Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra systémového inženýrství

Diplomová práce

Projekt implementace nařízení GDPR ve firmě

Martin Valeš

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Valeš

Projektové řízení

Název práce

Projekt implementace nařízení GDPR ve firmě

Název anglicky

Implementation of GDPR regulation in the company

Cíle práce

Cílem práce je popis a zhodnocení projektu implementace procesů pro soulad s nařízením GDPR ve vybrané společnosti. Projekt bude řízen podle standardu PRINCE2 a bude rozdělen na dílčí části, které budou nakonec zhodnoceny z hlediska jejich úspěšného dodání, dále budou popsány případné komplikace včetně způsobu jejich řešení.

Metodika

V první části diplomové práce bude vymezena teoretická část v oblastech projektového řízení, popis projektových standardů s hlavním zaměřením na PRINCE2, dále popis jednotlivých fází projektu a stručného vysvětlení nařízení GDPR.

Druhá část bude zaměřena na praktickou charakteristiku implementace GDPR, popis jednotlivých fází projektu včetně zhodnocení, případně doporučení alternativních možností řešení. Celková analýza projektu implementace GDPR bude provedena na základě teoretických a praktických znalostí v oblasti GDPR a Project managementu. V závěru práce bude celkové shrnutí projektu včetně doporučení, které pomohou zlepšit projektový management v dané společnosti. Výsledkem také bude typizovaný projekt na jehož základě může být provedena implementace nařízení GDPR i v obdobných společnostech.

Doporučený rozsah práce

50-60 stran

Klíčová slova

Projektové řízení, projekt, PRINCE2, implementace, GDPR, analýza

---

Doporučené zdroje informací

BARKER, S. – COLE, R. *Projektový management pro praxi.* Praha: Grada, 2009. ISBN 978-80-247-2838-4.
NĚMEC, V. *Projektový management.* Praha: Grada Publishing, 2002. ISBN 80-247-0392-0.
SCHWALBE, K. *Řízení projektů v IT : kompletní průvodce.* Brno: Computer Press, 2011. ISBN 978-80-251-2882-4.
SVOZILOVÁ, A. *Projektový management.* Praha: Grada, 2011. ISBN 978-80-247-3611-2.
ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

doc. Ing. Tomáš Šubrt, Ph.D.

Garantující pracoviště

Katedra systémového inženýrství

Elektronicky schváleno dne 1. 3. 2019

doc. Ing. Tomáš Šubrt, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 3. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Projekt implementace nařízení GDPR ve firmě" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.3.2019 _____

Poděkování

Rád bych touto cestou poděkoval panu doc. Ing. Tomáši Šubrtovi, PhD.za skvělé vedení a zejména za poskytnutí cenných rad a připomínek k diplomové práci v rámci konzultací.

Projekt implementace nařízení GDPR ve firmě

Souhrn

Diplomová práce se věnuje implementaci nařízení GDPR ve vybrané společnosti, která z důvodu anonymity nebude identifikována. První část práce je zaměřena na popsání teoretických východisek projektového řízení, mezinárodně uznávaných standardů a popis evropského nařízení GDPR.

Praktická část je vyhotovena na základě aktivní účasti autora práce, který byl v projektu na pozici projektového manažera.

Projekt byl veden pomocí projektového standardu PRINCE 2, kdy daný standard byl přizpůsoben relevantním podmínkám společnosti.

Po ukončení projektu došlo k následnému zhodnocení úspěšnosti a vzniklých nedostatků, které budou použity v dalších projektech ve společnosti, jako aplikace principu Lessons learned.

Klíčová slova: Projektové řízení, projekt, PRINCE2, implementace, GDPR, nařízení, analýza, proces, cíl, metodika

Implementation of GDPR regulation in the company

Summary

The diploma thesis deals with the implementation of the GDPR regulation in selected company, which will not be identified due to maintain anonymity. The first part of the thesis is focused on describing theoretical bases of project management, internationally recognized project's standards and description of the GDPR regulation.

