301	Nezamítnutí
E-shop v zahraničí	0,182	1	3,841	0,670	Nezamítnutí
E-shop v SR	0,411	1	3,841	0,521	Nezamítnutí
E-shop v další zemi EU kromě SR	2,237	1	3,841	0,135	Nezamítnutí
E-shop v kterékoliv zemi EU	0,146	1	3,841	0,703	Nezamítnutí
E-shop v evropském státu mimo EU	5,052	1	3,841	0,025	Zamítnutí
E-shop v neevropském státu	2,321	1	3,841	0,128	Nezamítnutí
Certifikace e-shopu (dle typů)	3,015	2	5,991	3,015	Nezamítnutí
Externí spolupráce během implementace	9,860	2	5,991	0,007	Zamítnutí
Zvláštní kategorie OÚ	7,873	1	3,841	0,005	Zamítnutí

Zdroj: vlastní zpracování

[77] Obecnou nevýhodou neparameritrických testů je dle Hendla (2015) jejich nižší citlivost na odchylky od nulové hypotézy.

Na základě definice nulových hypotéz a zvolené hladině významnosti (α=0,05) lze konstatovat, že na závislou proměnnou (počet činností implementace GDPR) maji statisticky významný dopad tyto charakteristiky e-shopů (v tabulce 6-14 vyznačeny červeně):

- **E-shop je provozován v dalším evropském státu, který není členem EU**

Z provedeného K-W testu vyplývá, že existuje statisticky významný rozdíl v počtu činností prováděných během implementace mezi e-shopy, které prodávají své zboží v Evropě mimo členské státy EU, a e-shopy ostatními. U sledované skupiny (viz Tabulka 6-15) činil medián počtu činností implementace 13 činností, u zbývající skupiny e-shopů medián činil činností 8 (rovněž medián celého souboru výsledků).

Tabulka 6-15: Prodej v evropských zemích mimo EU – analýza

Kriérium: „*E-shop prodává v evropských zemích mimo EU*“	**Počet respondentů**	**Počet činností implementace** *(medián)*	**Počet činností implementace** *(průměr)*	**Certifikace ISO 9000** *(podíl v %)*
Ano	10	13	14,2	50,0 %
Ne	136	8	9,1	7,5 %
Celkové výsledky	**146**	**8**	**9,4**	**11 %**

Zdroj: vlastní zpracování

Ačkoliv testem nalezené rozdíly jsou statisticky významné, je u této proměnné třeba uvažovat, že naměřený rozdíl vychází z údajů od 10 e-shopů majících tuto charakteristiku.

Kromě toho je zároveň u této charakteristiky potřeba uvažovat dle výsledků statisticky významnou souvislost mezi mimo EU (v Evropě) prodávajících e-shopů a různými formami certifikace (Tabulka 6-14). To je patrné i z Tabulka 6-15, kdy ve sledované skupině 50 % e-shopů je certifikováno standardem ISO 9000 oproti obecnému výsledku 11 %.

Fakt, že v naměřeném vzorku jsou tedy nalezeny rozdíly v počtu uvažovaných činností v rámci implementace GDPR, nutně nemusí znamenat kauzální vztah mezi prodejem zboží mimo EU (nezávislá proměnné) a implementací GDPR (závislá proměnná), jak by výsledky testu mohly napovídat.

S ohledem na výše zmíněné a z toho vyplývající možné zkreslení v interpretaci nebude v případě tohoto faktoru provedena dodatečná analýza k určení činností, u nichž se relativní četnost v provádění u sledovaných skupin liší.

- **Externí spolupráce během implementace**

Z výsledků provedených K-W testů (Tabulka 6-14) dále vyplývají statisticky významné rozdíly dle obecného přístupu, jakým bylo GDPR implementováno. Dle výsledků nejvíce činností bylo v rámci implementace realizováno e-shopy, které při implementaci využily externích prostředků v kombinaci s těmi interními (viz Tabulka 6-16).

Tabulka 6-16: Externí spolupráce během implementace GDPR - analýza

Způsob implementace	**Počet respondentů**	**Počet činností implementace** *(medián)*	**Počet činností implementace (***průměr)*
Interní implementace	82	8	8,1
Kombinace interní+externí	38	9,5	11,5
Externí služba	26	8,5	10,6
Celkové výsledky	**146**	**8**	**9,4**

Zdroj: vlastní zpracování

V případě, že je K-W testem nalezen rozdíl mezi více než dvěma nezávislými proměnnými, je třeba post-hoc analýzou určit, mezi kterými soubory tento rozdíl existuje (Hendl, 2015). V Tabulka 6-17 jsou uvedeny p-hodnoty provedeného Dunnova testu, kdy jsou všechny soubory na základě mnohonásobného srovnávání testovány zvlášť (Dinno, 2015). Z výsledků post hoc analýzy vyplývá, že existuje statisticky významný (na hladině spolehlivosti α=0,05) rozdíl mezi implementací, která je prováděna zcela interně a kdy kombinací aktivit prováděných interně s externí spoluprácí. Naopak významné rozdíly nejsou mezi implementací, kterou prováděl zcela externí subjekt/y. Samotné zapojení externího subjektu do implementace tedy nemusí znamenat, že bude provedena rozsáhlejší implementace GDPR s uvažováním více oblastí.

Tabulka 6-17: Post-hoc analýza – Ext. spolupráce během implementace (p-hodnoty)

Způsob implementace	Interní implementace	Kombinace interní+externí	Externí služba
Interní implementace	-	0,008	0,275
Kombinace interní+externí	0,008	-	1
Externí služba	0,275	1	-

Zdroj: vlastní zpracování

Naopak z výsledků měření vyplývá, že nejvíce činností je realizováno v kombinaci, kdy implementace probíhá jak s využitím interních, tak externích prostředků. U skupin, kde byl nalezen statisticky významný rozdíl rozdíl v počtu vykonávaných činností v rámci implementace, byla následně provedena analýza mající za cíl identifikovat konkrétní činnosti, u nichž se jejich četnost v obou skupinách signifikantně liší (α=0,05). Pro test dvou kategoriálních proměnných byl proveden Pearsonův chí-kvadrát test.

Tabulka 6-18 zobrazuje pouze ty činnosti, u nichž byl rozdíl v podílu ve srovnávaných skupin na základě provedeného testu statisticky významný.

Tabulka 6-18: Ext. spolupráce během implementace (činnosti s rozdílnou četností)

Činnost implementace	**Četnost v souboru (n=146)**	**Podíl** "Bez spolupráce s ex. subjekty "	**Podíl** „Část implementace interně, část externě "	**p-hodnota**
Zpracování plánu projektu implementace	25,3 %	13,4 %	36,8 %	0,003
Nastavení zodpovědnosti za implementaci GDPR	30,1 %	20,7 %	44,7 %	0,007
Seznámení se s textem nařízení	74,7 %	86,6 %	71,1 %	0,041
Zajištění práv subjektů (zapracování práv vyplývajících z Nařízení)	41,8 %	31,7 %	63,2 %	0,001
Zajištění zpracování u třetích stran	29,5 %	19,5 %	44,7 %	0,004
Provedení opatření organizačního charakteru	32,9 %	24,4 %	50,0 %	0,005
Neustálé zlepšování procesu ochrany osobních údajů	15,8 %	7,3 %	26,3 %	0,004
Problematika zpracování zvláštních kategorií osobních údajů (citlivých údajů)	19,2 %	7,3 %	34,2 %	<0,001

Zdroj: vlastní zpracování

Z výsledků vyplývá, že e-shopy, které v rámci implementace zvolily kombinovaný způsob pro implementaci, obecně přistoupily k implementaci systematičtějším způsobem. To je patrné především u činností „*Zpracování plánu projektu implementace*“ a „*Nastavení zodpovědnosti za implementace GDPR*“ v předimplementační fázi. Na druhé straně e-shopy implementující „svépomocí“ se častěji zabývaly „*Seznámením se s textem nařízení*“ tak, aby byly schopny implementaci zajistit.

V případě konkrétních činností během zapracování požadavků GDPR lze u skupiny e-shopů implementujících s využitím externích služeb najít častější provádění činností týkajících zajištění práv subjektů, zajištění zpracování u třetích stran, provedení opatření orgnaizačního charakteru stejně principy nastavení vedoucí k neustálému zlepšování procesu ochrany osobních údajů. Výrazně vyšší lze nalézt i podíl podniků zabývajících se zpracováním zvláštních kategorií osobních údajů. Tato aktivita vychází plně z kontextu zpracování, kdy ač nebyl prokázán statisticky větší podíl těchto firem (Tabulka 6-11), podíl firem, které se touto problematikou zabývaly je výrazně vyšší.

- **Zpracování OÚ, které spadají do zvláštních kategorií**

Již dříve byl zjištěn rozdíl v nákladech na implementaci GDPR mezi organizacemi obecně (Faifr & Januška, 2021). Dle výsledků K-W testu (Tabulka 6-12) byl jako významný zjištěn tento faktor u skupiny malých e-shopů, pokud je závislou proměnnou počet činnosti implementace GDPR. Lze tedy soudit, že při zpracování zvláštních kategorií osobních údajů lze očekávat rozsáhlejší a nákladnější implementaci GDPR.

Tabulka 6-19: Zvláštní kategorií OÚ - analýza

Kriérium: *„E-shop zpracovává zvláštní kategorie OÚ“*	**Počet respondentů**	**Počet činností implementace** *(medián)*	**Počet činností implementace** *(průměr)*
Ano, zpracovává	*22*	*12,5*	*13,2*
Ne, nezpracovává	*124*	*8*	*8,7*
Celkové výsledky	***146***	***8***	***9,4***

Zdroj: vlastní zpracování

Pro srovnání obou skupin byla dále provedena série chí-kvadrát testů kategoriálních proměnných s cílem zmapovat činnosti, u nichž se jejich četnost v porovnávaných skupinách významně liší (α=0,05). Činnosti, u nichž byl rozdíl v četnosti statisticky významný, jsou uvedeny v následující tabulce 6-20.

Tabulka 6-20: Zpracování kategorií OÚ (činnosti s rozdílnou četností)

Činnost implementace	**Četnost v souboru (n=146)**	**Podíl u citlivé údaje** "*Ano*"	**Podíl u citlivé údaje** "*Ne*"	**p-hodnota**
Předimplementační fáze				
Aktivní zvýšení povědomí o GDPR v organizaci	36,3 %	63,6 %	31,5 %	0,004
Nastavení zodpovědnosti za implementaci GDPR	30,1 %	59,1 %	25,0 %	0,001
Projektové aktivity				
Zpracování tzv. "Záznamů o zpracování osobních údajů"	69,2 %	90,9 %	65,3 %	0,017
DPO - jmenování "Pověřence pro ochranu osobních údajů"	15,8 %	40,9 %	11,3 %	<0,001
Provedení opatření organizačního charakteru	32,9 %	50,0 %	29,8 %	0,035
Dokumentace k prokázání implementace GDPR	27,4 %	54,5 %	22,6 %	0,002
Průběžná aktualizace a zlepšování ochrany OÚ	15,8 %	36,4 %	12,1 %	0,004
Problematika zpracování zvláštních kategorií osobních údajů (citlivých údajů)	19,2 %	54,5 %	12,9 %	<0,001
Životní cyklus dat	19,9 %	36,4 %	16,9 %	0,035

Hned u 9 činností byla v případě e-shopů zpracovávajících zvláštní kategorie OÚ zvýšená četnost v jejich provádění. Žádná z nich se nenachází v druhé fázi implementace.

Častěji se e-shopy zpracovávající citlivé OÚ v první fázi zabývaly „*Aktivním zvýšením povědomí o GDPR v organizaci*“ i „*Nastavením zodpovědosti za implementaci GDPR*“.

V případě zpracování konkrétních požadavků implementace, sledovaná skupina e-shopů výrazně častěji zpracovala „*Záznamy o zpracování osobních údajů*“, a to ve více než 90 % případů. Dále byl častěji jmenován Pověřenec pro ochranu osobních údajů a prováděna organizační opatření. Více než v 50 % případů se tyto e-shopy zabývaly zpracováním dokumentace pro budoucí prokázání plnění požadavků GDPR. Dle předpokladů byla v rámci této části častěji aktivně reflektována specifická pozornost zvláštním kategoriím osobních údajů. Nicméně se i tak jednalo o „pouze“ 54,5 % e-shopů.

6.2.4 Vyspělost RM malých e-shopů

Dle získaných výsledků lze soudit, že management rizik dosahuje v případě malých e-shopů obecně nízkých stupňů vyspělosti, kdy u všech šesti sledovaných oblastí managementu rizik většina respondentů ohodnotila vyspělost dané aktivity nejnižším stupněm. U pěti ze šesti aktivit se jednalo o více než 69 % respondentů. V tomto ohledu lze za nejvíce „vyspělou“ mezi e-shopy ohodnotit přístup vedoucí k ošetření rizik s nejnižším zastoupením e-shopů s nejnižším stupněm hodnocení.

Tabulka 6-21: Vyspělost RM u malých e-shopů

Úroveň vyspělosti (*Hodnotící škála)*	**Iniciační fáze** *(1)*	**Standardizované procesy** *(2)*	**Instit. Procesy** *(3)*	**Řízené procesy** *(4)*	**Optim. procesy** *(5)*	**Průměr hodnocení**
Plánování	113	19	6	4	4	**1,40**
Identifikace rizik	102	21	10	4	9	**1,61**
Analýza rizik	107	20	6	2	11	**1,56**
Opatření	74	56	9	3	4	**1,68**
Controlling	118	10	8	4	6	**1,42**
Dokumentace	111	22	3	5	5	**1,43**
Vyspělost RM *(metodika PMMM)*	**130**	**13**	**2**	**1**	**0**	**1,54**

Zdroj: vlastní zpracování

V kontextu obecného poznání v oblasti vyspělosti podniků, tyto výsledky odpovídají charakteristikám malých podniků, pro které je nižší vyspělost typická (kapitola 3.2.5). V kontextu prováděného výzkumu pak lze soudit, že pro malé e-shopy není management rizik prioritní oblastí.

Stejně jako v případě implementace GDPR i v případě vyspělosti byly dále zkoumány, které charakteristiky malých e-shopů mohou mít vliv na vyspělost v oblasti managementu rizik. Závislou proměnnou byl pro tyto potřeby uvažovan průměr vyspělosti v jednotlivých oblastech. Pro zkoumání vlivu nezávislých proměnných byl s ohledem na jiné než normální rozdělení provedena opět série K-W testů. Výsledky jsou uvedeny v Tabulka 6-22.

Tabulka 6-22: Faktory ovlivňující vyspělost RM (K-W test)

Faktor	**K–W test**	**Stupňů volnosti**	**$\chi 2$ rozdělení**	**p-hodnota**	**H_0**
Odvětví dle NACE	10,53	5	11,07	0,062	Nezamítnutí
E-shop v zahraničí	0,36	1	3,84	0,549	Nezamítnutí
E-shop v SR	0,44	1	3,84	0,506	Nezamítnutí
E-shop v další zemi EU kromě SR	2,35	1	3,84	0,125	Nezamítnutí
E-shop v kterékoliv zemi EU	0,12	1	3,84	0,732	Nezamítnutí
E-shop v evropském státu mimo EU	1,81	1	3,84	0,178	Nezamítnutí
E-shop v neevropském státu	4,94	1	3,84	0,026	Zamítnutí
Certifikace e-shopu (dle typů)	10,53	2	5,99	0,005	Zamítnutí
Externí spolupráce během implementace	2,04	2	5,99	0,361	Nezamítnutí
Zvláštní kategorie OÚ	0,003	1	3,84	0,955	Nezamítnutí

Zdroj: vlastní zpracování

Na vyšší vyspělost má v naměřeném souboru statisticky významný vliv, pokud e-shop prodává své zboží jinde než v Evropě. Dále také fakt, že je e-shop certifikován. Stejně jako v předchozí části, v případě zahraničního prodeje výsledky vycházejí ze souboru čítajícího 8 výsledků. Dále platí, že z 8 těchto e-shopů, v kontrastu vůči celkovým výsledků, je 5 e-shopů certifikováno (3 x certifikace ISO 9000 a 2 x ostatní certifikace). Samotný fakt, že e-shop prodává své zboží mimo státy Evropy tedy nemusí být předpokladem pro vyspělejší aktivity v rámci managementu rizik.

Další faktorem mající vliv na vyspělost aktivit managementu rizik je faktor certifikace e-shopu. Výsledky jednotlivých skupin e-shopů jsou uvedeny v Tabulka 6-23.

Tabulka 6-23: Vyspělost managementu rizik v kontextu certifikace e-shopu

Certifikace e-shopu	**Počet**	**Medián**	**Průměr**
Bez certifikace	113	1,2	1,4
ISO 9000	16	1,8	2,1
Ostatní certifikace a standardizace	17	1,5	1,8

Zdroj: vlastní zpracování

Vzhledem k tomu, že soubor zahrnuje více než 2 pozorování (nebinární proměnná), byl k určení skupin, které se odlišují opět proveden post-hoc Dunnův test. P-hodnoty jednotlivých testů jsou uvedeny v Tabulka 6-24. Statisticky významný je rozdíl mezi skupinou e-shopů, které nejsou z uvedených možností certifikovány vůbec a skupinou e-shopů certifikovaných standardem ISO 9000. Vztah mezi managementem rizik a standardizací ISO 9000 uvádí mimo jiné Durst et al. (2019). S ohledem na téma práce pak byl vztah mezi tímto standardem a managementem rizik uváděn, kdy byl ISO 9000 uváděn jako vhodný metodický podklad při souběžném využití standardu ISO 31000 během implementace GDPR (viz kapitola 4.6.3).

Tabulka 6-24: Post-hoc analýza vyspělosti RM - Certifikace (p-hodnoty)

Certifikace e-shopu	Bez certifikace	ISO 9000	Ostatní certifikace
Bez certifikace	-	0,026	0,134
ISO 9000	0,026	-	1
Ostatní certifikace a standardizace	0,134	1	-

Zdroj: vlastní zpracování

6.2.5 Souvislost managementu rizik s implementací GDPR

V této části práce je testován vztah mezi vyspělostí praktik managementu rizik a počtem činností, které jsou v rámci implementace GDPR prováděny. Vzhledem k tomu, že ani jedna z uvedených proměnných nemá parametry normálního rozdělení, je pro vyhodnocení síly vztahu mezi těmito dvěma proměnnými použit Spearemanův koeficient pořadové korelace ρ (Hendl, 2015). Statistická významnost testu je následně ověřena na základě provedeného t-testu o nulové korelaci dvou náhodných veličin (Pavlík, n.d.). Dle výsledků měření v Tabulka 6-25 mezi průměrnou úrovní vyspělosti jednotlivých aktivit a počtem činností v rámci implementace byl celkově zjištěn slabý pozitivní korelační vztah (ρ=0,29). Interpretace výsledků vychází z Hall (2020) a Statutor (n.d.). Stejně lze interpretovat výsledky, pokud byl měřen korelační vztah mezi průměrnou vyspělosti aktivit v rámci RM a počty činností v jednotlivých fázích implementace. Naměřené korelace jsou statisticky významné na hladině $\alpha = 0,05$.