The practical part is prepared on the basis of an active participation of the author of the work who was in the project roles as a project manager.

The project was managed using the PRINCE 2 project standard in the adapted form to the relevant company conditions.

After the end of the project, the success and deficiencies were subsequently evaluated and the results will be used in future company's projects, as well as the application of the Lessons learned principle.

Keywords: project management, project, PRINCE2, implementation, GDPR, regulation, analysis, process, goal, methodology

Obsah

Seznam obrázků

Seznam tabulek

Seznam grafů

1 Úvod

Ochrana osobních údajů je již delší dobu velmi diskutované téma, které bylo ještě více umocněno novým Evropským nařízením o ochraně osobních údajů GDPR (General Data Protection Regulation), jenž 25. května 2018 vstoupilo v platnost s působností ve všech členských státech Evropské unie a nahradilo tak dosavadní zákon č. 101/2000 Sb., o ochraně osobních údajů a Směrnici 95/46/ES.

Právní reforma v oblasti ochrany osobních údajů byla již nezbytným krokem, protože původní legislativa již nebyla schopna adekvátně reflektovat změny ve zpracování osobních údajů díky rozvoji informačních technologií a požadavků firem na automatizaci procesů. Zejména se jednalo o nové činnosti jako profilování nebo automatizované zpracování, která mohou mít přímý vliv na občany EU.

Nařízení se týká všech subjektů, které zpracovávají osobní údaje fyzických osob na území Evropské unie nebo pro správce osobních údajů, které působí v rámci EHP a má za účel přinést vyšší úroveň ochrany osobních údajů, hájit práva občanů Evropské unie proti neoprávněnému používání jejich osobních údajů a dat a také vytvořit jednotný přístup ke zpracování ve všech členských státech. V současné době již například není možné regulérně zpracovávat osobní údaje fyzických osob, aniž by zpracování nebylo založené na jednom z právních titulů, které ho definují jako zákonné.

Vzhledem k tomu, že implementace požadavků, které GDPR nařízení stanovuje není nijak snadné, tak je vhodné, aby k ní společnosti přistupovaly prostřednictvím projektového řízení a celkovou implementaci rozdělily do několika na sebe závislých kroků.

Diplomová práce se věnuje projektu implementace GDPR nařízení ve vybrané společnosti, která je poskytovatelem platebních služeb malého rozsahu, a to prostřednictvím doporučeného mezinárodně uznávaného projektového standardu PRINCE2. Práce je rozdělena do třech částí, kdy autor práce je ve funkci projektového manažera.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je popis a zhodnocení projektu implementace požadavků a procesů pro soulad s nařízením GDPR ve vybrané společnosti prostřednictvím projektového standardu PRINCE 2.

Dílčími cíli práce jsou vytvoření znalostní databáze z dokončeného projektu, která bude dále využívána pro budoucí projekty a eliminaci původních nedostatků. Dále vytvoření standardizovaného projektu, který může být použit pro implementaci nařízení GDPR v obdobných společnostech.

2.2 Metodika

První část práce je zaměřena na vymezení teoretických východisek projektového managementu s hlavním zaměřením na mezinárodně uznávaný projektový standard PRINCE2 a popis Obecného nařízení GDPR prostřednictvím odborné literatury.

Ve druhé části dochází k detailnímu popisu projektu implementace GDPR nařízení ve vybrané společnosti, kdy je dodržována metodika projektového standardu PRINCE2 z aktualizované podoby z roku 2017. V rámci analýzy současného stavu dojde ke sběru informací o současném stavu, tj. mapování zpracování, které budou použity pro definování potřebných kroků k dosažení souladu s nařízením.

V průběhu projektu je využíváno služeb externí advokátní kanceláře, která zajišťuje odborný dohled na projekt v rámci konzultací, vytváření interní dokumentace a revize interně vytvořené dokumentace a správce informačních technologií, který kontroluje a zabezpečuje společností používané nástroje pro zpracování osobních údajů.