Tabulka 6-25: Spearmanův korelační koeficient ρ (fáze implementace)

Aktivit v rámci implementace GDPR	**ρ**	**Interpretace**
Předimplementační fáze	0,28	slabá pozitivní korelace
Dokumenty a vstupní analýzy	0,24	slabá pozitivní korelace
Projektové činnosti	0,24	slabá pozitivní korelace
Činnosti celkem	**0,29**	**slabá pozitivní korelace**

Zdroj: vlastní zpracování

Naměřené výsledky tedy na jedné straně ukazují na existující vztah mezi zkoumanými proměnnými, zároveň se ovšem jedná o vztah, který lze interpretovat dle použité škály jako „**slabý**“. To znamená, že sice **existuje souvislost mezi proměnnými a vyšší vyspělost souvisí s vyšším počtem činností implementace GDPR**, nejedná se ovšem o faktor stěžejní a na podobě implementace GDPR či vyspělosti RM mají vliv další faktory a charakteristiky. Ty byly mimo jiné identifikovány v předchozích kapitolách 6.2.3. a 6.2.4.

Další část zkoumání vztahu mezi managemntem rizik a implementací GDPR je v následující tabulce 6-26 provedeno z perspektivy jednotlivých charakteristik. Tedy zkoumání těsnosti vztahu mezi RM a implementací GDPR v rámci skupin e-shopů dle jejich zkoumaných charakteristik. V rámci této analýzy jsou uvažovány pouze ty charakteristiky e-shopů, u nichž byl ověřen statisticky významný vliv na implementaci GDPR nebo vyspělost managementu rizik v předchozích kapitolách. U ostatních charakteristik nebyly významné rozdíly zjištěny.

Výsledky jsou uvedeny v Tabulka 6-26. Černě jsou vyznačeny statisticky nevýznamné výsledky, kde nelze vyloučit nulovou korelaci mezi oběma proměnnými. Červeně jsou vyznačeny výsledky, které lze interpretovat jako statisticky významné (na hladině $\alpha = 0{,}05$ lze vyloučit nulovu korelaci). Modře jsou vyznačeny ty výsledky, kde se interpretace korelačního vztahu liší v porovnání s obecnými výsledky v Tabulka 6-25. Tedy, kde $\rho \notin (0{,}2;0{,}4)$ a kde zároveň lze výsledky i vzhledem k počtu měření považovat za statisticky významné (na hladině $\alpha = 0{,}05$).

Tabulka 6-26: Spearmanův korelační koeficient (charakteristiky e-shopu)

Průměrná vyspělost RM	Počet záznamů (n)	Spearmanův koeficient pořadové korelace			
		Počet aktivit celkem	**Předimple-mentační fáze**	**Dokumenty a vstupní analýzy**	**Požadavky implementace**
Celý soubor	**146**	**0,292**	**0,284**	**0,236**	**0,240**
E-shop se zahraničním prodejem	71	0,315	0,248	0,226	0,287
E-shop bez zahraničního prodeje	75	0,274	0,321	0,245	0,196
E-shop v evropském státu mimo EU (ano)	10	0,427	0,602	**0,750**	0,305
E-shop v evropském státu mimo EU (ne)	136	0,259	0,252	**0,181**	0,217
E-shop v neevropském státu (ano)	8	0,200	0,507	0,698	-0,048
E-shop v neevropském státu (ne)	138	0,277	0,261	**0,184**	0,237
E-shop není certifikován	113	0,230	0,218	**0,160**	0,182
Certifikace ISO 9000	16	**0,659**	0,461	0,420	**0,610**
Ostatní certifikace	17	0,294	**0,502**	0,175	0,219
Zvláštní kategorie OÚ (ano)	22	0,310	**0,438**	0,414	0,130
Zvláštní kategorie OÚ (ne)	124	0,312	0,259	0,203	0,266
GDPR implementováno externě	26	0,378	0,364	0,225	0,385
Kombinace interních a externích zdrojů	38	0,296	0,289	0,208	0,263
Implementováno bez externích prostředků	82	0,260	0,265	0,235	**0,187**

Zdroj: vlastní zpracování

Pro zjištění nakolik jsou změřené rozdíly mezi korelačními koeficienty statisticky významné byla následně provedena Fisherova z-transformace (Taraldsen, 2021). Pro srovnávací test byla použita pouze ta měření, u nichž byla naměřená korelace (mezi průměrem vyspělosti RM a „Počtem aktivit celkem“) statisticky významná[78] a od obecných výsledků se lišila alespoň jedním stupněm interpretace (jiná než „pozitivní slabá“ korelace). Výsledky testu o shodě dvou korelací jsou uvedeny v Tabulka 6-27.

[78] Z testování bylo vyřazeno srovnání vždy dvou charakteristik, u nichž byl naměřený korelační koeficient statisticky nevýznamný.

Tabulka 6-27: Fisherova z-transformace (rozdíl korelací dle faktorů)

Porovnané charakteristiky	Fáze imp. GDPR	z-skóre	p-hodnota	Závěr (při α = 0,05)
Prodej v evropském státu mimo EU (ano x ne)	Dokumenty a analýzy	2,037	0,042	Zamítnutí, rozdíl je významný
Prodej v neevropském státu (ano x ne)	Dokumenty a analýzy	1,586	0,113	Významnost nelze potvrdit
Certifikace: ISO 9000 x žádná certifikace	Počet aktivit celkem	-1,898	0,058	Hraniční výsledek, významnost nelze potvrdit
Certifikace: ISO 9000 x ostatní certifikace	Počet aktivit celkem	-1,267	0,205	Významnost nelze potvrdit
Certifikace: ISO 9000 x ostatní certifikace	Předimp. fáze	-0,139	0,890	Významnost nelze potvrdit
Certifikace: Ostatní certifikace x žádná certifikace	Předimp. fáze	-1,164	0,244	Významnost nelze potvrdit
Certifikace: ISO 9000 x žádná certifikace	Dokumenty a analýzy	-0,976	0,329	Významnost nelze potvrdit
Certifikace: Ostatní certifikace x žádná certifikace	Dokumenty a analýzy	-0,054	0,957	Významnost nelze potvrdit
Certifikace: ISO 9000 x žádná certifikace	Realizace aktivit	1,790	0,074	Významnost nelze potvrdit
Certifikace: ISO 9000 x ostatní certifikace	Realizace aktivit	1,263	0,207	Významnost nelze potvrdit
Zvláštní kategorie OÚ (ano/ne)	Předimp. fáze	0,830	0,407	Významnost nelze potvrdit
Implementace: Externí x interní	Realizace aktivit	-0,915	0,360	Významnost nelze potvrdit
Implementace: Interní x kominace externí+interní	Realizace aktivit	-0,394	0,693	Významnost nelze potvrdit

Zdroj: vlastní zpracování

Z výsledků vyplývá, že kromě jednoho případu nelze považovat korelační vztah mezi vyspělostí aktivit RM a počtem činností implementace GDPR za vymykající se výsledkům obecným. Výjimku tvoří korelační vztah mezi proměnnými u e-shopů prodávajících v neunijiních evropských zemích, co se fáze zpracování podkladů pro implementaci týče. Zde byla zjištěna „silná“ korelace mezi proměnnými oproti ostatním e-shopům. Za související lze ovšem kromě této charakteristiky považovat i výrazně vyšší zastoupení e-shopů, jež jsou certifikovány standardy ISO 9000. Ačkoliv toto bylo statisticky potvrzeno pouze v případě počtu činností implementací. Standardizace ISO 9000 může synergicky posilovat vazbu mezi vyspělostí RM i implementací GDPR.

Toto tvrzení podporuje i zjištěna „silná pozitivní“ korelace v případě certifikace ISO 9000 v porovnání s ostatními e-shopy obecně. Na základě naměřených hodnot ovšem nelze toto tvrzení podpořit. P-hodnota se zde pohybovala těsně nad nastavenou hranicí α= 0,05 (p-hodnota = 0,058).

6.3 Shrnutí výsledků dotazníkového šetření

Cílem závěrečného dotazníkového šetření bylo popsat a zhodnotit důsledky pro management rizik malých e-shopů v souvislostí s implementací GDPR. Níže jsou uvedeny výsledky prizmatem položených specifických výzkumných otázek (Tabulka 6-1).

Hned v několika částech této disertační práce byla načrtnuta vazba mezi managementem rizik podniku a implementací GDPR. O obecné souvislosti hovoří kapitola 3.2.2:

- Regulatorní opatření (například i GDPR) jako jeden ze zdrojů rizik pro podnik.
- Regulatorní opatření mají vliv na systémy řízení podnikových rizik, systémy pro řízení rizik uvažují existenci regulatorních požadavků.
- Implementace regulatorních opatření vede v důsledku i k vyšší adopci metod řízení rizik.

V konkrétní souvislosti s GDPR je pak v rámci teoretického vyvození tento vztah popisován na více místech:

- V rámci ochrany osobních údajů je očekáván „rizikový přístup“, tedy přístup založený na předchozím posouzení rizik vyplývajících ze zpracování OÚ (kapitola 3.4.2).
- Vyhodnocení rizik zpracování je součástí implementace GDPR v organizaci (kapitola 3.4.5).
- Metodiky pro provedení DPIA zahrnují kroky analýzy rizik (kapitola 3.4.5).

Teoretická východiska byla následně potvrzena provedenou systematickou rešerší (kapitola 4):

- Řízení rizik (případně jako „Posouzení rizik“) je uváděno jako jeden z ovlivněných procesů v důsledku implementace GDPR (Tabulka 4-7). Konkrétní změny jsou uvedeny v kapitole 4.6.2.5).
- Řízení rizik a z této problematiky odvozené standardy lze využít jako podklad pro implementaci v organizaci.
- Posouzení rizik zpracování jako jednoho z kroků implementace (Tabulka 4-15).
- Nedostatky implementace GDPR v případě MSP jako důsledek chybějícího systému pro posuzování rizik (4.6.5).

Na podkladě provedené vícenásobné případové studie (kapitola 5) bylo provedeno dotazníkové šetření, jehož cílem bylo zkoumat těsnost vztahu mezi managementem rizik

a implementací GDPR na příkladech malých českých e-shopů. Jako nástroj pro hodnocení vyspělosti byla využita metodika hodnocení vyspělosti PMMM (Tabulka 6-2) v kombinaci s poznatky teoretické části práce.

Na základě získaných odpovědí lze malé e-shopy obecně charakterizovat z hlediska řízení rizik jako nevyspělé (kapitola 6.2.4), což dokládají i poznatky provedené případové studie, a z hlediska implementace GDPR jako málo připravené, kdy nedostatky mohou vycházet jak z obecných charakteristik MSP (kapitola 3.2.5), tak specifických charakteristik malých e-shopů, jež byly tímto dotazníkovým šetřením rovněž testovány.
Z pohledu implementace GDPR lze u malých e-shopů považovat za významné faktory:

- Prodej v zemích mimo EU (zde ovšem výsledky vychází z nízkého počtu měření).
- Způsob implementace GDPR – obvykle nejvíce činností v rámci implementace GDPR vykonávaly subjekty, které kombinovaly interní přístup s externími službami.
- Citlivost zpracovávaných informací – navazuje na požadavky GDPR (vyšší ochranná opatření musí být provedena tam, kde jsou zpracovávány zvláštní kategorie OÚ), ale také předchozí provedené výzkumy prováděné na obecném vzorku podnikatelských subjektů (Faifr & Januška, 2021).

V případě malých e-shopů je pak obecné nízká vyspělost ovlivněna prodejem do neevropských zemí či případnou certifikací e-shopu, kdy jen minoritní část 22,6 % e-shopů (Tabulka 6-8) je certifikována standardem ISO 9000 nebo jinou autoritou. Žádný z analyzovaných malých e-shopů pak nebyl certifikován standardy ISO 31000, ISO 27000 či ISO 27552, z čehož vyplývá, že možný důsledek na implementaci GDPR ani vyspělost RM nemohl být tímto šetřením vyhodnocen.

Klíčovou částí, i s uvážením výše shrnutých zjištění, bylo zkoumání těsnosti vztahu mezi managementem rizik a implementací GDPR. Na základě změřených Spearmanových korelačních koeficientů byly zjištěny **slabá pozitivní korelace** mezi počtem činností, jež jsou v rámci GDPR uvažovány a průměrnou vyspělosti managementu rizik malého e-shopu (Tabulka 6-25). A to v rámci všech tří definovaných fází implementace. Lze tedy soudit, že existuje měřitelný pozitivní vztah mezi oběma oblastmi a vyspělejší RM vede k implementaci GDPR, při které je uvažováno více činností. Případně naopak, že širší implementace GDPR může vést k rozvoji RM v e-shopu. Na druhou stranu obecný koeficient $\rho=0,29$ naznačuje, že na obě sledované

proměnné působí více specifických (viz například faktory určující rozsah implementace či průměrnou vyspělost RM) nebo společných faktorů. Například, že omezené znalosti či finanční prostředky malých e-shopů vedou současně k nižšímu rozsahu implementace GDPR a zároveň k nižší vyspělosti managementu rizik.

V tomto důsledku byla následně těsnost vztahu mezi oběma oblastmi testována v kontextu šetřením uvažovaných charakteristik malých e-shopů stran implementace GDPR, kde byly dále výsledky uvažovány i v rámci jednotlivých fází implementace. Za významně působící v tomto ohledu byl zjištěn dopad na těsnost vztahu v případě certifikace ISO 9000, která, kromě pozitivního dopadů na vyspělost praktik managementu rizik, synergicky působí i na rozsah implementace GDPR.

S ohledem na teoretická východiska práce lze soudit, že v případě sledovaných malých e-shopů a jejich charakteristik lze sledovat omezený vztah, kdy je pro tuto sledovanou skupinu i s ohledem na jejich dílčí charakteristiky typická současně malá vyspělost praktik RM a malý rozsah implementace GDPR. Teoretické poznatky týkající se vzájemného vztahu tedy s ohledem na zjištění ve skupině malých e-shopů nelze jednoznačně potvrdit, a to s ohledem na relativně nízké zastoupení e-shopů s vyšší vyspělostí praktik RM (Tabulka 6-21). Na druhé straně pozitivní pořadová korelace mezi oběma zkoumanými proměnnými znamená, že je ani nelze odmítnout. Naměřená síla vztahu mezi oběma proměnnými pak značí, že těsnost vztahu je v obou případech ovlivněna více faktory, z nichž některé byly tímto šetřením taktéž uvažovány.

6.4 Limity dotazníkového šetření

Při interpretaci výsledků je třeba uvažovat několik limitací, které jsou s provedeným šetřením spojeny. Prvním z nich je omezení zkoumání na skupinu e-shopů, které odpovídají definici malého podnikání (EC, 2019a) a zároveň jsou provozovány právnickými osobami. Ačkoliv zjištěné poznatky navazují na předchozí obecné poznatky týkající se dopadů implementace GDPR či vztahu mezi implementací a managementem rizik, lze je zobecňovat pouze pro skupinu malých e-shopů.

Dalším limitem šetření je zkoumaný vzorek respondentů. Ačkoliv jsou poznatky zjištěné od 146 respondentů statisticky významné (na 95% hladině spolehlivosti činí statistická chyba 8,1 %) s ohledem na velikost zkoumané skupiny, relativně menší počet výsledků neumožňoval otestovat některé charakteristiky e-shopů. V případě některých charakteristik či kombinací bylo k dispozici nedostatečné množství výsledků.

Mezi respondenty například nebyl dostatečný počet e-shopů, které by byly certifikovány některými ze standardů ISO, u kterých byla definována teoretická souvislost s implementací GDPR. Samotným předmětem šetření by mohlo být zmapování standardů, z nichž malé e-shopy při své organizaci vycházejí.

Třetím omezením je počet charakteristik e-shopů, jejichž vliv byl v rámci prováděného šetření prováděn. Čtvrtým a posledním limitem tohoto výzkumného šetření pak byly činnosti implementace, které byly vzhledem k odstupu od provedené implementace zkoumány pouze z hlediska jejich výskytu v rámci implementačního projektu. Nebyla přitom uvažována různá znalostní, stejně jako časová či finanční nákladnost dané aktivity.

7 Diskuze výsledků disertačního výzkumu

Dílčí výsledky provedených šetření a z nich vyvozená východiska byly blíže uvedeny v **kapitolách 4.6.6**, **5.7** a **6.3**. V této části jsou výsledky provedeného disertačního výzkumu diskutovány z hlediska stanovených výzkumných cílů v kapitole 1.

Dopady na klíčové činnosti malého e-shopu

V kontextu provedeného disertačního výzkumu je současnou literaturou definováno 13 různých podnikových oblasti, jež jsou implementací GDPR ovlivněny. Z pohledu malého e-shopu se jedná ve větší míře o činnosti podpůrné (řízení dat a informací či řízení lidských zdrojů). Z primárně sledovaných klíčových činností e-shopu (vymezeno v kapitole 3.1.5), jež jsou hlavním předmětem zkoumání této disertační práce, se jedná o oblasti **marketingu & prodeje** a **péče o zákazníka**, jakožto činností, v jejichž rámci dochází ke zpracování a další práci s osobními údaji zákazníků.

Dle literární rešerše (kapitola 4.6.2.3) lze soudit, že v odborné veřejnosti neexistuje jednotný pohled na povahu zmapovaných dopadů pro tuto oblast. V rámci marketingu a prodeje jsou uvedené důsledky pro tuto činnost na spektru od negativních (ztráta důvěryhodnosti vůči zákazníkovi, snížení kvality dat a efektivy reklamy, snížení tržeb apod.), přes neutrální (změny v aktivitách, změny v postojích zákazníků či potřebě vzdělání v této oblasti, automatizace zpracovávaných dat) až po dopady pozitivní (zlepšení výsledků kampaní, zlepšení vztahu se zákazníkem či zvýšení etičnosti prováděných kampaní). Pozitivní dopady lze v tomto ohledu ovšem vnímat jako důsledek adekvátního uchopení problematiky GDPR a ochrany osobních údajů. Což ale dle empirických šetření není případ malých e-shopů, pro něž je na podkladě provedené literární rešerše problematika zajišťování soukromí záležitostí okrajovou, a to s ohledem na existující bariéry, co se znalostí a postojů vůči dané problematice týče. V případě marketingu a prodeje tak jsou u malých e-shopů vnímány dopady jako snížení výkonnosti marketingových kampaní, omezení v oblasti přímého nebo retenčního marketingu či nuceného přehodnocení on-line marketingové strategie.

Vzhledem k charakteristikám malých e-shopů pak nebyly vysledovány dopady na další klíčové činnosti e-shopů (logistické aktivity nebo operativa). Nerelevantní pro tuto skupinu podniků jsou i změny v obecném procesním prostředí, která neprocházejí výraznou disrupcí (viz Tabulka 4-10). Dopady na činnosti podpůrné

lze pak rozdělit na dvě hlavní skupiny. Dopady krátkodobé v přímém důsledku implementace GDPR a dopady dlouhodobějšího účinku v důsledku změn v daných činnostech. Typickým krátkodobobým dopadem je v případě malých e-shopů provedení školení personálu či náklady na právní služby. Dlouhodobější změny se pak týkají změn ve zpracování dat v důsledků restrikcí při zpracování OÚ či zavedení nebo úprava politky zabezpečení dat.

V případě činností, jako jsou oblasti práva, vývoje a inovací, strategické řízení či účetnictví pak lze sledovat na jedné straně buď minimální aktivitu v těchto oblastech nebo nelze sledovat dopad na danou činnost.

Implementace GDPR malými e-shopy

Soudobá literatura poměrně široce definuje možné přístupy a postupy vedoucí k implementaci GDPR. Velký počet uvažovaných činností vyplývá i z faktu, že implementace GDPR vychází z kontextu dané organizace. Některé činnosti, které jsou relevantní pro jednu skupinu podniků, tak nemusí být relevantní pro skupinu další.

Pozornost byla v případě této disertační práce věnována malým e-shopům. Jak na podkladu provedené případové studie, tak na podkladu provedeného dotazníkového šetření lze vyvozovat, že implementace v prostředí této skupiny podniků je spojena s řadou omezení, která mají na způsob implemenace přímý vliv.