Dále budou v rámci projektu použity základní dokumenty standardu se zaměřením zejména na řízení rizik, kvality a vytvoření směrného plánu projektu, které jsou v jeho průběhu aktualizovány.

Třetí část této práce je věnována vyhodnocení výsledků projektu a práce autora se zaměřením na vytvoření znalostní databáze pro další projekty ve společnosti.

3 Teoretická východiska

3.1 Projektové řízení

Jedná se o aplikování znalostí, dovedností, nástrojů a technik na činnosti projektu takovým způsobem, aby byly splněny kladené požadavky na projekt. V projektovém řízení je zapotřebí plánovat, organizovat, monitorovat a reportovat zprávy o všech parametrech projektu a motivaci veškerých zainteresovaných stran za účelem dosažení cílů projektu. Při řízení projektů je nezbytná optimalizace parametrů času, nákladů a rizik s dalšími požadavky a na základě těchto daných omezení projekt organizovat.

Projektové řízení lze rozdělit do pěti základních oblastí, kterými jsou:

1) Projektová komunikace
2) Týmová spolupráce
3) Životní cyklus projektu
4) Vlastní součásti projektového managementu
5) Organizační závazek

(Doležal, et al., 2012)

3.1.1 Definice projektu

Za projekt lze považovat jakýkoli jedinečný sled aktivit a úkolů, které mají určitý specifický cíl, který má být naplněn jeho realizací, dále je časově ohraničen (tj. má svůj začátek a konec) a má omezený rozsah zdrojů pro jeho čerpání. (Svozilová, 2011)

Projekt podle PRINCE 2

Projekt je dočasná organizace, která je vytvořena za účelem dodání jednoho nebo více produktů na základě stanoveného Business casu.

Existuje řada charakteristik projektové práce, které se liší od obvyklého podnikání:

1) **Změna** = projekty jsou prostředkem přinášející změny
2) **Dočasnost** = Projekty mají vždy dočasný charakter. Požadovaná změna byla uskutečněna a podnikání jako takové pokračuje v nové podobě, přičemž potřeba projektu již není. Projekty by tedy měly mít předem určený začátek a konec.

3) **Cross-functional** (v překladu multifunkční tým) = Projekty zahrnují týmy lidí s různými dovednostmi, kteří spolupracují (na dočasné bázi) na provedení změny, která ovlivní celou společnost.

   Projekty jsou často mimo normální funkční rozdělení v rámci organizace a někdy zasahují i mimo organizaci, což také často vytváří napětí v rámci organizace, mezi zákazníky i dodavateli, neboť každý je ovlivněn odlišnými zájmy na projektu a tím i přístupu k němu a přinášené změně.
4) **Unikátnost** = Každý projekt musí být svým způsobem jedinečný, ať už z hlediska lokality, jiného složení týmu či jiného zákazníka.
5) **Nejistota** = Je patrné, že výše uvedené charakteristiky představují hrozby a příležitosti, které přesahují ty, s nimiž se běžně setkáváme v rámci obvyklých činností. Proto lze projekty označit za riskantnější. (AXELOS, 2017)

Produkt projektu

Každý projekt je realizován za účelem vytvoření specifického jedinečného produktu, služby případně jejich kombinaci, jehož prostřednictvím bude naplněno očekávání zadavatele a zároveň dojde k naplnění stanoveného strategického či taktického cíle.

Produktem může být hmotná věc, která je kvantifikovatelná, dále služba sloužící k zefektivnění podnikového procesu nebo vstup, který bude použit pro další procesy, např. závěrečná zpráva z výzkumu. (Svozilová, 2011)

3.1.2 Životní cyklus projektu

Projekt je díky svým vlastnostem charakterizován jako proces. Projekt po dobu své existence prochází vývojem, a tedy i různými fázemi projektu, které představují životní cyklus projektu.