Převládajícím přístupem ve skupině malých e-shopů je implementace bez externí spolupráce, kdy je zapracováním požadavků pověřený jeden konkrétní interní pracovník (velmi často jednatel nebo majitel společnosti, případně řidíci pracovník). V kontextu se znalostními požadavky na implementaci GDPR je pak implementace prováděna s cílem splnit minimální legislativní požadavky bez potřeby uchopit danou problematiku v širším kontextu řízení organizace.

Kritické faktory a bariéry implementace GDPR u malých e-shopů

Nedostatky v implementaci GDPR lze v případě malých e-shopů vnímat z pohledu existujících faktorů a bariér, které mají na implementaci GDPR vliv. Tyto faktory lze kategorizovat na ty, jež jsou platné pro celou skupinu malých a středních podniků, a na skupinu faktorů, které jsou charakteristické specificky pro skupinu malých e-shopů.

Z pohledu implementace GDPR lze za kritické uvažovat obecné charakteristiky malých podniků, a totiž finanční a znalostní bariéry. Ty mají přímý vliv na přístup k implementaci GDPR – prioritizaci dané problematiky v organizaci, rozpočet na implementaci a nižší rozsah implementace v synergii s nedostatečnými znalostmi dané problematiky v organizaci. Tyto poznatky lze sledovat jak v rámci provedené literární rešerše a vícenásobné případové studie, tak provedeným dotazníkovým šetřením.

Druhou skupinou faktorů ovlivňujících implementaci GDPR v prostředí malých e-shopů jsou ty, které byly specificky sledovány v rámci provedeného dotazníkového šetření. Statisticky významný vliv na implementaci má situace, kdy e-shop prodává své zboží do zahraničí, konkrétně do evropských zemí, které nejsou členským státem EU. Zde se ovšem může jednat o současně vyšší incidenci certifikace ISO 9000.

Zjevný dopad na implementaci GDPR pak má v případě malých e-shopů dále externí spolupráce při implementaci, k čemuž vzhledem k výše uvedeným obecným charakteristikám MSP dochází jen méně často. Třetím faktorem ovlivňujícím implementaci GDPR je povaha zpracovávaných dat, kdy zpracování zvláštních kategorií OÚ má dle nařízení vést k vyšší ochraně údajů. V kontextu malých e-shopů se zpravidla jedná o častější provádění činností týkající se systematického přístupu k implementaci a činností týkající se prokazování implementace GDPR nebo opatření organizačního charakteru.

Zhodnocení souvislostí mezi implementací GDPR a managementem rizik

Třetím výzkumných cílem této disertační práce bylo zkoumání souvislostí mezi implementací GDPR a oblastí řízení rizik. K popsání a zhodnocení souvislostí bylo využito vícero nástrojů, a to od teoretického vymezení existujícího vztahu, po rešerši v soudobé literatuře až po empirické sledování tohoto vztahu případovou studií a dotazníkovým šetřením.

Empirická šetření vycházela ze dvou základních teoretických východisek:

- Lepší praktiky RM povedou ke kvalitní implementaci GDPR
- Implementace GDPR (zahrnující činnosti týkající se RM) povede k rozvoji praktik RM

Tento možný vztah byl dále sledován jak v rámci kvalitativního, tak kvantitativního šetření. V rámci kvalitativních zjištění lze tento vztah u malých e-shopů zhodnotit jen do té míry, že v důsledku implementace GDPR je vyšší pozornost věnována dalším

regulatorním rizikům. Ovšem bez dalšího rozvoje praktik RM v organizaci, které lze i na podkladu provedeného dotazníkové šetření soudit nadále jako převážně nevyspělé.

V případě kvantitativního zhodnocení vztahu mezi sledovanými oblasti byla zjištěna slabá pozitivní korelace. U skupiny malých e-shopů tak lze sice sledovat vzájemné působení obou proměnných, na druhé straně jak vyspělost RM, tak implementace GDPR je u této skupiny ovlivněna širších spektrem faktorů (viz například kap. 6.2.3. nebo 6.2.4).

Výrazněji se pak na základě měření tento vztah projevuje u e-shopů, které prodávájí své zboží také do evropských zemí mimo EU při současné vyšší incidencí certifikace ISO 9000.

8 Přínosy a doporučení

Přínosy a doporučení vyvozená ze zpracovávané disertační práce lze rozdělit do čtyřech různých kategorií. Přínosů a doporučení pro **oblast akademickou**, **pedagogickou**, pro **praxi podniků**. Přínosem práce pak mohou být kromě doporučení pro oblast ekonomiky a managementu vybrané skupiny společností i směr doporučení pro **moc výkonnou a zákonodárnou**.

Přínosy a doporučení pro akademickou oblast

S ohledem na platný a stále ještě relativně nový legislativní rámec ochrany osobních údajů disertační práce shrnuje pro akademickou sféru současné poznání v oblasti výzkumu dopadů GDPR na klíčové činnosti a oblasti a RM podniků, potažmo řízení podniků obecně, kdy do současného poznání jsou kromě zdrojů akademické literatury uvažovány i zdroje neakademické (komerční a veřejné). Samotné současné poznání tak souhrnně popisuje znalosti v těchto oblastech:

- Konkretizace vztahu mezi implementací GDPR a řízením klíčových činností podniku
- Konkretizace vztahu mezi GDPR a managementem rizik
- Vymezení a souhrn klíčových a podpůrných činností, vůči kterým má GDPR a jeho implementace dopad
- Konkretizace dopadů na řízení výše zmapovaných činností a oblastí podniku
- Zmapování teoretických přístupů vedoucích k implementaci
- Vymezení a souhrn aktivit, jež je třeba k implementaci provést
- Specifika implementace v prostředí malých podniků

Takto shrnuté výsledky jsou dále verifikovány, doplněny a rozšířeny o výsledky vlastního empirického šetření v aplikované oblasti malých e-shopů v České republice, a to především doplněním o další existující dopady na činnosti podniku, vymezením přístupu k implementaci u této skupiny podniků a kvalitativní i kvantitativnímu zhodnocení implementace GDPR a popsání a zhodnocení souvislostí mezi implementací GDPR a managementem rizik.

Obecně provedený disertační výzkum přispívá do současného poznání novými poznatky v těchto výzkumných oblastech:

- **GDPR, ochrana osobních údajů, potažmo ochrana soukromí**
- **Management rizik a modely vyspělosti RM**
- **Řízení malých podniků a řízení e-shopů**

V širším kontextu tato práce volně navazuje a je podkladem pro další zkoumání dopadů platných legislativních opatření na řízení podniků.

Disertačním výzkumem získané poznatky nastiňují i doporučení pro v budoucnu potenciálně prováděné výzkumy v oblasti zkoumání dopadů GDPR na podnikové procesy a podniky obecně, stejně jako výzkumy v oblasti managementu rizik. Jeden ze směrů dalšího výzkumu by se měl zaměřit na další rozšíření současného poznatků v této oblasti implementace GDPR, kdy vlivu nařízení na podniky je věnována poměrně krátká doba posledních pěti let.

Konkrétně by se mohlo jednat o navazující výzkum dopadů implementace GDPR z hlediska vyčíslení nákladů jednotlivých dopadů, stejně jako popisu zmapovaných dopadů na základě dalších charakteristik (pracnost, časová perspektiva, identifikace potřebných znalostí a schopností apod.).

Další část zkoumání by se pak měla v podobném duchu věnovat i samotné implementaci GDPR, a to:

- činnostem implementace (vyčíslení nákladů na jednotlivé činností, pracnosti jednotlivých činností apod.)
- zkoumání dalších faktorů, které ovlivňují implementaci GDPR
- definici best-practices pro implementaci GDPR a zajišťování soukromí zákazníků

Další část zkoumání by se pak měla věnovat komparaci dopadů v různých prostředích, a to dle odvětví či velikosti organizace, kde i již na základě předchozích šetření autora (Faifr & Januška, 2021) byly na základě těchto faktorů sledovány rozdíly v přístupech k implementaci, stejně jako v různých právních prostředích (zemích), kdy vliv na přístupy k implementaci a ochraně osobních údajů má faktor národních autorit a vymahání požadavků regulace v daném prostředí (Custers et al., 2018). Výstupy z provedených šetření by mohly přispět k uceleným doporučením a metodickým přístupům k implementaci pro podnikatelské subjekty.

Přínosy a doporučení pro pedagogickou oblast

Výstupy disertační práce mohou být využity pro výuku předmětů, které se zabývají řízením podniků, kdy GDPR je nedílným aspektem řízení všech firem, které zpracovávají, byť v minimální míře, osobní údaje občanů EU. Širší a konkrétní uplatnění pak naleznou výstupy této práce v předmětech s vazbou na řízení podnikových procesů, řízení rizik a předměty zabývající se řízením malých podniků a on-line podnikání.

Výstupy této práce již na Fakultě ekonomické Západočeské univerzity v Plzni například nalezly své uplatnění při výuce předmětu Management znalostí, inovací a rizik. Vzhledem k povaze této disertační práce mohou být její výstupy podkladem pro teoretické zpracování bakalářských a diplomových prací, což se v současnosti (rok 2023) již rovněž děje.

Přínosy a doporučení pro praxi

Provedený výzkum má deskriptivní charakter, jeho zamýšleným obecně formulovaným výstupem je tedy obecné popsání současné reality malých e-shopů s ohledem na implementaci GDPR a management rizik. I přesto z provedeného výzkumu vyplývají přínosy pro podnikovou praxi.

Za první přínos práce je ve vazbě na řízení podniků považována sumarizace současného jak akademického, tak „komerčního“ poznání v oblasti implementace GDPR a jeho dopadů na činnosti podniku, kdy součástí výstupů je mimo jiné přehled dotčených klíčových i podpůrných činností, sumarizace možných dopadů na tyto činnosti, stejně jako na obecné procesní prostředí. Dále pak práce sumarizuje všechny aktivity, jež jsou v rámci implementace prováděny. V obou případech mohou podniky s ohledem na vlastní kontext při plánování a realizaci implementačního projektu vycházet. Získané výsledky šetření pak mohou rovněž nejen u skupiny malých e-shopů sloužit jako nástroj pro srovnání vlastních provedených činností v rámci implementace GDPR a identifikaci případných nedostatků v implementaci.

Vůči zkouma

né skupině malých e-shopů lze definovat i konkrétní doporučení pro oblasti ochrany osobních údajů a managementu rizik:

- Obecná **revize provedené implementace GDPR** z hlediska možných nedostatků, a to i s ohledem na další možné pozitivní synergické efekty (zlepšení podnikových praktik či zvýšení důvěryhodnosti z pohledu zákazníka)
- I s uvažením existujících bariér u skupiny malých e-shopů **oslovení expertů v oblasti zajišťování soukromí** s cílem zvýšit kvalitu ochrany osobních údajů
- **Systematický přístup k řízení rizik** s ohledem na možné negativní důsledky vyplývající nejen z regulatorních rizik

Doporučení pro výkonnou moc

Zamýšleným přínosem práce jsou i doporučení vůči moci zákonodárné či výkonné, kdy, jak z dílčích zjištění vyplývá, nemusí současný právní a výkonný rámec vést nejen v případě malých e-shopů k naplňování účelu platné regulace.

Je-li cílem GDPR chránit osobní údaje občanů EU, a to prostřednictvím jednotné regulace a jejím vymáhání na jedné straně a plněním z nařízení vyplývajících požadavků ze strany (nejen) podnikatelských subjektů na straně druhé, pak jak z dosavadního poznání v této oblasti vyplývá, především správná implementace v kategorii malých podniků může narážet na řadu objektivních limitů, jež v konečném důsledku naplnění podstaty nařízení brání. Jedná se především o nízké znalosti v oblasti zajišťování ochrany OÚ a omezené finanční možnosti požadavky nařízení případně plnit i ve spolupráci externích subjektů.

Doporučení pro výkonnou a zákonodárnou moc pak mohou být definována rámcově takto:

- Poskytnutí možnosti proplacení části nákladů na poradenství v oblasti ochrany OÚ a implementace GDPR[79]
- Poradenství v oblasti implementace GDPR pro MSP[80]
- Zpracování metodiky postupu implementace GDPR odpovídající kontextu MSP (především znalostem problematiky ve sledované skupině)[81]

[79] Obdobným způsobem, jako se již například děje v případě proplacení nákladů na poradenství v oblasti duševního vlastnictví (Úřad průmyslového vlastnictví, 2023).

[80] ÚOOÚ v současnosti poskytuje možnost konzultace týkající se ochrany osobních údajů. Jak ale z vyjádření úřadu vyplývá, je konzultační činnost poskytována zejména DPO při implicitně předpokládané pokročilé úrovni znalostí problematiky ochrany OÚ (ÚOOÚ, 2023b).

[81] Příručky a manuály dedikované malým a středním podnikům například MPO (2018a, 2018b). Oba materiály dle vyjádření v dokumentech ovšem poskytuji pouze základní vzhled do dané problematiky a zároveň implikují využití externích služeb.

Závěr

Zajišťování soukromí se v posledních letech stalo běžným aspektem řízení nejen evropských firem. Svůj podíl na tomto má i Obecné nařízení o ochraně osobních údajů (GDPR), které vešlo v platnost před třemi lety a které musí být v evropském hospodářském prostoru dodržováno (EP & EUC, 2016). I bez takto přijaté regulace se ovšem stává soukromí důležitým aspektem v rozhodovacím procesu zákazníka (Bakhoum et al., 2018; Bleier et al., 2020; Martin et al., 2020), který je novými legislativní požadavky dále zvýrazněn. Kromě EU i ostatní státy světa již přistupují k přísnějšímu režimu v oblasti kontroly a ochrany dat (Bleier et al., 2020; Annant et al., 2020), jejichž důsledky ve velké míře pociťují organizace, které data zpracovávají.

Již v úvodu této práce byla definována existující výzkumná mezera v tom, jaký dopad na řízení podniků mají nová legislativní opatření obdobná GDPR, pokud v případě jmenované regulace platí, že implementace vyžaduje dostatečné množství znalostí a různých typů zdrojů, stejně jako nově závaděných praktik, které si ovšem ne všechny organizace, a především pak firmy malé, dokáží osvojit. V tomto ohledu byl definován i cíl této disertační práce, který je zaměřen na skupinu malých podnikatelských subjektů podnikajících na internetu (malé e-shopy). S ohledem na tento výzkumný problém byl sestaven návrh výzkumu zakotvující strategii smíšeného výzkumu s ambicí blíže prozkoumat dopady na klíčové činnosti e-shopu v důsledku platnosti a implementace GDPR v podnicích.

V rámci již realizovaných výzkumných šetření byla provedena systematická literární rererše. S cílem, kromě vymezení současného poznání v oblasti dopadů implementace GDPR, pochopit i současné chování podnikatelských subjektů na trhu, byla v rámci systematické rešerše provedena i rešerše zdroju šedé literatury (Paez, 2018), které jsou pro implementaci komerčními subjekty využívány zpravidla častěji (Briner & Denyer, 2012). Výsledky systematické rešerše tak zahrnují syntézu poznání jak v oblasti akademické, tak komerční a veřejné.

Shrnuté teoretické poznatky pak byly využity k upřesnění designu následně provedené vícenásobné případové studie, která kombinuje poznatky a zkušenosti praxe třech českých malých e-shopů. Získané poznatky zároveň empiricky rozšiřují znalosti v oblasti dopadů GDPR na realitu řízení podnikových procesů.

Poslední částí disertačního výzkumu bylo na základě teoretických východisek i dílčích poznatků předchozích výzkumných šetření bližší popis vztahu mezi GDPR a řízením rizik, jakožto procesem, který je v nařízení explicitně uveden a jehož dílčí aktivity jsou během samotné implementace rovněž uvažovány (EP & EUC, 2016). Poslední část výzkumu se proto věnovala souvislostem mezi oběma těmito oblastmi. Prvním sledovaným efektem je možný pozitivní dopad managementu rizik malého e-shopu na rozsah implementace GDPR. Druhým efektem pak je možná adopce managementu rizik v důsledku implementace, tedy rozšíření dovedností organizace v důsledku plnění požadavků regulatorních opatření. Na základě provedeného měření byla zjištěna slabá pozitivní korelace mezi sledovanými proměnnými, přičemž byly dále zkoumány charakteristiky, které mohou mít na sílu tohoto vztahu vliv. Kromě zkoumání souvislostí mezi zmíněnými oblastmi poskytuje závěrečné dotazníkové šetření informaci o rozsahu implementace GDPR mezi malými e-shopy, stejně jako informaci o vyspělosti těchto podniků v oblasti řízení rizik, a to včetně možných ovlivňujících faktorů.

Přínosy vyplývající ze zpracované disertační práce byly podrobně uvedeny v předchozí kapitole 8. Předpokládaná významnost práce spočívá především v rozšíření teoretických i empirických znalostí v problematice, jež má své důsledky nejen pro téměř každou evropskou firmu, ale také vysoký počet mimoevropských subjektů, které zpracovávají osobní údaje, byť zcela minimálního počtu, občanů Evropské unie (FRA & Rada Evropy, 2018). Výstupy této práce shrnují a rozšiřují poznatky v oblasti dopadů implementace GDPR na klíčových činností, které naleznou své uplatnění i mimo skupinu primárně zkoumaných malých e-shopů.

Na druhé straně je návrh výzkumu i dílčích šetření spojen s některými omezeními, a to s ohledem na fakt, že se jedná o výzkum prováděný pouze na území České republiky a u pouze specifické skupiny organizací. Limity dílčích výzkumných šetření jsou uváděny vždy v závěru příslušné kapitoly. Obecně z hlediska teritoriálních limitů je třeba následně výsledky výzkumu vnímat i z pohledu různého legislativního kontextu ostatních, nejen evropských zemí (Custers et al., 2018). Druhou obecnou limitací tohoto výzkumu pak je výběr zkoumaných činností, kdy rozsah zkoumaných činností je omezen a bližšímu zkoumání bylo podrobeno pouze řízení rizik (Voigt & von dem Bussche, 2017; Sharma, 2020).

V kapitole 8 autor definoval přínosy a doporučení pro oblast akademickou, pedagogickou a praxi. Doporučení autora vůči oblasti akademické jsou definované jako doporučení pro navazující výzkum zkoumané problematiky. Svůj význam dle autora této disertační práce by mohl mít i výzkum dopadů jiných přijímaných regulací, které jakožto externí faktor mají vliv na principy a přístupy, s jakými jsou řízeny podnikové procesy.

Publikační činnost autora

Faifr, A. (2022). Případová studie implementace GDPR v malém e-shopu. In *Sborník příspěvků konference Trendy v podnikání 2022.* Plzeň: Západočeská univerzita v Plzni.

Faifr, A. & Januška, M. (2021). Factors determining the extent of GDPR implementation within organizations: Empirical evidence from Czech republic. *Journal of Business Economics and Management, 22(5), 405-422.* https://doi.org/10.3846/jbem.2021.15095

Januška, M. & **Faifr, A.** (2021). Evaluation of Framework Conditions Supporting Young Innovators in Central Europe. *Ekonomický časopis/Journal of Economics, 69(4),* s. 405–422. https://doi.org/10.31577/ekoncas.2021.04.04.

Faifr, A. (2020). Use of Project Management Maturity Models as a Evaluation Framework for Project Risk Maturity Assessment. In *DOKBAT 2020 - 16th International Bata Conference for Ph.D. Students and Young Researchers*. Zlín: Tomas Bata University in Zlín, Faculty of Management and Economics, 2020, s. 123-138.

Faifr, A., Stehlík, M., Kick, M. & Lindemann, J. (2019). Competencies of graduates with regards to industry 4.0. In *International Cross Cultural Projects in Human Resource Management*. Plzeň, s.80-99.