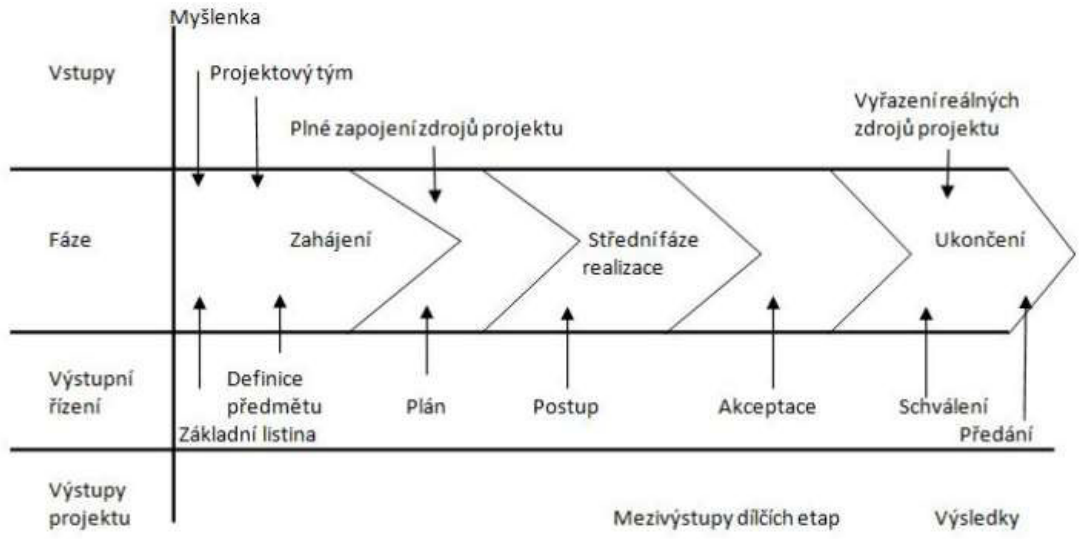
Při aplikaci teorie systémů, kterou popsali Cleland a King lze následně životní cyklus projektu rozdělit na následujících 5 fází:

1. **Konceptuální návrh** – v této fázi dochází k vymezení základních účelů projektu s následným hodnocením benefitů a možných dopadů, které realizace projektu přinese. V neposlední řadě dochází ke stanovení odhadu nákladů, potřebného času na jeho realizaci a prvotní analýze rizik;
2. **Definice projektu** – na základě první fáze dochází k bližšímu upřesnění výstupů z konceptuálního návrhu s hlavním zaměřením na diverzifikaci cílů, sestavení

seznamu subsystémů, přípravu metodik, dovedností a znalostí, které jsou k dispozici pro projekt, identifikování zdrojů, rizik a předpokládaných omezení včetně jejich možných dopadů, dále na realistické stanovení časového rámce včetně kalkulace nákladů a detailního plánování realizace projektu;

3. **Produkce (vlastní realizace projektu)** – vlastní vedení projektu, kontrola postupu projektu dle časového harmonogramu, rozpočtu, správa projektové dokumentace a komunikace mezi členy projektového týmu, kontroly kvality a naplnění dílčích cílů včetně hodnocení výstupů;
4. **Operační období** – sloučení předmětu projektu s existujícími systémy organizace, hodnocení dosavadních dopadů, vznik zpětné vazby pro plánování budoucích projektů;
5. **Vyřazení projektu** – předání projektu do odpovědnosti organizace a stádia podpory projektu. Vytvoření závěrečného reportu za účelem získání ponaučení ze získaných zkušeností pro další projekty. (Svozilová, 2011)

Obrázek 1 - Životní cyklus projektu



Zdroj: (Svozilová, 2011 str. 38)

3.1.3 Cíl projektu

Účel, pro který je projekt realizován se nazývá cíl projektu. Jedná se o slovní popis požadovaného budoucího stavu, který by měl být vytvořen realizací projektu.

Cíl projektu je zpravidla hierarchická struktura určitých stavů, podmínek a charakteristik, které definují budoucí projektový výstup.