Faifr, A. & Januška, M. (2018). Companies' readiness of GDPR and implementation barriers. In *Proceedings of the 41st International Academic Conference*. Prague : International Institute of Social and Economic Sciences, 2018, s.31-49.

Čech, M., Januška, M. & **Faifr, A.** (2018). Using Self-Assessment Tool as Part of Risk Management Maturity Model. In *Proceedings of the 32nd International Business Information Management Association Conference (IBIMA)*. Sevilla : IBIMA, s.3262-3285.

Januška, M., Čech, M. & **Faifr, A.** (2018). Development of Broadband in SEE Territory through Public Private Partnership Concept. In *Proceedings of the 32nd International Business Information Management Association Conference (IBIMA)*. Sevilla : IBIMA, 2018, s.606-622.

Januška, M. & **Faifr, A**. (2017). Optimization of the in-process control process using Six sigma methods and tools. In *Proceedings of the 28th DAAAM International Symposium*. Vienna : DAAAM International, s.280-288.

Januška, M. & **Faifr, A**. (2016). Project Quality Management Lifecycle: A Case Study of the Commencement of Insulin Pen Mass Production. In *Proceedings of the 26th DAAAM International Symposium*. Viena. DAAAM International, s.343-349.

Seznam použitých zdrojů

Aba-bulgu, M. & Islam, S.M.N. (2006). *Corporate Crisis and Risk Management: Modelling, Strategies and SME Application (International Business and Management 21).* Elsevier Ltd.

Ackermann, T. (2013). *IT Security Risk Management: Perceived IT Security Risks in the Context of Cloud Computing*. Springer Gabler. https://doi.org/10.1007/978-3-658-01115-4

Adams, R.J., Smart, P. & Huff, A.S. (2017). Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies. *International Journal of Management Reviews*, 19, 432-454. https://doi.org/10.1111/ijmr.12102

Agentura Evropské unie pro základní práva [FRA] & Rada Evropy (2018). *Handbook on European data protection law* (2018 edition). Dostupné 4.5.2021 z https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

Alford, S. (2020). GDPR: *A Game of Snakes and Ladders. How Small Business Can at the Compliance Game*. Taylor & Francis Group.

Ambroise, L. & Prim-Allaz, I. (2017). Reputation Risk: Anticipation and Management Reputation Failure. In Bérard, C. & Teyssier, C. (Eds), *Risk Management: Lever for SME Development and Stakeholder Value Creation (65-84).* John Wiley & Sons, Inc.

Andersen, TJ. (2008). The Performance Relationship of Effective Risk Management: Exploring the Firm-Specific Investment Rationale. *Long Range Planning*, 41(2), 155-176. https://dx.doi.org/10.1016/j.lrp.2008.01.002

Andersen, TJ. (2016). *The Routledge Companion to Strategic Management*. Taylor & Francis Group.

Anderson, E.J. (2013). *Business Risk Management: Models and Analysis*. John Wiley & Sons Ltd.

Anic, I-D., Škare, V. & Milaković, I.K. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications*, 36. https://doi.org/10.1016/j.elerap.2019.100868

Antonucci, D. (2016). *Risk Maturity Models: How to assess risk management effectiveness*. Kogan Page Limited.

Annant, V., Donchak, L., Kaplan, J. & Soller, H. (2020). *The consumer-data opportunity and the privacy imperative*. McKinsey.com. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Asociace pro elektronickou komerci [APEK]. (2023a). *Studie: Přínosy e–commerce v ČR*. Dostupné 3.2.2023 z https://data.apek.cz/

Asociace pro elektronickou komerci [APEK]. (2023b). *On-line prodeje v roce 2022 klesly o 12 %, e-shopy se vyrovnávají s prvním propadem v historii*. Dostupné 3.2.2023 z https://www.apek.cz/clanky/on-line-prodeje-v-roce-2022-klesly-o-12-e-shopy

Asociace pro elektronickou komerci [APEK]. (2023c). *Seznam členů*. Dostupné 28.7.2023 z https://www.apek.cz/seznam-clenu

Asociace pro elektronickou komerci [APEK]. (2023d). *APEK Vzorové obchodní podmínky*. Dostupné 28.9.2023 z https://www.apek.cz/vzorove-obchodni-podminky-apek

Aureli, S., & Salvatore, F. (2013). The current state of Risk Management in Italian Small and Medium-sized entrerprises. *Proceedings of the 8th International Conference Accounting and Management Information Systems AMIS 2013*. Bucharest (Romania). http://doi.org/10.6092/unibo/amsacta/3947

Baak, M., Koopman, R., Snoek, H. & Klous, S. (2020). A new correlation coefficient between categorical, ordinal and interval variables with Pearson characteristics. *Computational Statistics & Data Analysis*, 152. https://doi.org/10.1016/j.csda.2020.107043

Baily, P., Farmer, D., Crocker, B. & Jessop, D. (2022). Procurement principles and management in the digital age. Twelfth edition. Pearson.

Bakhoum, M., Gallego, B.C., Mackenrodt, M.O. & Surblyté-Namavičiené, G. (2018). *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*. Springer Nature. https://doi.org/10.1007/978-3-662-57646-5

Banerjee, S., Xu, S. & Johnson, S.D. (2020). How does location based marketing affect mobile retail revenues? The complex interplay of delivery tactic, interface mobility and user privacy. *Journal of Business Research*, 130, 398-404. https://doi.org/10.1016/j.jbusres.2020.02.042

Barafort, B. Mesquida, A.-L. & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. Computer Standards & Interfaces, 54(3), 176-185. https://doi.org/10.1016/j.csi.2016.11.010

Barth, S., de Jong, M.D.T., Junger, M., Hartel, P.H. & Roppelt, J.C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41, 55-69. https://doi.org/10.1016/j.tele.2019.03.003

Bashir, M., Hayes, C, Lambert, A.D. & Kesan, J.P. (2016). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, 52(1), 1-10. https://doi.org/10.1002/pra2.2015.145052010043

Baxter, R., Bedard, J.C. Hoitash, R. & Yezegel, A. (2013). Enterprise Risk Management Program Quality: Determinants, Value Relevance, and the Financial Crisis. *Contemporary Accounting Research*, 30(4), 1264-1295. https://doi.org/10.1111/j.1911-3846.2012.01194.x

Beckett, P. (2017). GDPR compliance: your tech department's next big opportunity. *Computer Fraud & Security*, 2017(5), 9-13. https://doi.org/10.1016/S1361-3723(17)30041-6

Benjamin, A.S. (2017). *Enterprise Risk and Opportunity Management*. John Wiley & Sons, Inc.

Bérard, C. & Teyssier, C. (2017). *Risk Management: Lever for SME Development and Stakeholder Value Creation*. John Wiley & Sons, Inc.

Bititci, U. (2015). *Managing Business Performance: The Science and the Art*. John Wiley & Sons.

Bizmachine. (2023). *Přítomnost e-shopů na srovnávačích.* Dostupné 28.7.2023 z https://www.lupa.cz/clanky/e-shopu-je-v-cesku-vic-nez-se-rika-vetsina-ma-obrat-do-20-milionu-a-petina-neni-na-srovnavacich/

Bleier, A., Goldfarb, A. & Tucker, C. (2020). Consumer privacy and the future of data-based Innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466-480. https://doi.org/10.1016/j.ijresmar.2020.03.006

Booch, G., Rumbaugh, J. & Jacobson, I. (2005). Unified Modeling Language User Guide. *Addison-Wesley Professional*.

Bracanović, T. (2018). Predictive analytics, personalized marketing and privacy. *Revue Roumaine de Philosophie*, 63(2), 263-275.

Brin, S. & Page, L. (1998). *The Anatomy of a Large-Scale Hypertextual Web Search Engine*. Stanford University, Stanford, Spojené státy Americké. http://infolab.stanford.edu/~backrub/google.html

Briner, R.B. & Denyer, D. (2012). *Systematic Review and Evidence Synthetis as a Practice and Scholarship Tool*. In Rousseau, D.M., *The Oxford Handbook of Evidence-Based Management*. Oxford Library of Psychlogy. http://dx.doi.org/10.1093/oxfordhb/9780199763986.013.0007

Bindley, P. (2019). Joining the dots: how to approach compliance and data governance. *Network Security*, 2, 14-16. https://doi.org/10.1016/S1353-4858(19)30023-6

Bissonette, M.M. (2016). *Project Risk Management: A Practical Implementation Approach*. Project Management Institute, Inc.

Brustbauer, J. (2016). Enterprise risk management in SMEs: towards a structural model. *International Small Business Journal*, 34(1), 70–85. https://doi.org/10.1177/0266242614542853

Bureau Van Dijk. (2023). *Export-31-07-2023*. Interní report Bureau Van Dijk (nepublikováno)

Cloarec, J. (2020). The personalization-privacy paradox in the attention economy. *Technological Forecasting and Social Change*. 2020, 161. https://doi.org/10.1016/j.techfore.2020.120299

Crawford, J.K. (2014). *Project Management Maturity Model* (3rd ed.). CRC Press

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.), SAGE Publications, Inc.

Crovini, C. (2019). *Risk Management in Small and Medium Enterprises*. Routledge Taylor & Francis.

Crovini, C. Ossola, G. & Britzelmaier, B. (2021). How to reconsider risk management in SMEs? An Advanced, Reasoned and Organised Literature Review. *European Management Journal*, 39(1). 118-134. https://doi.org/10.1016/j.emj.2020.11.002

Custers, B., Dechesne, F., Sears, A. M., Tani, T., & van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review, 34(2), 234–243*. https://doi.org/10.1016/j.clsr.2017.09.001

CzechCrunch s.r.o. (2023). *Česká e-commerce v datech*. Dostupné 5.9.2023 z https://cc.cz/ecommerce-2023/data/

Čegan, J. (2019). *Harmonizace systému managementu bezpečnosti informací a práce s utajovanými skutečnostmi* (Diplomová práce). Masarykova Univerzita, Fakulta informatiky, Česká republika

Čech, M., Januška, M. & Faifr, A. (2018). Using Self-Assessment Tool as Part of Risk Management Maturity Model. *Proceedings of the 32nd International Business Information Management Association Conference (IBIMA)*, 3262 - 3285.

Čech, M. & Januška, M. (2020). Evaluation of Risk Management Maturity in the Czech Automotive Industry: Model and Methodology. *Amfiteatru Economic*, 22(55), 824-845. http://dx.doi.org/10.24818/EA/2020/55/824

Čermák, M. (2009). *Řízení informačních rizik v praxi (1. vydání)*. Tribun EU.

Česká obchodní inspekce (2022). Novela zákona o ochraně spotřebitele. Dostupné 21.7.2023 z https://www.coi.cz/novela-zakona-o-ochrane-spotrebitele/

Český statistický úřad [ČSÚ]. (2019). *Evropská unie je rájem e-shopů*. Dostupné 3.2.2023 z https://www.czso.cz/csu/stoletistatistiky/evropska-unie-je-rajem-e-shopu

Český statistický úrad [ČSÚ]. (2023). *Klasifikace ekonomických činností (CZ-NACE) - systematická část*. Dostupné 2.9.2023 z https://www.czso.cz/documents/10180/23174387/85048625.xls/30885b22-9bac-4c7a-ad2c-5db96e69ea24?version=1.0

Da Costa Lewis, N. (2012). *The Fundamental Rules of Risk Management*. CRC Press, Taylor & Francis Group.

Dammann, U. & Simitis, S. (1997). *EG-Datenschutzrichtlinie, Kommentar*. Nomos.

Deloitte Touche Tohmatsu Limited (2013). *Global risk management survey, eight edition. Setting a higher bar*. Dostupné 2.5. 2021 z https://fek.zcu.cz/blob.php?table=internet_list&type=FileType&file=Data&name=FileName&idname=IDInternet&id=3532

Dessler, G. (2020). Human Resource Management. *Pearson Education Limited, Harlow, New York.*

Dickinson, G. (2001). Enterprise risk management: its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 26, 360 – 366. https://link.springer.com/content/pdf/10.1111/1468-0440.00121.

Dionne, G. (2013). Risk Management: History, Definition, and Critique'. *Risk Management and Insurance Review*, 16(2), 147–166. https://doi.org/10.1111/rmir.12016

Diamantopoulou, V., Tsohou, A. & Karyda, M. (2020). From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls. *Information and Computer Security*, 28(4), 645-662. https://doi.org/10.1108/ICS-01-2020-0004

Dillman, D.A., Phelps, G., Tortora, R., Swift, K., Kohrell, J., Berck, J. & Messer, B.L. (2009). Response rate and measurement differences in mixed-mode surveys using mail, telephone, interactive voice response (IVR) and the Internet. *Social Science Research, 38(1), 1-18*. https://doi.org/10.1016/j.ssresearch.2008.03.007

Dinno, A. (2015). Nonparametric pairwise multiple comparisons in independent groups using Dunn's test. *Stata Journal, 15(1), 292-300*. https://doi.org/10.1177/1536867X150150011

Dörr, D. & Weaver, R.L. (2014). *Perspectives on Privacy: Increasing regulation in the USA, Canada and European countries*. De Gruyter.

Durst, S., Hinteregger, C. & Zieba, M. (2019). The linkage between risk management and organizational performance. *Journal of Business Research*, 105, 1-10. https://doi.org/10.1016/j.jbusres.2019.08.002

Ecorys (2012). *EU SMEs in 2012: at the crossroads, Annual report on small and mediumsized enterprises in the EU*. Dostupné 7.5.2021 z https://ec.europa.eu/docsroom/documents/16106/attachments/1/translations/en/renditions/native

Eger, L. & Egerová, D. (2014). *Základy metodologie výzkumu pro studenty ekonomických oborů.* Západočeská Univerzita v Plzni. Česko.

Ekwere, N. (2016). Framework of Effective Risk Management in Small and Medium Enterprises (SMEs): a Literature Review. *Business*. https://doi.org/10.26593/BE.V20I1.1894.23-46

El Fikri, M., Putra, F.A., Suryanto, Y. & Ramli, K. (2019). Risk Assesment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Techniques in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. *Procedia Computer Science*, 161, 1206-1215. https://doi.org/10.1016/j.procs.2019.11.234

Elmaallam, M. & Kriouile, A. (2011). Towards a model of Maturity for is IS Risk management. *International Journal of Computer Science & Information Technology (IJCSI*T), 3(4). http://dx.doi.org/10.5121/ijcsit.2011.3414

European Data Protection Supervisor. (n.d.a). Privacy by Design. Dostupné 3.2.2023 z https://edps.europa.eu/data-protection/our-work/subjects/privacy-design_en

European Data Protection Supervisor. (n.d.b). The History of the General Data Protection Regulation. Dostupné 3.2.2023 z https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Eurostat. (2013). Glosary: Business Functions. *Dostupné 3. 10. 2023 z https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Business_functions*

Eurostat. (2015). Glosary: E-commerce. *Dostupné 3. 2. 2023 z http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:E-commerce*

Eurostat (2023). Glossary: E-commerce. Evropská Komise. *Dostupné 21.7.2023 z https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:E-commerce*

Evropská komise [EC]. (2012). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. https://web.archive.org/web/20121203024154/http://ec.europa.eu/justice/data-protection/document/review2012/com_20(12_11_en.pdf

Evropská komise [EC]. (2019a). *Uživatelská příručka k definici malých a středních podniků*. Dostupné 15.5.2022 z https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1/language-cs

Evropská komise [EC]. (2019b). *Special Eurobarometer 487a: The General Data Protection Regulation (SUMMARY)*. Dostupné 3.6. 2022 z

https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/06/ebs487a_en.pdf

Evropská komise [EC] (2020). *Druhy právních předpisů EU*. Dostupné 7.5.2021 z https://ec.europa.eu/info/law/law-making-process/types-eu-law_cs

Evropský parlament & Rada Evropské unie [EP & EUC]. (1995). *SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob vsouvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Dostupné 6.5.2021 z* https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:31995L0046&from=EN

Evropský parlament & Rada Evropské unie [EP & EUC]. (2016). *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. Dostupné 26.7.2022 z https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

Evropský parlament & Rada Evropské unie [EP & EUC]. (2017). *Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).* Dostupné 27.1.2023 z https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52017PC0010&from=CS

Faifr, A. & Januška, M. (2018). Companies' readiness of GDPR and implementation barriers. *Proceedings of the 41st International Academic Conference*. International Institute of Social and Economic Sciences, 31-49. http://dx.doi.org/10.20472/IAC.2018.041.013

Faifr, A. (2020). *Use of Project Management Maturity Models as a Evaluation Framework for Project Risk Maturity Assessment*. In DOKBAT 2020 - 16th International Bata Conference for Ph.D. Students and Young Researchers. Zlín. Tomas Bata University in Zlín, Faculty of Management and Economics, 123-138.

Faifr, A. & Januška, M. (2021). Factors determining the extent of GDPR implementation within organizations: Empirical evidence from Czech republic. *Journal of Business Economics and Management*, 22(5), 1124-1141- https://doi.org/10.3846/jbem.2021.15095

Faifr, A. (2021). Soukromí zákazníka a jeho dopady na marketing organizací v kontextu implementace GDPR. *Západočeská univerzita v Plzni. (nepublikovaný text)*

Faifr, A. (2022). Případová studie implementace GDPR v malém e-shopu. In *Sborník příspěvků konference Trendy v podnikání 2022, Západočeská univerzita v Plzni, 74-87*.

Farrel, M. & Gallagher, R. (2019). Moderating influences on the ERM maturity-performance relationship. *Research in International Business and Finance*, 47, 616-628. https://doi.org/10.1016/j.ribaf.2018.10.005

Fernandes, A., Tarafdar, M. & Spring, M. (2021). The nature of IT use in temporary organizations. *The Journal of Strategic Information Systems*, 30(1). https://doi.org/10.1016/j.jsis.2021.101655

Ferreira de Araújo Lima, P., Crema, M. & Verbano, C. (2020). Risk management in SMEs: A systematic literature review and future directions. European Management Journal, 38(1), 78-94. https://doi.org/10.1016/j.emj.2019.06.005

Ferreira de Souza, T. & Gomes, C.F. (2015). Assessment of Maturity in Project Management: A bibliometric Study of Main Models. Procedia Computer Science, 55, 92-101. https://doi.org/10.1016/j.procs.2015.07.012.

Fox, S., Aranko, O., Hielala, J. & Vahala, P. (2020). Exoskeletons Comprehensive, comparative and critical analyses of their potential to improve manufacturing performance. *Journal of manufacturing technology management*, 31(6), 1261-1280. https://doi.org/10.1108/JMTM-01-2019-0023

Fraser, J. & Simkin, B.J. (2010). *Enterprise Risk Management*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118267080

Gal, M. S. & Aviv, O. (2020). The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 16(3), 349-391. https://doi.org/10.1093/joclec/nhaa012

Gao, H., Kim, J.Y.,Hussain, W., Iqbal, M., & Duan, Y. (2022). Intelligent Processing Practices and Tools for E-Commerce Data, Information, and Knowledge. *Springer*.

Garber, J. (2018). GDPR – compliance nightmare or business opportunity. *Computer Fraud & Security Review*, 2018(6), 14-15. https://doi.org/10.1016/S1361-3723(18)30055-1

Garousi, V., Felderer, M. & Mäntylä, M. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106, 101-121. https://doi.org/10.1016/j.infsof.2018.09.006

Gibson, D. & Igonor, A. (2020). *Managing Risk in Information Systems* (3rd edition). Jones & Bartlett Learning, LLC.

Girling, P.X., (2013). *Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework*. John Wiley & Sons, Inc., Hoboken, New Jersey.

Golbeck, J. (2020). *Taking Control of Your Personal Data*. The Great Courses.

González Fuster, G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. *Springer International Publishing Switzerland*. https://doi.org/10.1007/978-3-319-05023-2

Gray, D. (2009). *Doing research in the real world* (2nd ed.). SAGE Publishing Inc.

Green, P.E.J. (2016). *Enterprise Risk Management: A common Framework for the Entire Organization*. Elsevier, Inc.

Gusenbauer, M. & Haddaway, N. (2020). Which Academic Search Systems are Suitable for Systematic Reviews or Meta-Analyses? Evaluating Retrieval Qualities of Google Scholar, PubMed and 26 other Resources. *Research Synthesis Methods*, 11(2), 181-217. https://doi.org/10.1002/jrsm.1378

Hall, R. (2020). *Mixing methods in social research: Qualitative, Quantitative and Combined Methods*. SAGE Publishing.

Hall, M. (2021). E-Commerce Management - A Simplified Guide to Manage Your Online Store Successfully. Independent.

Hamilton, R.H. & Sodeman, W.A. (2020). The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons*, 63(1), 85-95. https://doi.org/10.1016/j.bushor.2019.10.001

Hanáková, L. (2020). *The Impact of GDPR on Marketing and Protection of Customers´Personal Data*. DOKBAT 2020 - 16th International Bata Conference for Ph.D. Students and Young Researchers, 176-185. https://doi.org/10.7441/dokbat.2020.15

Hardy, K. (2014). *Enterprise Risk Management: A Guide for Government Professionals*. John Wiley & Sons, Inc.

Harkins, M.W. (2016). *Managing Risk and Information Security*. Apress Open.

Hassel, H. & Cedergren, A. (2021). Integrating risk assessment and business impact assessment in the public crisis management sector. *International Journal of Disaster Risk Reduction*, 56. https://doi.org/10.1016/j.ijdrr.2021.102136

Harrington, S.E. & Niehaus, G. (2004). *Risk management and insurance*. McGraw-Hill. Harris and Patten.

Hatto, P. (2013). Standards and standardisation: A practical guide for researchers. *European Commission, Publications Office of the European Union*.

Heinemann, G. (2023). The new online trade - Business models, business systems and benchmarks in e-commerce. *Springer*.

Helgesson, Y.Y. & Höst, M. & Weyns, K. (2012). A review of methods for evaluation of maturity models for process improvement. *Journal of Software Maintenance and Evolution Research and Practice*, 24(4). http://dx.doi.org/10.1002/smr.560

Helmond, M. (2022). Performance Excellence in Marketing, Sales and Pricing: Leveraging Change, Lean and Innovation Management. *Springer*

Hendl, J. (2005). *Kvalitativní výzkum: Základní metody a aplikace*. Portál.

Hendl, J. (2015). *Přehled statistických metod : analýza a metaanalýza dat*. Portál.

Henschel, T. & Durst, S. (2016). Risk management in Scottish, Chinese and German small and medium-sized enterprises: A country comparison. *International Journal of Entrepreneurship and Small Business*,29(1), 112-132. http://dx.doi.org/10.1504/IJESB.2016.078048

Henschel, T. (2010). Typology of risk management practices: an empirical investigation into German SMEs. *International Journal of Entrepreneurship and Small Business*, 9(3), 264–294. http://dx.doi.org/10.1504/IJESB.2010.031922

Hoekstra, R., Vugteveen, J., Warrens, M.J. & Kruyen, P.M. (2018). An empirical analysis of alleged misunderstandings of coefficient alpha. *International Journal of Social Research Methodology*, 22(4), 1-14. http://dx.doi.org/10.1080/13645579.2018.1547523

Hofman, D., Lemieux V. L. & Batista, D. (2019). The margin between the edge of the world and infinite possibility: Blockchain, GDPR and information governance. *Records Management Journal*, 29(1137). https://doi.org/10.1108/RMJ-12-2018-0045

Hoofnagle, C. J., Sloot, B. & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Hospodářská komora ČR. (2018). Účet za GDPR? Podnikatele nařízení vyjde na 25 miliard korun. Dostupné 22.2.2021 z https://www.komora.cz/press_release/ucet-za-gdpr-podnikatele-narizeni-vyjde-na-25-miliard-korun

Hoyt, R.E. & Liebenberg, A.P. (2011). The value of Enterprise Risk Management. *Journal of Risk and Insurance*, 78(4), 795-822. https://doi.org/10.1111/j.1539-6975.2011.01413.x

Hubbard, D.W. (2020). *The Failure of Risk Management: Why It´s Broken and How to Fix It (2nd ed.)*. John Wiley & Sons, Inc.

Hunziker, S. (2019). *Enterprise Risk Management: Modern Approaches to Balancing Risk and Reward*. Springer Gabler. https://doi.org/10.1007/978-3-658-25357-8

Chapman, R.J. (2019). Exploring the value of risk management for projects: improving capability through the deployment of a maturity model. *IEEE Engineering Management Review*, 47(1), 126-143. https://doi.org/10.1109/EMR.2019.2891494

Chih-Liang, Y. (2018). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*, 42(4), 282-292. https://doi.org/ 10.1016/j.telpol.2017.12.001

Choi, J.P., Jeon D-S. & Kim, B-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics, 173, 113-124*. https://doi.org/10.1016/j.jpubeco.2019.02.001

Chrissis, M.B., Konrad, M. & Shrum,S. (2013). CMMI for Development, Guidelines for Process Integration and Product Improvement. *Carnegie Mellon* (3. vydání).

Cowton, C.J. (1998). The use of secondary data in business ethics research. *Journal of Business Ethics*, 17(4)., 423-434. https://doi.org/10.1023/A:1005730825103

ICAEW (2005). *Risk management among SMEs, Executive report of discovery research*. Consultation & Research Centre of the Institute of Chartered Accountants in England and Wales. Dostupné 6.5.2021 z https://silo.tips/download/risk-management-among-smes

Information Commissioner´s Office (n.d.). The UK GDPR. Dostupné 27.10.2021 z https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/the-uk-gdpr

International Organization for Standardization [ISO] (2013). *ISO/IEC 19510:2013(en)*. Dostupné 3.2.2022 z https://www.iso.org/standard/62652.html

International Organization for Standardization [ISO] (2017). *ISO/IEC 27003:2017(en)*. Dostupné 3.5.2021 z https://www.iso.org/obp/ui/#iso:std:iso-iec:27003:ed-2:v1:en

International Organization for Standardization [ISO] (2018a). *ISO 31000 Risk Management*. Dostupné 3.5.2021 z https://www.iso.org/iso-31000-risk-management.html

International Organization for Standardization [ISO] (2018b). *ISO/IEC 27000:2018*. Dostupné 3.5.2022 z https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

Jaatinen, T. (2016). The relationship between open data iniciative, privacy, and government transparency: a love triangle? *International data privacy law*. 6, 28-38. https://doi.org/10.1093/idpl/ipv029

Jenkins, A. (2020). Guide to Inbound and Outbound Logistics: Processes, Differences and How to Optimize. *Oracle NetSuite*. Dostupné 21.7.2023 z https://www.netsuite.com/portal/resource/articles/inventory-management/inbound-outbound-logistics.shtml

Jesson, J.K., Matheson, L. & Lacey, F.M. (2011). *Doing Your Literature Review: Traditional and Systematic Techniques*. SAGE Publications Ltd.

Julien, P-A, Joyal, A., Deshaies, L. & Ramangalahy, C. (1996). A Typology of Strategic Behaviour among Small and Medium-Sized Exporting Businesses. A Case Study. *International Small Business Journal*, 15(2), 33-50. http://dx.doi.org/10.1177/0266242697152002

Kemell K.K., Wang X., Nguyen-Duc A., Grendus J., Tuunanen T. & Abrahamsson P. (2020). Startup Metrics That Tech Entrepreneurs Need to Know. In: Nguyen-Duc A.,

Münch J., Prikladnicki R., Wang X., Abrahamsson P. (eds) *Fundamentals of Software Startups*. Springer, Cham. https://doi.org/10.1007/978-3-030-35983-6_7

Kerzner, H. (2001). *Strategic Planning for Project Management using a project management maturity model.* New Jersey: John Wiley & Sons.

Keřkovský, M. & Vykypěl, O. (2006). *Strategické řízení: Teorie pro praxi* (2. vyd.). C.H.Beck

Khan, M.J., Hussain, D. & Mehmood, W. (2016). Why do firms adopt enterprise risk management (ERM)? Empirical evidence from France. *Management Decision*, 54(8), 1886-1907. http://dx.doi.org/10.1108/MD-09-2015-0400

Kindt, E. J. (2018). Having yes, using no? About the new legal regime for biometric data. *Computer Law & Security review*, 34(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Kirytopoulos, K., Leopoulos, V. & Malandrakis, C. (2001). Risk management: a powerful tool for improving efficiency of project oriented SMEs. *Proceedings of the 4th SMESME International Conference*, 331–339.

Kotler, P.T. & Armstrong, G. (2020). Principles of Marketing. *Pearson*.

Kouns, J. & Minoli, D. (2010). *Information Technology Risk Management in Enterprise Environments*. John Wiley & Sons., Inc.

Kounoudes, A. D. & Kapitsaki, G. M. (2020). A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet of Things*, 11. https://doi.org/10.1016/j.iot.2020.100179

Krafft, M., Arden, C.M. & Verhoef, P.C. (2017). Permission Marketing and Privacy Concerns – Why Do Customers (Not) Grant Permissions? *Journal of Interactive Marketing*, 39, 39-54. https://doi.org/10.1016/j.intmar.2017.03.001

Kraus, S., Breier, M. & Dasí-Rodriguez, S. (2020). The art of crafting a systematic literature review in entrepreneurship research. *International Entrepreneurship and Management Journal*, 16, 1023-1042. https://doi.org/10.1007/s11365-020-00635-4

Kuner, C., Bygrave, L.A. & Docksey, C. (2020). The EU General Data Protection Regulation (GDPR): A commentary. *Oxford University Press*.

Kunešová, H. & Eger, L. (2017). Evaluation and comparison of B2C e-commerce intensity in EU member states. *E & M EKONOMIE A MANAGEMENT*, 20(4), 151-167. https://doi.org/10.15240/tul/001/2017-4-011

Kunešová, H. (2017). *Vývoj B2C e-commerce v České republice a komparace se zeměmi EU* (Disertační práce). Západočeská univerzita v Plzni, Česká republika. https://theses.cz/id/464368/?lang=en

Lam, J. (2017). Implementing Enterprise Risk Management: From Methods to Applications. John Wiley & Sons, Inc.

Lark, J. (2015). *ISO 31000 Risk management, a practical guide for SMEs*. International Organization for Standardization

Larrucea, X., Moffie, M., Asaf, S. & Santamaria, I. (2020). Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Computer Standards & Interfaces*, 69. https://doi.org/10.1016/j.csi.2019.103408

Laudon, K.C. & Traver, C.G. (2022). E-commerce - business, technology and society. *Pearson*.

Libguides.com (2021). *Web of Science platform: Web of Science: Summary of Coverage*. Dostupné 11.5.2021 z https://clarivate.libguides.com/webofscienceplatform/coverage

Lindgren, P. (2018). GDPR Regulation Impact on Different Business Models and Businesses. *Journal of Multi Business Model Innovation and Technology*, 4(3), 241-254. https://doi.org/ 10.13052/jmbmit2245-456X.434

Longras, A., Pereira, T., Carneiro, P. & Pinto, P. (2018). On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations. *2018 International IEEE Conference on Intelligent Systems*, 1541-1672. https://doi.org/10.1109/IS.2018.8710558

Lueck, M. (2020). GDPR in the new remote-working normal. *Computer Fraud & Security*, 8, 14-16. https://doi.org/10.1016/S1361-3723(20)30086-5

MacGregor, R. & Vrazalic, L. (2007). E-commerce in Regional Small to Medium Enterprises. *IGI Publishing*.

Mahura, A. & Birollo, G. (2021). Organizational practices that enable and disable knowledge transfer: The case of a public sector project-based organization. *International Journal of Project Management. 39(3)*, 270 – 281. https://doi.org/10.1016/j.ijproman.2020.12.002

Mali, P. (n.d.). *GDPR Articles with Commentary & EU laws*. Cyber Infomedia.

Maňourová, M. (2019). *GDPR - Vyhodnocení dopadů GDPR na podniky v České republice* (Diplomová práce). Západočeské Univerzita v Plzni, Fakulta ekonomická, Česká republika

Martin, K.D. & Murphy, P.E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45, 135-155. https://doi.org/10.1007/S11747-016-0495-4

Martin, K.D., Kin, J., Palmatier, R.W., Steinhoff, L., Stewart, D.W., Walker, B.A., Wang, Y. & Weaven, S.K. (2020). Data Privacy in Retail. *Journal of Retailing*, 96(4), 474-489. https://doi.org/10.1016/j.jretai.2020.08.003

Maths and Stats Support Centre (n.d.). *Chí-kvadrát test v kontingenčních tabulkách*. Masarykova univerzita v Brně. Dostupné 20.10.2023 z https://mathstat.econ.muni.cz/media/19046/chikv.pdf

Merna T. & Al-Thani, F.F. (2007). *Risk management: řízení rizika ve firmě*. Brno, Computer Press.

McNiff, K. (2016). *What is Qualitative Research?* The NVivo Blog, QSR International. Dostupné 19.1.2023 z https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/resources/blog/what-is-qualitative-research

Mesquida, A. L. & Mas, A. (2015). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers & Security*, 48, 19-34. https://doi.org/10.1016/j.cose.2014.09.003

Meriah, I. & Ben Arfa Rabai, L. (2019. Comparative Study of Ontologies Based ISO 27000 Series Security Standards. Procedia Computer Science, 160, 85-92. https://doi.org/10.1016/j.procs.2019.09.447

Miles, J.G. (2021). E-Commerce Power. *Morgan James Publishing*.

Ministerstvo pro místní rozvoj České republiky [MMR] (2018). *Několik poznámek k GDPR v oblasti pohřebnictví*. Dostupné 8.2.2023 z https://www.mmr.cz/cs/ministerstvo/pohrebnictvi/aktuality/nekolik-poznamek-k-gdpr-v-oblasti-pohrebnictvi

Ministerstvo průmyslu a obchodu České republiky [MPO]. (2018a). Stručný a jasný GDPR manuál pro podnikatele a malé firmy. Dostupné z https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/2018/6/GDPR-manual_poslanec-Blaha_Final-1_revize-PV.pdf

Ministerstvo průmyslu a obchodu České republiky [MPO]. (2018b). Přiručka pro přípravu malých a středních firem na GDPR. Dostupné 15.11.2023 z https://www.mpo.cz/cz/podnikani/ochrana-osobnich-udaju-gdpr/podpurna-opatreni-mpo/prirucka-pro-pripravu-malych-a-strednich-firem-na-gdpr--236691/

Ministerstvo průmyslu a obchodu České republiky [MPO]. (2021). Vyhlášení transpoziční novely zákona o elektronických komunikacích ve Sbírce zákonů. Dostupné 21.7.2023 z https://www.mpo.cz/cz/e-komunikace-a-posta/elektronicke-komunikace/narodni-legislativa-a-predpisy/vyhlaseni-transpozicni-novely-zakona-o-elektronickych-komunikacich-ve-sbirce-zakonu--264027

Ministerstvo průmyslu a obchodu České republiky [MPO]. (2022). Novela zákona o ochraně spotřebitele a občanského zákoníku. Dostupné 21.7.2023 z https://www.mpo.cz/cz/ochrana-spotrebitele/informace-pro-spotrebitele/novela-zakona-o-ochrane-spotrebitele-a-obcanskeho-zakoniku--271440/

Mikkonen, T. (2014). Perceptions of controllers on EU data protection reform: A finnish perspective. Computer Law & Security Review, 30(2), 190-195. https://doi.org/10.1016/j.clsr.2014.01.011

Mishkin, F. S., & Eakins, S. G. (2018). *Financial Markets and Institutions* (9th Ed.). Harlow, UK: Pearson.

Mohammed, H. K., & Knápková, A. (2016). The impact of total risk management on company's performance. *Procedia-Social Behavioral Science*, 220, 271–277. https://doi.org/10.1016/j.sbspro.2016.05.499.

Národní úřad pro kybernetickou bezpečnost (n.d.). *Legislativa KB*. Dostupné 15.5.2021 z https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

NBN Shop (1998). *Standard NBN EN 45020:2009: Standardization and related activities - General vocabulary (ISO/IEC Guide 2:2004)*. Dostupné 2.5.2021 z https://www.nbn.be/shop/en/standard/preview/32555/en/

Newman, A.L. (2008). Protectors of Privacy: Regulating Personal Data in the Global Economy. Cornell University Press.

OECD & Eurostat. (2018). Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation (4th Edition). *OECD Publishing, Paris*. Dostupné 17.8.2023 z http://dx.doi.org/10.1787/9789264304604-en

OECD. (2019). Unpacking E-commerce. Business Models, Trends and Policies. *OECD Publishing, Paris*.

O'Hara R., Dickety, N. & Weyman A. (2005). Good practice in assessing workplace risks by small and medium-sized enterprises. *Risk Management*, 7(1), 31–41. http://dx.doi.org/10.1057/palgrave.rm.8240203

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, 37. https://doi.org/10.17705/1CAIS.03743

Olbrich, R., Schultz, C.D. & Holsing, C. (2019). Electronic Commerce und Online Marketing - Ein einführendes Lehr- und Übungsbuch. *Springer Gabler*

Oliva, F.L. (2016). A maturity model for enterprise risk management. International Journal of Production Economics, 173, 66-79. https://doi.org/10.1016/j.ijpe.2015.12.007

Paez, A. (2017). Gray literature: An important resource in systematic reviews. *Journal of Evidence-Based Medicine*, 10(3), 233-240. https://doi.org/10.1111/jebm.12266

Palmaccio, M., Dicuonzo, G. & Belyaeva, Z.S. (2021). The internet of things and corporate business models: A systematic review. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2020.09.069

Parlament České republiky. (2019). *ZÁKON ze dne 12. března 2019 o zpracování osobních údajů*. https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=

Pavlík, T. (n.d.). Základy korelační analýzy. Masarykovo univerzita. Dostupné 25.10.2023 z https://is.muni.cz/www/98951/41610771/43823411/43823458/44159634/44707073/Pavlik_-_Biostatistika_-_kapitola_11.pdf

Pearce, A. & Robinson, B. (2000). Formulation and Control of Competitive Strategy. Boston: Irwin McGraw-Hill.

Perry, R. (2019). GDPR – Project or permanent reality? *Computer Fraud & Security. 2019(1), 9-11*. https://doi.org/10.1016/S1361-3723(19)30007-7

Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide*. Blackwell Publishing. https://doi.org/10.1002/9780470754887

Plunkett, J.W. (2023). Plunkett's E-Commerce & Internet Business Almanac. E-Commerce & Internet Business Industry Market Research, Statistics, Trends and Leading Companies. *Plunkett Research, Ltd.*

Politou, E., Alepis, E. & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity*, 4(1). https://doi.org/10.1093/cybsec/tyy001

Politou, E., Alepis, E., Patsakis, C., Casino, F., & Alazab, M. (2020). Delegated content erasure in IPFS. *FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE*, 112, 956-964. https://doi.org/10.1016/j.future.2020.06.037

Pollfish. (2020). *Margin of Error & Sample Size Calculator*. Dostupné 15.8.2023 z https://www.pollfish.com/margin-of-error-calculator/

Porter, M. E. (1985). The Competitive Advantage: Creating and Sustaining Superior Performance. *NY: Free Press.*

Prakash M. & Singaravel G. (2015). An approach for prevention of privacy breach and information leakage in sensitive data mining. *Computers & Electrical Engineering*, 45, 134-140. https://doi.org/10.1016/j.compeleceng.2015.01.016

Presthus, W. & Sorum, H. (2019). Consumer perspectives on information privacy following the implementation of the GDPR. *IJISPM-INTERNATIONAL JOURNAL OF INFORMATION SYSTEMS AND PROJECT MANAGEMENT*. 7(3). 19-34. https://doi.org/ 10.12821/ijispm070302

Punch, K. (2015). Úspěšný návrh výzkumu. *Portál*.