Při formulaci projektového cíle je vhodné vycházet z techniky SMART, kdy cíle musí být:

S – specifické

M – měřitelné

A – přidělitelné (lze přidělit odpovědnost a autoritu jedinému subjektu)

R – dosažitelné

T – časově ohraničené

Projektové cíle lze rozdělit na globální cíl a konkrétní dílčí cíle projektu, kdy globální cíl určuje mandatorní cíl projektu, který zároveň udává jeho jasný celkový směr a finální výsledek. Dílčí konkrétní cíle jsou dekompozicí globálního cíle, které upřesňují požadavky zadavatele projektu a zároveň napomáhají ke správnému pochopení celkového zadání projektu ze strany projektového realizátora. (Svozilová, 2011)

3.2 Světově uznávané projektové standardy

3.2.1 PMBOK

PMBOK (Project Management Body of Knowledge) je projektový standard, navržený v roce 1987 institucí Project Management Institute (PMI). Účelem standardu PMBOK je poskytnout ucelený pohled projektovým manažerům na problematiku projektového řízení a zároveň popsat jeho veškeré aspekty. (Maule, 2004)

Standard je založen na přístupu procesního pojetí problematiky řízení projektů, při čemž definuje 5 mandatorních procesů, 9 znalostních oblastí a vazby mezi jednotlivými procesy. Všechny procesy a jejich kroky mají určené transformační nástroje (aktivity, metody a techniky), dále mají určené vstupy a výstupy. (Doležal, a další, 2012)

Procesy PMBOK

1) **Zahajovací procesy** (procesy od iniciace až po spuštění projektu)
2) **Plánovací procesy** (procesy od plánování rozsahu prací až po sestavení projektového plánu)
3) **Prováděcí procesy** (se skládají z hlavních a pomocných procesů a zahrnují procesy od realizace projektového plánu až do výstupy projektu)
4) **Procesy operativního řízení** (procesy týkající se zejména vykazování výkonů a celkové koordinace změn)
5) **Uzavírací procesy** (procesy zahrnující ukončení smluvních vztahů a procesů uzavírající administrativní stránku, jako je například archivace dokumentace, či zaznamenání získaných zkušeností) (Řeháček, 2013)

Znalostní oblasti projektového řízení, nástroje a techniky

Znalostní oblasti charakterizují kostru rámce projektového managementu a zároveň slouží jako popis hlavních kompetencí projektového manažera, které musí být rozvíjeny. Základní znalostní oblasti můžeme rozdělit na devět okruhů:

1) **Řízení rozsahu** = určení a vedení veškerých nezbytných prací pro úspěšné dokončení projektu
   Nástroje a techniky = Work breakdown structure (WBS), analýza požadavků

2) **Řízení času** = stanovení odhadů časové náročnosti jednotlivých činností, vytvoření časového plánu a zajištění jeho dodržování
   Nástroje a techniky = Ganttův diagram, CPM, MPM, PERT
3) **Řízení nákladů** = tvorba plánu, kontrola a pravidelná aktualizace projektového rozpočtu
   Nástroje a techniky = NPV, ROI, EVM
4) **Řízení kvality** = kontrola přinášených výsledků z hlediska kvality
   Nástroje a techniky = kontrolní seznamy, Paretův diagram, Diagram rybí kosti
5) **Řízení lidských zdrojů =** zajišťování, že lidské zdroje v projektu jsou využívány efektivně
   Nástroje a techniky = matice RACI, teambuildingy, techniky motivace
6) **Řízení komunikace =** zajištění vhodné správy informací o projektu
   Nástroje a techniky = meetingy, reporting, online komunikační kanály, sestavy
7) **Řízení rizik** = identifikování, analyzování a následná minimalizace rizik v projektu
   Nástroje a techniky = metoda Risk Project Analysis, mapa rizik
8) **Řízení obstarávání =** zajištění potřebných vstupů ze strany externích dodavatelů
   Nástroje a techniky = evaluace dodavatelů, analýza vlastních sil, smluvní zajištění
9) **Integrované řízení** = činnost, která je kombinací všech výše uvedených oblastí a projektový manažer by měl mít potřebné znalosti a zkušenosti ze všech uvedených oblastí.
   Nástroje a techniky = analýza zájmových skupin, podpůrný software pro projektový management, SWOT analýza
   (Doskočil, 2013)

3.2.2 IPMA Competence Baseline

IPMA Competence Baseline je mezinárodně uznávaný projektový standard, který spravuje mezinárodní asociace projektového řízení (International Project Management Association, dále jen IPMA), aktuálně je vydána čtvrtá verze ICB.