Purssell, E. & McCrae, N. (2020). How to Perform a Systematic Literature Review: A Guide for Healthcare Researchers, Practitioners and Students. *Springer Nature*. https://doi.org/10.1007/978-3-030-49672-2

Qin, Z., Shuai, Q., Wang, G., Zhang, P., Cao, M. & Chen, M. (2022). E-Commerce - Concepts, Principles, and Application. *Springer*

Ramos, E.F. & Blind, K. (2020). Data portability effects on data-driven innovation of online platforms: Analyzing Spotify. Telecommunications Policy, 44(9). https://doi.org/10.1016/j.telpol.2020.102026

Reijers, H.A. (2021). Business Process Management: The Evolution of a discipline. *Computer in Industry*, 126. doi:10.1016/j.compind.2021.103404

Rohrbeck, R. (2011). Corporate foresight towards a maturity model for the future orientation of a firm. Heidelberg: Physica-Verlag.

Rostami, A., Sommerville, J., Wong, I.L. & Lee, C. (2015). Risk management implementation is small and medium enterprise in the UK construction industry. *Engineering, Construction and Architectural Management*, 22(1), 91–107. http://dx.doi.org/10.1108/ECAM-04-2014-0057

Rust, R.T. (2020). The future of marketing. *International Journal of Research in Marketing, 37, 15-26*. https://doi.org/10.1016/j.ijresmar.2019.08.002

Řepa, V. (2007). Podnikové procesy. Procesní řízení a modelování. *Grada Publishing*, a.s.

Sánchez-Gordón, M. & Colomo-Palacios, R. (2021). 2 Managing software development risk: Risks of introducing the role of agile coach – a multivocal literature review. In K. Engemann & R. O'Connor (Ed.), *Volume II Project Risk Management: Managing Software Development Risk (pp. 25-48)*. Berlin, Boston: De Gruyter Oldenbourg. https://doi.org/10.1515/9783110652321-003

Sanchez-Ruiz, L. & Blanco, B. (2019). Survey dataset on reasons why companies decide to implement continuous improvement. *Data in Brief, 26*. https://doi.org/10.1016/j.dib.2019.104523

Sciencedirect.com. (2021). Dostupné 3.5. z: https://www.sciencedirect.com/search?qs=gdpr

Segwick, P. (2010). Statistical hypothesis testing. BMJ, 340, 2059. https://doi.org/10.1136/bmj.c2059

Senzing (2018). *Finding the missing link in GDPR compliance*. [cit. 14.5.2021] Dostupné z: https://senzing.com/wp-content/uploads/Senzing-GDPR-Missing-Link-Report.pdf

Seville, M. & Teyssiér, C. (2017). Role of the Governance System in Strategic Risk Management. In Bérard, C. & Teyssier, C. (Eds), *Risk Management: Lever for SME Development and Stakeholder Value Creation (3-24).* John Wiley & Sons, Inc.

Sharma, S. (2020). Data Privacy and GDPR Handbook. John Wiley & Sons, Inc., Hoboken, New Jersey.

Shevlyakov, G.L. & Oja, H. (2016). *Robust Correlation. Theory and Applications*. John Wiley & Sons, Ltd.

Shoaib, M., Lim, M.K. & Wang, C. (2020). An integrated framework to prioritize blockchain-based supply chain success factors. *Industrial Management and Data Systems*, 120(11), 2103-2131. doi: 10.1108/IMDS-04-2020-0194

Shui, Q., Li, Z. & Zhang, Y. (2023). E-Commerce Industry Chain. Theory and Practice. *Springer*

Schneider, G.P. (2017). Electronic Commerce. *Gengage Learning*.

Schwambach, G.C.S., López, Ó.H., Sott, M.K., Tedesco, L.P.C. & Molz, R.F. (2022). Acceptance and perception of wearable technologies: A survey on Brazilian and European companies. *Technology in Society, 68*. https://doi.org/10.1016/j.techsoc.2021.101840

Sinning, C. (2021). International Strategic Management of Brands and Online Firms - Essays on Perceived Brand Globalness, Endorsed Branding and E-commerce Firms Internationalization. *Springer Gabler*.

Sirur S., Nurse, J. & Webb H. (2018). *Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*. 25th ACM Conference on Computer and Communication Security, Canada, pp. 1-8.

Slepchuk, A.N. & Milne, G.R. (2020). Informing the design of better privacy policies. *Current Opinion in Psychology*, 31, 89-93. https://doi.org/10.1016/j.copsyc.2019.08.007

Smejkal, V. & Rais, K. (2013). *Řízení rizik ve firmách a jiných organizacích*. Praha. Grada.

Smith, H.J., Dinev, T. & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quaterly, 35(4), 989-1015*. https://doi.org/10.2307/41409970

Starčevič, K., Crnkovič, B. & Glavaš, J. (2018). Implementation of the General Data Protection Regulation in companies in the Republic of Croatia. *Ekonomski Vjesnik / Econviews*. 31(1), 163-176.

Statcounter Global Stats (2023). Search Engine Market Share Worldwide. Dostupné 19.1.2023 z https://gs.statcounter.com/search-engine-market-share

Statistics Canada. (2016). Retail e-commerce in Canada. Dostupné 11.7.2023 z http://www.statcan.gc.ca/pub/11-621m/11-621-m2016101-eng.htm

Statutor (n.d.). *Spearman´s correlation*. Dostupné 2.10.2023 z https://www.statstutor.ac.uk/resources/uploaded/spearmans.pdf

STEM/MARK a.s. (2023). *CAWI; CASI*. Dostupné 2.9.2023 z https://stemmark.cz/encyklopedie-cawi-casi/

Steppe, R. (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective. *Computer Law & Security Review*, 33(6), 768-785. https://doi.org/10.1016/j.clsr.2017.05.008

St-Pierre, J. & Lacoursiére, R. (2017). Proactive Management of Operating Risks: A Lever to Improve External Funding for SMEs. In Bérard, C. & Teyssier, C. (Eds), *Risk Management: Lever for SME Development and Stakeholder Value Creation (87-106).* John Wiley & Sons, Inc.

Sweet, M. & Moynihan, R. (2007). *Improving Population Health: The Uses of Systematic Reviews*. Milbank Memorial Fund and Centers for Disease Control and Prevention.

Škeřík, O. (2016). *Systém řízení bezpečnosti informací prostřednictvím normy ČSN/EN ISO/IEC 27001* (Diplomová práce). Univerzita Hradec Králové, Fakulta informatiky a managementu, Česká republika

Tahri, H. & Drissi-Kaitouni, O. (2015). New design for calculating Project Management Maturity (PMM). *Procedia - Social and Behavioral Sciences,* 181, 171-177. https://doi.org/10.1016/j.sbspro.2015.04.878

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5–8. https://doi.org/10.1016/s1353-4858(16)30056-3

Taraldsen, G. (2021). The Confidence Density for Correlation. *Sankhya A 85, 600–616*. https://doi.org/10.1007/s13171-021-00267-y

Tarver, E. (2021). What Are the Primary Activities of Michael Porter's Value Chain? Investopedia.com. Dostupné 21.7.2023 z https://www.investopedia.com/ask/answers/050115/what-are-primary-activities-michael-porters-value-chain.asp

Teixeira, G.A., Mira da Silva, M. & Pereira, R. (2019). The critical success factors of GDPR implementation - a systematic literature review. *Digital Policy, Regulation and Governance. 21(4), 402-418*. https://doi.org/ 10.1108/DPRG-01-2019-0007

TIBCO Software Inc. (2023). TIBCO Statistica® 14.1.0 (Product Documentation). Dostupné 30.9.2023 z https://docs.tibco.com/products/tibco-statistica-14-1-0

Tikkinen-Piri, C., Rohunen, A. & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Thomaz, F., Salge, C., Karahanna, E. & Hulland, J. (2020). Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science, 48, 43-63.* https://doi.org/10.1007/s11747-019-00704-3

Tranfield, D., Denyer, D. & Smart, P. (2003). Towards a Methodology for Developing Evidence-Inferomed Management Knowledge by Means of Systematic Review. British Journal of Management, 14, 207-222. https://doi.org/10.1111/1467-8551.00375

Turban, E., Outland, J., King, D., Lee, J.K., Liang, T-P &Turban, D. (2018). Electronic Commerce 2018. A Managerial and Social Networks Perspective. *Springer*

Úřad na ochranu osobních údajů [ÚOOU] (2017). *Základní příručka k ochraně údajů.* https://www.uoou.cz/zakladni-prirucka-k-ochrane-udaju/ds-4744/p1=4744

Úřad na ochranu osobních údajů [ÚOOU] (2018a). *GDPR a přímý elektronický*. Dostupné 5.4.2021 z https://www.uoou.cz/gdpr-a-primy-elektronicky-marketing/d-30715

Úřad na ochranu osobních údajů [ÚOOU] (2018b). *K internetovým obchodům.* Dostupné 5.4.2021 z https://www.uoou.cz/k-internetovym-obchodum/ds-5269/archiv=0&p1=2619

Úřad na ochranu osobních údajů [ÚOOU] 2018c). *Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA).* Dostupné 5.4.2021 z https://www.uoou.cz/navod-k-posouzeni-vlivu-na-ochranu-osobnich-udaju-u-navrhu-pravnich-predpisu-dpia/ds-5344

Úřad na ochranu osobních údajů [ÚOOU] (2019). *Adaptační legislativa k GDPR vstoupila v účinnost.* Dostupné 5.4.2021 z https://www.uoou.cz/adaptacni-legislativa-k-gdpr-vstoupila-v-ucinnost/d-33656

Úřad na ochranu osobních údajů [ÚOOU] (2021a). Právní předpisy. Dostupné 5.4.2021 z https://www.uoou.cz/pravni-predpisy/ds-1257

Úřad na ochranu osobních údajů [ÚOOU] (2021b). Cookies od začátku roku 2022 pouze se souhlasem. Dostupné 22.10.2022 z https://www.uoou.cz/cookies-od-zacatku-roku-2022-pouze-se-souhlasem/d-53646

Úřad na ochranu osobních údajů [ÚOOU] (2023a). Právní předpisy. Dostupné 27.1.2023 z https://www.uoou.cz/pravni-predpisy/ds-1257/p1=1257

Úřad na ochranu osobních údajů [ÚOOU] (2023b). Konzultační kritéria. Dostupné 27.10.2023 z https://uoou.gov.cz/verejnost/konzultacni-kriteria

Úřad průmyslového vlastnictví (2023). SME Fund. Dostupné 10.11. z https://upv.gov.cz/sluzby/cosme-fund

van der Corput, M. & van der Storm, T. (2019). *Direct Marketing and its Relevance: The 'Opt-in Challenge*. https://www.opt-insight.com/wp-content/uploads/2018/09/Direct-Marketing-and-its-Relevance-The-Opt-in-Challenge.pdf

van der Waerdt, P.J. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. *Computer Law & Security Review*, 38. https://doi.org/10.1016/j.clsr.2020.105436

van Rosing, M., Kemp, N., Hove, M. & Ross, J.W. (2014). *The Complete Business Process Handbook: Body of Knowledge from Process Modeling to BPM*. Morgan Kaufman.

Veverková, S. (2021). Ochrana spotřebitele u smluv uzavřených mimo obchodní prostory [Disertační práce]. *Masarykova univerzita: Brno*.

Veverková, S. & Horáková, N. (2022). *Obchodní podmínky: Jak je použít a co do nich dát*. Dostupné 21.8.2023 z https://www.pravniprostor.cz/clanky/obchodni-pravo/obchodni-podminky-jak-je-pouzit-co-do-nich-dat

Voigt, P. & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). (2018). https://www.zakonyprolidi.cz/cs/2018-82

Woodside, A.G. (2010). *Case Study Research. Theory. Methods. Practice*. Emerald Group Publishing Limited.

Wieczorek-Kosmala, M. (2014). Risk management practices from risk maturity models perspective. *Journal for East European Management Studies*, 19(2), 133-159. http://dx.doi.org/10.1688/JEEMS-2014-02-Wieczorek-Kosmala

Wieringa, J., Kannan, P.K., Ma, X., Reutterer, T. & Risselada, H. (2021). Data analytics in a privacy-concerned world. *Journal of Business Researc*h, 122, 915-925. https://doi.org/10.1016/j.jbusres.2019.05.005

Williams, R.J., Clark, L.A. Clark, W.R. & Raffo, D.M. (2021). Re-examining systematic literature review in management research: *Additional benefits and execution protocol. European Management Journal*. https://doi.org/10.1016/j.emj.2020.09.007

Wohlin, C. (2014). *Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering*. Dostupné 20.5. z https://www.wohlin.eu/ease14.pdf

Xu, H., Luo, X., Carrol, J.M. & Rosson, M.B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42-52. https://doi.org/10.1016/j.dss.2010.11.017

Yamani, Z., Akhavan, M. (1996). Role of Pr substitution as deoxygenation in suppression of superconductivity in GdPr-123 system. *Physica C: Superconductivity*, 268 (1-2), 78-86. https://doi.org/10.1016/0921-4534(96)00401-7

Yeo, K.T. & Lai, W.C. (2004). Risk management strategies for SME investing in China – a Singaporean perspective. *IEEE International Engineering Management Conference Proceedings*, Singapore, 794–798. https://doi.org/10.1109/IEMC.2004.1407489

Yin, R.K. (2014). Case Study Research: Design and Methods. 5th ed. *SAGE Publications, Inc*.

Yuan, B. & Li, J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health*. 16(6), 1070. https://doi.org/10.3390/ijerph16061070.

ZÁKON ze dne 12. března 2019 o zpracování osobních údajů. (2019). Dostupné 26.7.2021 z https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38632

ZÁKON ze dne 3. února 2012 občanský zákoník. (2012). Dostupné 26.7.2021 z http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=24084

ZÁKON č. 89/2012 Sb. Zákon občanský zákoník. (2012). Dostupné 22.7.2023 z https://www.zakonyprolidi.cz/cs/2012-89

ZÁKON č. 634/1992 Sb. o ochraně spotřebitele ve znění pozdějších předpisů. (1992). Dostupné 22.7.2023 z https://www.zakonyprolidi.cz/cs/1992-634

ZÁKON č. 468/2011 Sb. Zákon, kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony. (2011). Dostupné 22.7.2023 z https://www.zakonyprolidi.cz/cs/2011-468

ZÁKON č. 480/2004 Sb. Zákon o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). (2004). Dostupné 22.7.2023 z https://www.zakonyprolidi.cz/cs/2004-480

ZÁKON o kybernetické bezpečnosti a o změně souvisejících zákonů. (2014). Dostupné 26.7.2021 z http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6688

ZÁKON č. 365/2000 Sb. o informačních systémech veřejné správy. (2000). Dostupné 26.7.2021 z https://www.mvcr.cz/clanek/legislativa-zakon-c-365-2000-sb-o-informacnich-systemech-verejne-spravy.aspx

ZÁKON č. 480/2004 Sb. o některých službách informační spolehlivosti. (2004). Dostupné 26.7.2021 z https://www.mpo.cz/cz/e-komunikace-a-posta/postovni-sluzby/sluzby-informacni-spolecnosti/zakon-c--480-2004-sb---o-nekterych-sluzbach-informacni-spolecnosti--84535/

ZÁKON č. 262/2006 Sb., zákoník práce (2006). Dostupné 26.7.2021 z https://ppropo.mpsv.cz/zakon_262_2006

ZÁKON č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. (2005). Dostupné 26.7.2021 z https://www.nbu.cz/download/UZ-zakon_412_2005.pdf

ZÁKON č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů. (2000). Dostupné 26.7.2021 z https://www.zakonyprolidi.cz/cs/2000-101

Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, 2017(6), 8-11. https://doi.org/10.1016/S1353-4858(17)30060-0)

Zhang, H., Mao, R., Huang, H., Dai, Q., Zhou, X., Shen, H. & Rong, G. (2021). Processes, challenges and reccommendations of Gray Literature Review: An experience report. *Information and Software Technology*, 137. https://doi.org/10.1016/j.infsof.2021.106607

Zhang, R., Fang, L. He, X. & Wei, C. (2023). The Whole Process of E-commerce Security Management System. Design and Implementation. Springer

Zhanga L., Xua, X., Luob, Z., Shena, D. & Wua, H. (2009). Identification of an unusual AT(D)Pase-like activity in multifunctional NAD glycohydrolase from the venom of Agkistrodon acutus. *Biochimie*, 91(2), 240-251. https://doi.org/10.1016/j.biochi.2008.09.003

Zhuo, R., Huffaker, B. Claffy, K. & Greenstein, S. (2021). The impact of the General Data Protection Regulation on internet interconnection. *Telecommunications Policy*, 45(2). https://doi.org/ 10.1016/j.telpol.2020.102083

Přílohy

Příloha A: Vyspělost projektového řízení (Model PMMM – řízení rizik)

Definované praktiky (řádky) / Úroveň vyspělosti (sloupce)	**Iniciační fáze**	**Standardizované procesy**	**Institucionalizované procesy**	**Řízené procesy**	**Optimalizované procesy**
Plánování řízení rizik	Není definován plán řízení rizik	Existuje plán pro řízení rizik. Využívají jej především velké projekty	Plán využíván všemi projekty, jsou specifikovány jednotlivé oblasti řízení rizik	Principy řízení rizik jsou přizpůsobeny potřebám každého projektu	Hodnota a zlepšení jsou klíčovými aspekty při sestavování plánů řízení rizik
Identifikace rizik	Rizika nejsou identifikována systematicky	Existuje rámcový plán pro identifikace, soustředění na klíčové oblasti	Dokumentovatelný a opakovatelný proces identifikace rizik v projektech	Plná integrace rizik do plánu náklady a harmonogramu projektu	Neustálé zlepšování procesu identifikace rizik
Kvalitativní analýza rizik	Improvizovaný způsob analýzy	Standardní metodologie, obvykle třístupňový přístup	Sofistikovanější metody analýzy	Jsou používány pokročilé metody k odhadu dopadu na většinu aspektů projektu	Analýza na základě předchozích zkušeností, neustálé zlepšování metod analýzy
Kvantitativní analýza rizik	Improvizovaný způsob analýzy	Standardní metodologie, semikvantitativní přístup	Pokročilé kvantitativní metody	Jsou používány pokročilé metody k odhadu dopadu na většinu aspektů projektu. Měřena efektivita opatření	Analýza na základě předchozích zkušeností, neustálé zlepšování metod analýzy
Plánování opatření rizik	Reaktivní přístup	Základní metodologie, základní integrace s plánem projektu	Standardizovaná opatření. Jsou ošetřována všechna rizika projektu	Plná integrace s plány nákladů, harmonogramem a dalšími oblastmi projektu.	Zpětné vyhodnocování efektivity opatření, a to i na základě čerpání rezerv projektu.
Controlling rizik	Reakce pouze v případě výskytu rizika	Každý projektový tým má vlastní přístup ke kontrolování rizik	Všechny projekty průběžně monitorují rizika, průběžné úpravy v opatřeních	Systém controllingu plně integrován s podnikovým systémem.	Zdokumentovaný proces využívající hodnocení rizik a údaje o aktuálním stavu rizikového managementu pomáhá při rozhodování o řízení během provádění projektu.
Dokumentace rizik	Rizika nejsou dokumentována	Jsou uvažována historická data, nekonzistentní sběr	Jsou sbírána historická data, spouštěče negativních událostí, poklad pro ostatní projekty	Dokumentace projektů je plně s organizační dokumentací.	Zkušenosti z předchozích projektů jsou zachyceny a použity ke zlepšení sběru dat. Jsou prováděna hodnocení po ukončení projektu.

Příloha B: Mnohostranná literární rešerše (zkrácený seznam zdrojů)

Vysvětlivka: A = akademická literatura; G = šedá literatura

Kód	Název publikace	Rok publikace	Autoři / Organizace	URL adresa publikace
A01	Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions	2018	Politou, E.; Alepis, E.;Patsakis, C.	https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056
A02	Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation	2018	van den Broek, T.;van Veenstra, A.F.	https://www.sciencedirect.com/science/article/pii/S0040162517314695
A03	Implementation of the General Data Protection Regulation in Companies in the Republic of Croatia	2018	Starcevic, K.;Crnkovic, B.;Glavas, J.	https://hrcak.srce.hr/file/297314
A04	The critical success factors of GDPR implementation: a systematic literature review	2019	Teixeira, G.A.;da Silva, M.M.;Perreira, R.	https://www.researchgate.net/publication/333581339_The_critical_success_factors_of_GDPR_implementation_a_systematic_literature_review
A05	Consumer privacy and the future of data-based innovation and marketing	2020	Bleier, A., Goldfarb, A. & Tucker, C.	https://www.sciencedirect.com/science/article/pii/S0167811620300331?via%3Dihub
A06	Machine Understandable Policies and GDPR Compliance Checking	2020	Bonatti, P.A.; Kirrane, S.; Petrova, I.M.; Sauro, L.	https://link.springer.com/article/10.1007/s13218-020-00677-4
A07	A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices	2019	Layton. R.;Elaluf-Calderwood. S.	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8962288
A08	Challenges of Complying with Data Protection and Privacy Regulations	2021	Lonzetta, A. M.;Hayajneh, T.	https://eudl.eu/pdf/10.4108/eai.26-5-2020.166352
A09	From ISO/IEC27001:2013 and ISO/IEC27002:2013 to GDPR compliance controls	2021	Diamantopoulou, V.;Tsohou, A.;Karyda, M.	https://www.researchgate.net/publication/342025264_From_ISOIEC270012013_and_ISOIEC270022013_to_GDPR_compliance_controls
A10	GDPR and Business Processes: an effective solution	2019	Bartolini, C.; Calabró, A.; Marchetti, E.	https://www.webofscience.com/wos/woscc/full-record/WOS:000519037800007
A11	Achieving GDPR Compliance of BPMN Process Models	2019	Agostinelli, S.; Maggi, F.M.; Marrella, A.; Sapio, F.	https://iris.uniroma1.it/retrieve/handle/11573/1290908/1184104/Agostinelli_Postprint_Achieving-GDPR_2019.pdf
A12	GDPR in Labout Relations - with or without consent of the employee	2018	Švec, M., Horecký, J. & Madleňák, A.	https://www.semanticscholar.org/paper/GDPR-in-labour-relations-with-or-without-the-of-the-Svec-Horeck%C3%BD/6998b89531484efe41b37298f0789cefb3460e1d
A13	Risk Management for Cloud Compliance with the EU General Data Protection Regulation	2018	Duncan, B.;Zhao, Y.	https://www.researchgate.net/publication/326482794_Risk_Management_for_Cloud_Compliance_with_the_EU_General_Data_Protection_Regulation
A14	Factors determining the extent of GDPR implementation within organizations: Empirical Evidence from Czech Republic	2021	Faifr, A.;Januška, M.	https://journals.vilniustech.lt/index.php/JBEM/article/view/15095/10687
A15	Implementation of GDPR into Payroll Accounting in the Czech republic	2020	Šišková, J; Lörinczová, E.	https://digilib.uhk.cz/bitstream/handle/20.500.12603/291/%C5%A0i%C5%A1kov%C3%A1%20aj..pdf?sequence=1&isAllowed=y
A16	The Core of Enterprise Architecture as a Management Tool: GDPR implementation case study	2018	Rozehnal, P.; Novák, V.	https://link.springer.com/article/10.1007/s10257-020-00500-5
A17	How ISO 27001 can help achieve GDPR compliance	2019	Lopes, I.M.;Gurda, T.;Oliveira, P	https://ieeexplore.ieee.org/document/8760937
A18	Understanding the notion of risk in the General Data Protection Regulation	2018	Gellert, R.	https://www.sciencedirect.com/science/article/pii/S0267364917302698
A19	With GDPR, preparation is everything. Computer Fraud & Security	2017	Krystlik, J.	https://www.sciencedirect.com/science/article/pii/S1361372317300507
A20	What the GDPR means for businesses. Network Security	2016	Tankard, C.	https://www.sciencedirect.com/science/article/pii/S1353485816300563
A21	EU General Data Protection Regulation: Changes and implications for personal data collecting companies	2017	Tikkinen-Piri, Ch.;Rohunen, A.;Markula, J.	https://www.sciencedirect.com/science/article/pii/S0267364917301966
A22	GDPR: a milestone in convergence for cyber-security and compliance	2017	Zeerlang, J.	https://www.sciencedirect.com/science/article/pii/S1353485817300600
A23	GDPR compliance: your tech department's next big opportunity	2017	Beckett, P.	https://www.sciencedirect.com/science/article/pii/S1361372317300416
A24	GDPR Compliance in SMEs	2018	Freitas, M.C.;Mira da Silva, M.	https://www.jisem-journal.com/download/gdpr-compliance-in-smes-there-is-much-to-be-done-3941.pdf
A25	A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises	2019	Brodin, M.	https://www.researchgate.net/publication/333669136_A_Framework_for_GDPR_Compliance_for_Small-_and_Medium-Sized_Enterprises

A26	GDPR – compliance nightmare or business opportunity?	2018	Garber, J.	https://www.sciencedirect.com/science/article/pii/S1361372318300551
A27	The European Union general data protection regulation: what it is and what it means	2019	Hoofnagle, C.J.;Sloot, B.;Borgesius, F.Z.	https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501
A28	The need for continuous compliance	2018	Khan, J.	https://www.sciencedirect.com/science/article/pii/S1353485818300576
A29	Implementation of the General Data Protection Regulation: A Survey in Health Clinics	2018	Lopes, I.M.;Oliveira, P	https://ieeexplore.ieee.org/document/8399156
A30	GDPR – project or permanent reality	2019	Perry, R.	https://www.sciencedirect.com/science/article/pii/S1361372319300077
A31	Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)	2018	Sirur, S.;Nurse, J.;Webb H.	https://www.researchgate.net/publication/327160034_Are_We_There_Yet_Understanding_the_Challenges_Faced_in_Complying_with_the_General_Data_Protection_Regulation_GDPR
A32	Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors	2018	Kurtz, C.;Semmann, M.	https://www.researchgate.net/publication/325415927_Privacy_by_Design_to_Comply_with_GDPR_A_Review_on_Third-Party_Data_Processors
A33	Strategy and Solution to comply with GDPR: Guideline to comply major articles and save penalty from non-compliance	2017	Priyadharshini, G.;Shyamala, K.	https://ieeexplore.ieee.org/document/8653696
A34	The Impact of GDPR on Global Technology Development	2019	Li, H.;Yu, L.;He, W.	https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1569186
A35	The Role of IS in the Conflicting Interests Regarding GDPR	2020	Jakobi, T.;von Grafestein, M.;Legner, C.;Labadie, C.;Mertens, P.;Oksuez, A.;Stevens, G.	https://www.webofscience.com/wos/woscc/full-record/WOS:000538250200007
A36	A readiness assessment tool for GDPR compliance certification	2019	Chatzipoulidis, Ar.;Tsiakis, T.;Kargidis, T.	https://www.sciencedirect.com/science/article/pii/S1361372319300867
A37	Information Security Frameworks Assisting GDPR Compliance in Bank Industry	2020	Serrado, J.;Perreira, R.F.;da Sivla, M.M.;Bianchi, I.S.	https://www.webofscience.com/wos/woscc/full-record/WOS:000558458500001
A38	Using Models to Enable Compliance Checking against the GDPR: An Experience Report	2019	Torre, D.;Soltana, G.;Sabetzadeh, M.;Briand, L.C.;Auffinger, Y.;Goes, P.	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8906896
A39	Enterprise architecture management as a solution for addressing general data protection regulation requirements in a big data context: a systematic mapping study	2021	Georgiadis, G.;Poels, G.	https://link.springer.com/content/pdf/10.1007/s10257-020-00500-5.pdf
A40	Data protection and tech startups: The needfor attention, support, and scrutiny	2021	Norval, C.;Janssen, H.;Cobbe, J.;Singh, J.	https://onlinelibrary.wiley.com/doi/10.1002/poi3.255
A41	Backups and the right to be forgotten in the GDPR	2018	Politou, E.;Michota, A.;Alepis, E.;Pocs, M.;Patsakis, C.	https://reader.elsevier.com/reader/sd/pii/S0267364918301389?token=7AE6B33650B289905BC5FD853F0DF601C7D4ACF6F236DBC899C5A7F6226DCEE929303A094C591CEA21BDF999DAB6C2B6&originRegion=eu-west-1&originCreation=20210801132257
A42	Data protection: Prepare now or risk disaster	2016	Mansfield-Devine, S.	https://www.sciencedirect.com/science/article/pii/S1361372316300987
A43	GDPR: What's in a Year (and a Half)?	2019	Ferreira, A.	https://www.scopus.com/record/display.uri?eid=2-s2.0-85091399238&origin=inward&txGid=d34a265e407132a4f8ea7ee027dd0774
A44	The Grace Period Has Ended: An Approach to Operationalize GDPR Requirements	2018	Ayala-Rivera, V.;Pasquale, L.	https://ieeexplore.ieee.org/document/8491130
A45	A framework for security technology cohesion in the era of the GDPR	2018	Wilson, S.	https://www.sciencedirect.com/science/article/pii/S1361372318301192
A46	Enhancing Information Governance with Enterprise Architecture Management: Design Principles Derived from Benefits and Barriers in the GDPR Implementation	2020	Burmeister, F.;Huth, D.;Drews, P.;Schirmer, I.	https://www.researchgate.net/publication/336588966_Enhancing_Information_Governance_with_Enterprise_Architecture_Management_Design_Principles_Derived_from_Benefits_and_Barriers_in_the_GDPR_Implementation
A47	One Model For Implementation GDPR Based On ISO Standards	2018	Tzolov, T.	https://www.scopus.com/record/display.uri?eid=2-s2.0-85057128449&origin=resultslist&sort=plf-f&src=s&sid=821d66065af3f74882d8b486ba77a989&sot=b&sdt=b&sl=45&s=%28AUTHOR-NAME%28tzolov%29+AND+TITLE-ABS-KEY%28gdpr%29%29&relpos=2&citeCnt=2&searchTerm=
A48	Using an Enterprise Architecture Model for GDPR Compliance Principles	2020	Blanco-Laine, G.;Sottet, J.S.;Dupuy-Chessa, S.	https://www.webofscience.com/wos/woscc/full-record/WOS:000611409100013
A49	Methods and tools for GDPR compliance through privacy and data protection engineering,'' in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), Apr. 2018, pp. 108–111.	2018	Martin, Y.-S.;Kung, A.	https://www.semanticscholar.org/paper/Methods-and-Tools-for-GDPR-Compliance-Through-and-Mart%C3%ADn-Kung/2e461882b8f55b11efca5edf74c1a1b40e404075
A50	Continuous Requirements: An Example Using GDPR	2019	Li, Z.S.; Werner, C.; Ernst, N.	https://ieeexplore.ieee.org/abstract/document/8933680
A51	An innovative online process mining framework for supporting incremental GDPR compliance of business processes	2019	Zaman, R.;Cuzzorcrea, A.;Hassani, M.	https://ieeexplore.ieee.org/document/9005705
G01	Step Plan GDPR Implementation	2020	Taylor Wessing	https://www.taylorwessing.com/en/insights-and-events/insights/2020/08/step-plan-gdpr-implementation

G02	6 Steps to GDPR Implementation	2018	Bauer, D. / Risk Management Magazine	http://www.rmmagazine.com/home/2018/04/02/-6-Steps-to-GDPR-Implementation-
G03	OCHRANA ÚDAJOV pre malé a stredné firmy	2019	ESET.com	https://www.eset.com/sk/blog/firemna-it-bezpecnost/ako-na-ochranu-udajov-v-malych-a-strednych-firmach/
G04	Twists and turns in the road Driving toward GDPR	2017	Cheng, S.;Prior, P. / Compliance Week	https://www.complianceweek.com/download?ac=5809
G05	10 GDPR Implementation Pitfalls to Avoid	2019	Lighthouse	https://www.lighthouse-services.com/newsletters/10-gdpr-implementation-pitfalls-to-avoid/
G06	The Importance of BPM in GDPR Compliance	2018	Holenstein M. / Corporate Compliance Insights	https://www.corporatecomplianceinsights.com/importance-bpm-gdpr-compliance/
G07	GDPR for Small Businesses: A Beginner's Guide	2018	Compliance Junction	https://www.compliancejunction.com/gdpr-for-small-business/
G08	GDPR simplified: A guide for your small business	2021	Microsoft	https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide
G09	GDPR for Small Businesses: A Beginner's Guide to GDPR Compliance Requirements	2018	OneTrust Pro	https://www.onetrustpro.com/blog/gdpr-for-small-businesses-beginners-guide/
G10	Top 10 GDPR Frameworks	2018	Medium	https://medium.com/alpin-io/top-10-gdpr-frameworks-ec5ad4bfdeab
G11	GDPR Implementation in 4 Steps!	2018	Przybylla, T. / SAP Signavio	https://www.signavio.com/post/gdpr-implementation-in-4-steps/
G12	GDPR Small Business Survey	2019	GDPR.eu	https://gdpr.eu/wp-content/uploads/2019/05/2019-GDPR.EU-Small-Business-Survey.pdf
G13	Report on the SME experience of the GDPR	2019	Barnard-Wills, D.;Cochrane, L.;Matturi, K.;Marchetti, F. / STAR II (Projekt EU)	https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf
G14	Guidance Note: GDPR Guidance for SMEs	2019	Data Protection Commission	http://edepositireland.ie/bitstream/handle/2262/91029/190708%20Guidance%20for%20SMEs.pdf?sequence=1&isAllowed=y
G15	Příručka pro přípravu malých a středních firem na GDPR	2018	Ministerstvo průmyslu a obchodu ČR	https://www.mpo.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/Podpurna-opatreni-mpo/2018/4/Prirucka-pro-pripravu-malych-a-strednich-firem-na-GDPR.pdf
G16	Obecné nařízení o ochraně osobních údajů	2018	CzechInvest	https://www.czechinvest.org/cz/Sluzby-pro-male-a-stredni-podnikatele/GDPR
G17	How long does GDPR Implementation take?	2018	Ecomply	https://www.ecomply.io/blog-en/how-long-does-gdpr-implementation-take
G18	GDPR Starter Kit	2018	TayllorCox	
G19	The Ultimate Guide to GDPR Compliance	2021	OneTrust	https://www.onetrust.com/resources/the-guide-to-gdpr-compliance/
G20	How Blackboard's GDPR implementation supports our clients	2018	Korba, Z. / Blackboard	https://help.blackboard.com/search?search=gdpr&f%5B0%5D=&f%5B1%5D=&_ga=2.91694424.314083576.1629887230-1140958308.1629887230
G21	The GDPR: Six Months After Implementation	2019	Delloitte	https://www2.deloitte.com/bg/en/pages/legal/articles/gdpr-six-months-after-implementation-2018.html
G22	A new era for privacy GDPR six months on	2019	Delloitte	https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf
G23	Implementation of GDPR and Its Impact on Mobile App Marketing	2021	Ashwin, S.L. / Moengage	https://www.moengage.com/blog/one-year-of-gdpr-and-its-impact-on-mobile-app-marketing/
G24	How to overcome GDPR implementation roadblocks with the help of automation	2018	Vinit Sinha / WiPRO	https://www.wipro.com/business-process/how-to-overcome-gdpr-implementation-roadblocks-with-the-help-of-automation/
G25	Almost two years of GDPR: celebrating and improving the application of Europe's data protection framework	2020	Digital Europe	https://www.digitaleurope.org/resources/almost-two-years-of-gdpr-celebrating-and-improving-the-application-of-europes-data-protection-framework/
G26	7-Step Checklist for GDPR Compliance	2021	Ekran	https://www.ekransystem.com/en/blog/how-to-prepare-for-gdpr
G27	Complete Guide to General Data Protection Regulation (GDPR) Compliance	2021	OneTrust	https://www.onetrust.com/blog/gdpr-compliance/
G28	How to make your business GDPR compliant	2021	Netherlands Enterprise Agency & Netherlands Chamber of Commerce	https://business.gov.nl/running-your-business/business-management/administration/how-to-make-your-business-gdpr-compliant/
G29	GDPR – The Challenges and the Opportunity	2018	Planet Compliance	https://www.planetcompliance.com/gdpr-challenges-opportunity/
G30	10 Ways GDPR Will Impact Your Business Operations – Part 1	2018	Bridewell Consulting	https://www.bridewellconsulting.com/10-ways-gdpr-will-impact-business-operations-part-1