Standard ICB je oproti PRINCE2 a PMBOK založen na kompetencích projektových manažerů a nikoli na definování procesů projektového řízení. Cílem standardu je umožnit projektovému manažerovi, ověřit si, v jaké míře má rozvinuté má rozvinuté klíčové kompetence ve veškerých oblastech, které jsou mandatorní pro správné řízení projektů. (PM Consulting, 2019)

*„Kompetence projektového manažera je chápána jako aplikace znalostí, dovedností a schopností tak, aby byly dosaženy požadované výsledk*y.*“* (IPMA, 2017 str. 11)

Kompetenční model ICB je založen na třech klíčových oblastech, které jsou dále rozděleny do 29 elementů neboli kompetencí. Tyto tři klíčové oblasti dohromady tvoří „OKO KOMPETENCÍ“:

1) **Behaviorální kompetence** (osobní a interpersonální kompetence, které jsou potřebné ke správnému vedení a koordinaci projektu);
2) **Technické kompetence** (metody, techniky a nástroje, které jsou využívány, aby bylo dosaženo projektového cíle);
3) **Kontextové kompetence** (metody, techniky a nástroje, které používají projektoví manažeři ke komunikaci se svým okolím, dále tyto kompetence definují důvody, kvůli kterým jsou iniciovány činnosti na projektech ze strany projektových manažerů, organizace nebo společnosti). (IPMA, 2017)

Obrázek 2 - Kompetence a elementy podle IPMA

Kontextové kompetence		Behaviorální kompetence		Technické kompetence	
K1	Strategie	B1	Sebereflexe a sebeřízení	T1	Návrh projektu, programu nebo portfolia
K2	Systém řízení, struktura a procesy	B2	Osobní integrita a spolehlivost	T2	Požadavky a cíle, Přínosy a cíle
K3	Shoda se standardy a předpisy	B3	Komunikační dovednost	T3	Rozsah projektu
K4	Moc a zájem	B4	Zainteresovanost a vztahy	T4	Čas
K5	Kultura a hodnoty	B5	Vůdcovství	T5	Organizace projektu, programu, portfolia a práce s informacemi
		B6	Týmová práce	T6	Kvalita
		B7	Konflikty a krize	T7	Finance
		B8	Kreativita, vynalézavost a důvtip	T8	Zdroje
		B9	Vyjednávání	T9	Obstarávání (a partnerství)
		B10	Orientace na výsledky	T10	Plánování a operativní řízení
				T11	Rizika a příležitosti
				T12	Zainteresované strany
				T13	Transformace a organizační změny
				T14	Výběr a vyváženost

Zdroj: Vlastní zpracování (text IPMA)

3.2.3 PRINCE 2

PRINCE2 je integrovaný rámec procesů a témat, které se zaměřují na plánování, delegování, monitorování a kontrolu všech šesti aspektů výkonu projektu.

3.2.3.1 Struktura PRINCE2

Metoda PRINCE2 se zaměřuje na řízení projektů prostřednictvím čtyř integrovaných proměnných, kterými jsou principy, témata, procesy a projektové prostředí.

Metoda PRINCE2 definuje 7 principů, které jsou řídící povinnosti a osvědčené postupy určující, zda je projekt skutečně řízen pomocí metody PRINCE2, neboť pokud nejsou využívány všechny, tak nelze vůbec hovořit o tom, že projekt je řízen podle této metodiky.