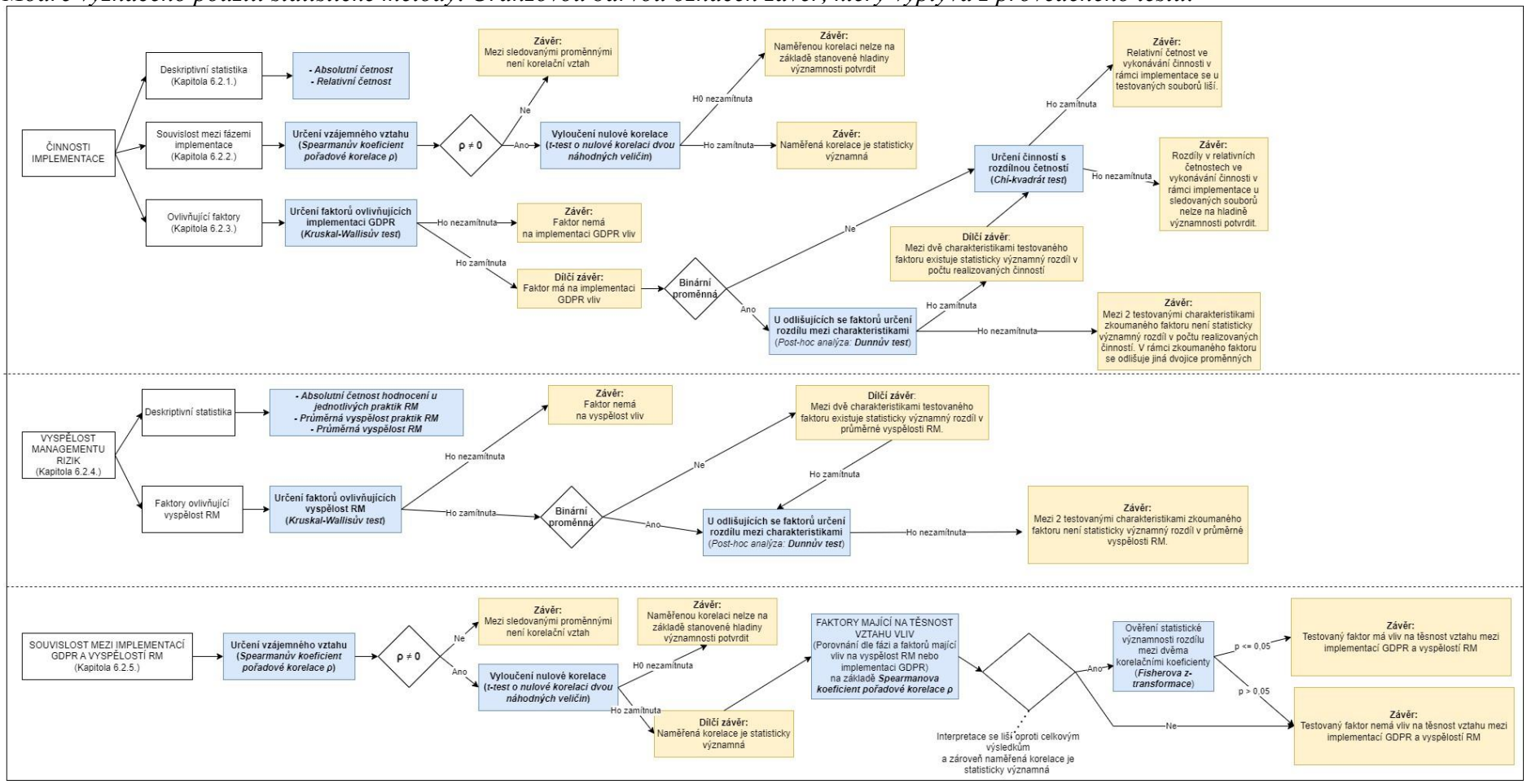
G31	Will GDPR affect your business processes? You bet!	2017	Tamsar, T. / Nortal	https://nortal.com/blog/gdpr-affects-business-processes/
G32	GDPR is a Process Issue	2017	Gotts, I. / BPM Institute	https://www.bpminstitute.org/resources/articles/gdpr-process-issue
G33	How does the GDPR impact business marketing and customer engagement?	2021	Sahoo, N. / Cisomag	https://cisomag.eccouncil.org/gdpr-impact-business-marketing-customer-engagement/
G34	What is GDPR? How it Impacts Different Industries?	2020	Stealthlabs	https://www.stealthlabs.com/blog/what-is-gdpr-how-it-impacts-different-industries/
G35	The Impact of GDPR on Users and Business: The Good, The Bad and the Uncertain	2018	Litkov, D. / Martenscentre	https://www.martenscentre.eu/wp-content/uploads/2020/06/gdpr-impact-users-business-good-bad-uncertain.pdf
G36	GDPR and its Impact On Businesses	2018	Multidots	https://www.multidots.com/gdpr-impact-businesses/
G37	How might GDPR affect different business functions?	2018	Page, M. / Michael Page	https://www.michaelpage.co.uk/our-expertise/technology/how-might-gdpr-affect-business
G38	The General Data Protection Regulation	2018	Sponselee, A. / Delloitte	https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-deloitte-gdpr-report.pdf
G39	How Vendor Risk Management Can Impact Your GDPR Compliance	2018	Lack, B. / Poradenská společnost	https://reciprocity.com/how-vendor-risk-management-can-impact-your-gdpr-compliance/
G40	The GDPR made simple® for SMEs	2021	Jasmontaité-Zaniewicz, L.;Calvi, A.;Nagy, R.;Barnard-Wills, D. / VUB Press	https://www.aspeditions.be/en-gb/book/the-gdpr-made-simpler-for-smes/18137.htm
G41	How to make your website compliant with the GDPR	2017	Secure Privacy	https://secureprivacy.ai/solution/gdpr
G42	GDPR: The Compliance Journey	2018	To Increase	https://www.to-increase.com/download-ebook-gdrpr-compliance-journey
G43	GDPR survey: Benefits beyond compliance	2020	Baker & McKenzie	https://www.bakermckenzie.com/-/media/files/insight/publications/2020/04/gdpr_survey.pdf?sc_lang=en&hash=4975FCC8AECB96A9116ED3275D4293B6
G44	Global Privacy and Information Management Handbook	2018	Baker & McKenzie	https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en
G45	GDPR compliance since May 2018: A continuing challenge	2019	McKinsey	https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/gdpr-compliance-after-may-2018-a-continuing-challenge
G46	EU General Data Protection Regulation in 13 Game Changers	2018	Baker & McKenzie	https://www.lexology.com/library/detail.aspx?g=fba01535-2824-437f-ad95-f96ed963ab83
G47	ENSURING COMPLIANCE WITH THE GDPR	2017	Software AG	https://info.softwareag.com/general-data-protection-regulation-compliance-white-paper.html
G48	Delivering the Microsoft GDPR Assessment	2018	Microsoft	https://docs.microsoft.com/en-us/compliance/regulatory/gdpr
G49	Getting ready for the GDPR, 2017	2017	Information Commissioner's Office (ICO) UK.	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
G50	Maintaining data protection and privacy beyond GDPR implementation	2018	Clemens, T. / ISACA	http://resources.titus.com/GDPR-the-end-of-the-beginning
G51	GDPR still a mystery to SMEs: the risks of non-compliance	2019	Hiscox	https://www.hiscox.co.uk/business-blog/gdpr-still-mystery-smes-risks-non-compliance
G52	Leveraging the Lessons Learnt from GDPR in the New Deal for Consumers	2020	Baker & McKenzie	https://www.bakermckenzie.com/en/insight/publications/2020/02/leveraging-lessons-gdpr
G53	Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR	2017	IaPP	https://iapp.org/resources/article/comparing-the-benefits-of-pseudonymization-and-anonymization-under-the-gdpr/
G54	Using ISACA Privacy Principles for GDPR Compliance	2017	ISACA	https://www.isaca.org/resources/news-and-trends/industry-news/2017/using-isaca-privacy-principles-for-gdpr-compliance
G55	Přístup k architektuře pro GDPR	2018	KPMG Česká republika	

Příloha C: Bariéry implementace GDPR u MSP

Zdroj	Typ výsledků	Bariéry týkající se nedostatečných zdrojů či dovedností	Finanční náročnost implementace nebo nedostatečný rozpočet	Nepochopení textu regulace	Nízké povědomí o regulaci, podcenění rozsahu	Nedostatek znalostí	Nedostatek odborníků interních či externích	Nedostatek lidských zdrojů pro implementaci	Časová náročnost implementace	Nedostatečná podpora ze strany externích subjektů	Nedůvěra v odborníky	Nedostatečná politická moc	Lepší flexibilita v MSP	Celkem bariér
G13	Empirický výsledek	X	X	X	X	X			X	X	X			**8**
A30	Expert		X	X		X	X		X					**5**
A31	Empirický výsledek	X	X	X						X	X			**5**
G21	Rešerše	X	X		X		X							**4**
G24	Rešerše		X	X			X							**3**
G35	Expert	X	X						X					**3**
A05	Rešerše		X									X	X	**3**
A08	Rešerše		X					X						**2**
G12	Empirický výsledek	X		X										**2**
G40	Expert		X					X						**2**
A24	Empirický výsledek		X					X						**2**
A40	Empirický výsledek	X		X										**2**
A42	Expert	X		X										**2**
A04	Rešerše					X								**1**
A07	Rešerše	X												**1**
A12	Empirický výsledek				X									**1**
A15	Empirický výsledek	X												**1**
G03	Návod	X												**1**
G04	Návod		X											**1**
G08	Návod				X									**1**
G25	Návod	X												**1**
A35	Rešerše		X											**1**
G47	Návod	X												**1**
G51	Expert			X										**1**
Celkem bariér		**12**	**12**	**8**	**4**	**3**	**3**	**3**	**3**	**2**	**2**	**1**	**1**	**50**

Příloha D: Schéma použití statistických metod (dotazníkové šetření)

Modře vyznačeno použití statistické metody. Oranžovou barvou označen závěr, který výplývá z provedeného testu.



Vazba na výzkumný cíl	**Hypotézy dle kapitoly 6.1.1**	**Výstup**	**Popis testu**	**Statistická metoda**	**Ověření významnostii provedeného testu**
Cíl 2 - úkol 2		Tabulka 6-12	Četnosti činností v rámci implementace GDPR	Absolutní a relativní četnost	-
		Tabulka 6-13	Korelace mezi fázemi implementace GDPR	Spearmanův koeficient pořadové korelace ρ	t-test o nulové korelaci dvou náhodných veličin
Cíl 2 - úkol 3	H2+H3	Tabulka 6-14	Určení faktorů ovlivňujících rozsah implementace GDPR	Kruskal-Wallisův H test	-
	H2+H3 (dodatečná analýza)	Tabulk 6-15, Tabulka 6-16, Tabulka 6-19	Analýza proměnných v rámci ovlivňujících faktorů	Medián, průměr počtu činností	
		Tabulka 6-17	Určení odlišujících se proměnných u testovaného faktoru (více než 2 pozorovnání)	Dunnův test	
		Tabulka 6-18, Tabulka 6-20	Určení činnosti u ovlivňujících faktorů s odlišnou mírou četnosti realizace	Rozdíl v relativní četnosti	Pearsonův chí-kvadrát test
Cíl 3 (obecný)		Tabulka 6-12	Vyspělost RM u malých e-shopů	Absolutní četnost, průměr	
		Tabulka 6-22	Určení faktorů ovlivňujících vyspělost RM	Kruskal-Wallisův H test	
		Tabulka 6-23	Analýza proměnných v rámci ovlivňujících faktorů	Medián, průměr počtu činností ve skupině	
		Tabulka 6-24	Určení odlišujících se proměnných u ovlivňujícího faktoru (více než 2 pozorování)	Dunnův test	
Cíl 3 - úkol 3	H1	Tabulka 6-25, Tabulka 6-26	Souvislost RM a implementace GDPR	Spearmanův koeficient pořadové korelace ρ	t-test o nulové korelaci dvou náhodných veličin
	H1 (dodatečná analýza)	Tabulka 6-27	Analýza faktorů majících vliv na těsnost vztahu mezi RM a implementací GDPR (oproti obecné těsnosti proměnných)	Rozdíl spearmanových koeficientů pořadové korelace ρ	Fisherova Z-transformace

Příloha E: Návrh dotazníku

BLOK 1: Charakteristika společnosti a respondenta

- **Jak byste nazval/a vaši pracovní pozici?** (otevřená otázka, nepovinná otázka)
- **Zadejte název vaší společnosti** (otevřená otázka, nepovinná otázka)
- **Naše společnost provozuje e-shop v těchto zemích** (více možností, zaškrtnutí alespoň 1 možnosti)
  - Česká republika
  - Slovensko
  - Další země EU (kromě Slovenska)
  - Evropské státy (mimo EU)
  - Státy mimo Evropu
- **V naší společnosti jsem…** (více možností, zaškrtnutí alespoň 1 možnosti)
  - Osobou zodpovědnou za implementaci GDPR
  - Osobou v současnost zodpovědnou za zajišťování ochrany osobních údajů
  - Byl členem týmu, který v našem podniku GDPR implementoval
  - Se na implementaci GDPR nepodílel
- **Naše společnost je certifikována některou z následujících standardů ISO, včetně podskupin** (více možností, zaškrtnutí alespoň 1 možnosti)
  - ISO 9000 (Řízení kvality)
  - ISO 31000 (Řízení rizik)
  - ISO 27000 (Bezpečnost informací)
  - ISO 27552 (Správa osobních údajů)
  - Naše společnost není certifikována žádný z uvedených standardů
  - Nedokážu posoudit
- **Za citlivé osobní údaje se považují např. informace o rasovém či etnickém původu, náboženském vyznání, zdravotním stavu, sexuální vyznání, informace o politických názorech a osobní údaje nezletilých. Naše společnost některé z těchto osobních údajů zpracovává.** (jedna možnost)
  - Ano, zpracovává
  - Ne, nezpracovává
  - Nedokážu posoudit

BLOK2: Implementace GDPR

- **Implementace GDPR v naší společnosti proběhla** (jedna odpověď)
  - Pouze interními prostředky - bez spolupráce s externími subjekty (konzultační společnosti, právní služby apod.)
  - Implementaci GDPR v naší společnosti zajišťoval externí subjekt
  - Kombinovaný přístup interních a externích prostředků
  - Nedokážu posoudit
- **Před zahájením implementace GDPR jsme realizovali tyto činnosti.** (Zaškrtněte platné. 0 až 5 možností)
  - Seznámení se s textem nařízení
  - Posouzení vlivu GDPR na organizaci (nakolik se nařízení společnosti týká)
  - Aktivní zvýšení povědomí o GDPR v organizaci
  - Nastavení zodpovědnosti za implementaci GDPR
  - Zpracování plánu projektu implementace
- **S ohledem na ochranu osobních údajů máme zpracovány tyto dokumenty.** (Zaškrtněte platné. 0 až 5 možností)
  - Mapování datových toků a zpracování osobních údajů
  - Analýza současného stavu ochrany osobních údajů + GAP analýza
  - Posouzení rizik zpracování (vyhodnocení rizik spojených se zpracováním osobních údajů)
  - DPIA - zpracování Posouzení vlivu na ochranu osobních údajů
  - Definice strategie zpracování dat v organizaci

- **Během zapracování požadavků GDPR jsme se zabývaěmito oblastmi (jsme realizovali následující činnosti.** (Zaškrtněte platné. 0 až 5 možností)
    - Nastavení zodpovědností za ochranu osobních údajů v organizaci
    - Vytvoření postupů pro případ úniku dat a jiných bezpečnostních incidentů
    - Zpracování Podmínek pro zpracování OÚ na webových stránkách
    - Zpracování tzv. "Záznamů o zpracování osobních údajů"
    - Trénink personálu a školení
    - Zajištění zákonnosti, férovosti a transparentnosti zpracování (čištění dat, výmaz dat, agenda správy souhlasů, zajištění adekvátních právních základů pro zpracování)
    - DPO - jmenování "Pověřence pro ochranu osobních údajů"
    - Problematika cookies
    - Zajištění práv subjektů (zapracování práv vyplývajících z Nařízení)
    - Provedení opatření organizačního charakteru (přístupová práva apod.)
    - Provedení technických opatření (např. šifrování, pseudonymizace dat, zavedené nových bezpečnostních systémů apod.)
    - Zajištění zpracování u třetích stran (analýza rizik dodavatelů, pravidla pro předávání údajů třetím stranám apod.)
    - Dokumentace GDPR a prokazování plnění požadavků
    - Minimalizace dat
    - Řízení životního cyklu dat
    - Problematika zpracování zvláštních kategorií osobních údajů (citlivých údajů)
    - Neustálé zlepšování procesu ochrany osobních údajů
    - Komunikace s ÚOOÚ
    - Monitoring a kontrolní mechanismy (systém pro monitoring ochrany osobních údajů)
    - Aplikace přístupů privacy by design a privacy by default v podnikových procesech

BLOK 3: Vyspělost managementu rizik

- **Charakterizujte, jakým způsobem se ve vaší společnosti tvoří plány pro řízení rizik.** (jedna možnost)
    - Plán pro řízení rizik v naši společnosti neexistuje
    - Existuje rámcový plán pro řízení rizik. Využívají jej především větší projekty a hlavní procesy.
    - Existuje plán pro řízení rizik. Zahrnuje všechny realizované projekty i oblasti.
    - Existuje plán pro řízení rizik specificky upraveného pro každý projekt a oblast.
    - Existuje plán pro řízení rizik specificky upraveného pro každý projekt a oblast. Zaměřujeme se na jejich neustálé zlepšování.
    - Nedokážu posoudit
- **Charakterizujte, jakým způsobem jsou ve vaší společnosti identifikována rizika.** (jedna možnost)
    - Rizika nejsou systematicky identifikována - neexistuje jednoznačný přístup k jejich identifikaci
    - Existuje rámcový plán pro identifikaci. Identifikujeme rizika týkající se klíčových oblastí, procesů a projektů.
    - Existuje standardizovaný a dokumentovaný proces, podle kterého rizika identifikueme.
    - Proces identifikace rizik je plně integrován s plány nákladů a harmonogramu.
    - Plně integrovaný proces, na jehož zlepšování neustále pracujeme.
    - Nedokážu posoudit
- **Charakterizujte kvalitativní analýzu rizik ve vaší společnosti. Kvalitativní analýza rizik znamená, že je identifikovaným rizikům dáno slovní, zpravidla neměřitelné, hodnocení (malé, střední, velké riziko apod.).** (jedna možnost)
    - Nemáme nastavený žádný standardizovaný postup analýzy.
    - Máme stanovenou metodiku - máme nastavené slovní stupnice (škály) pro hodnocení pravděpodobnosti a dopadu.
    - Máme stanovenou metodiku - používáme sofistikovanější metody pro stanovení závažnosti.
    - Máme stanovenou metodiku - pro každý projekt či proces je používána vlastní metodika.
    - Analyzujeme na základě předchozích zkušeností, metody analýzy neustálé aktualizujeme a zlepšujeme.
    - Nedokážu posoudit

- **Charakterizujte kvantitativní analýzu rizik ve vaši společnosti. Kvantitativní analýza rizik znamená, že je identifikovaným rizikům číselné ohodnocení. Rizika je tak možné seřadit dle závažnosti nebo lze vyčíslit míru dopadu.** (jedna možnost)
    - Nemáme nastavený žádný standardizovaný postup analýzy.
    - Máme nastavenou standardní metodiku - např. bodovací stupnice 1-5 apod.
    - Máme nastavenou standardní metodiku - používáme pokročilejší metody hodnocení.
    - Máme stanovenou metodiku + zpětně měříme efektivitu případných opatření.
    - Metodiky neustále aktualizujeme na základě předchozích zkušeností.
    - Nedokážu posoudit

- **Jak ve vaší firmě provádíte opatření vůči rizikům? Jak se proti existujícím rizikům bráníte**? (jedna možnost)
    - Reaktivní přístup - rizika ošetřujeme, až když se projeví.
    - Máme základní metodiku, ošetřujeme pouze nejzávažnější rizika.
    - Máme standardizovanou metodiku, způsob ošetření plánujeme pro všechna rizika.
    - Strategie ošetření je plně integrována s plány nákladů, harmonogramem a dalšími oblastmi projektů či procesů.
    - Zpětně vyhodnocujeme efektivitu opatření, a to i na základě čerpání rezerv projektu apod.
    - Nedokážu posoudit
- **Charakterizujte proces controllingu rizik. Jedná se o aktivitu, která má za cíl průběžně monitorovat rizika po jejich prvotním ošetření.** (jedna možnost)
    - Reagujeme pouze v případě výskytu rizika.
    - Každý tým má vlastní přístup ke monitorování rizik.
    - Průběžně monitorujeme všechna rizika a provádíme průběžné úpravy v opatřeních dle aktuálního stavu.
    - Monitoring rizik je plně integrován s podnikovým systémem.
    - Využíváme hodnocení rizik a údaje o aktuálním stavu rizik k rozhodování o řízení během prováděných projektů, procesů.
    - Nedokážu posoudit
- **Charakterizujte proces dokumentace rizik. Tedy, jak sbíráte a dokumentujete informace o rizicích.** (jedna možnost)
    - Rizika ani informace o nich nedokumentujeme.
    - Uvažujeme historická data, sběr a dokumentace nejsou konzistentní.
    - Sbíráme historická data, spouštěče negativních událostí.
    - Dokumentace rizik je součástí organizační dokumentace.
    - Zkušenosti z předchozích projektů jsou zachyceny a použity ke zlepšení sběru dat. Jsou prováděna hodnocení po ukončení projektu.
    - Nedokážu posoudit