Principy jsou univerzální a aplikovatelné na jakýkoli projekt, prověřené mnohaletou praxí a podporující, protože dávají manažerům praktikující metodu větší důvěru a schopnost ovlivňovat, jakým způsobem bude projekt řízen. (AXELOS, 2017)

1) Neustálé zdůvodňování opodstatněnosti projektu

Projekt musí mít opodstatněný důvod pro jeho zahájení, musí zůstat validní po celou dobu životního cyklu projektu. Opodstatnění musí být zdokumentováno a schváleno prostřednictvím Business Casu.

Vzhledem k tomu, že projekt je neoddělitelně spojen s podnikatelským zdůvodněním, řídí procesy rozhodování, aby zajistil, že projekt bude i nadále v souladu s požadovanými obchodními cíli a jasnými benefity. Organizace, které postrádají přísnost v rozvíjení Business casu, mohou zjistit, že některé projekty probíhají dokonce i tam, kde existuje jen málo reálných přínosů, nebo projekt není v souladu s firemní strategií. Špatné přizpůsobení se podnikovým strategiím může také vést k tomu, že organizace mají portfolio projektů, které mají vzájemně nekonzistentní nebo i duplicitní cíle. Dokonce i projekty, které jsou povinné (například, které musí být provedeny pro soulad s legislativou), vyžadují zdůvodnění zvolené možnosti, neboť může existovat několik možností, které přinášejí různé náklady, přínosy a rizika.

I když by ospravedlnění mělo zůstat platné, může se změnit. Je proto důležité, aby projekt a vyvíjející se odůvodnění zůstaly v platnosti. Pokud projekt z jakéhokoli důvodu již není oprávněný, projekt by měl být zastaven. Zastavení projektu za těchto okolností je pozitivním přínosem pro organizaci, neboť její prostředky a zdroje mohou být reinvestovány do dalších projektů, které jsou prospěšné. (AXELOS, 2017)

2) Učení se ze zkušeností

Vzhledem k tomu, že každý projekt je jedinečný, tak může být projekt pro současný projektový tým náročný, protože nemají s předmětem projektu dostatečné zkušenosti. Proto by ještě při zahájení projektu mělo dojít k přezkoumaní předchozích obdobných projektů, aby se zjistilo, jestli je možné se z nich určitým způsobem poučit. Nemusí se však nutně jednat o interní projekty, ale mohou být použity také externí projekty, a tedy čerpat ze zkušeností ostatních.

Učení ze zkušeností by však mělo probíhat dále současně s projektem včetně ve fázi ukončení projektu, kdy jednotlivá poučení by měla být zaznamenána do příslušné dokumentace Lessons learned. (AXELOS, 2017)

3) Definované role a odpovědnosti

Aby projekt byl úspěšný, tak musí mít explicitní strukturu projektového týmu s jasně definovanými rolemi a k nim přiřazenými zodpovědnostmi pro zajištění efektivní komunikace mezi členy týmu.

Všechny projekty mají vždy definované tři primární stakeholdery, kterými jsou sponzor projektu, uživatel a dodavatel.

4) Řízení po etapách

PRINCE2 rozděluje projekt do sekcí, které se nazývají projektové etapy, kdy počet etap je závislý na mnoha faktorech, jako je například velikost a složitost projektu, významnost rozhodnutí a kontrolní body vyžadované životním cyklem projektu, politiky a standardy organizace. Každý projekt by však měl mít alespoň dvě etapy, a to iniciační etapu a další volitelnou etapu. (AXELOS, 2017)

5) Řízení na základě výjimky

PRINCE2 umožňuje určité přenesení pravomoci z jedné úrovně organizace na jinou, a to za předpokladu respektování šesti aspektů výkonnosti (náklady, čas, kvalita, rozsah, benefity a rizika). Dále jsou nastaveny kontrolní mechanismy pro případ, že dojde k překročení tolerančních limitů, které jsou nazývány výjimkami. V takových případech dojde k eskalaci těchto výjimek na jinou úroveň řízení, aby došlo k adekvátnímu manažerskému rozhodnutí. (AXELOS, 2017)

6) Zaměření se na produkty

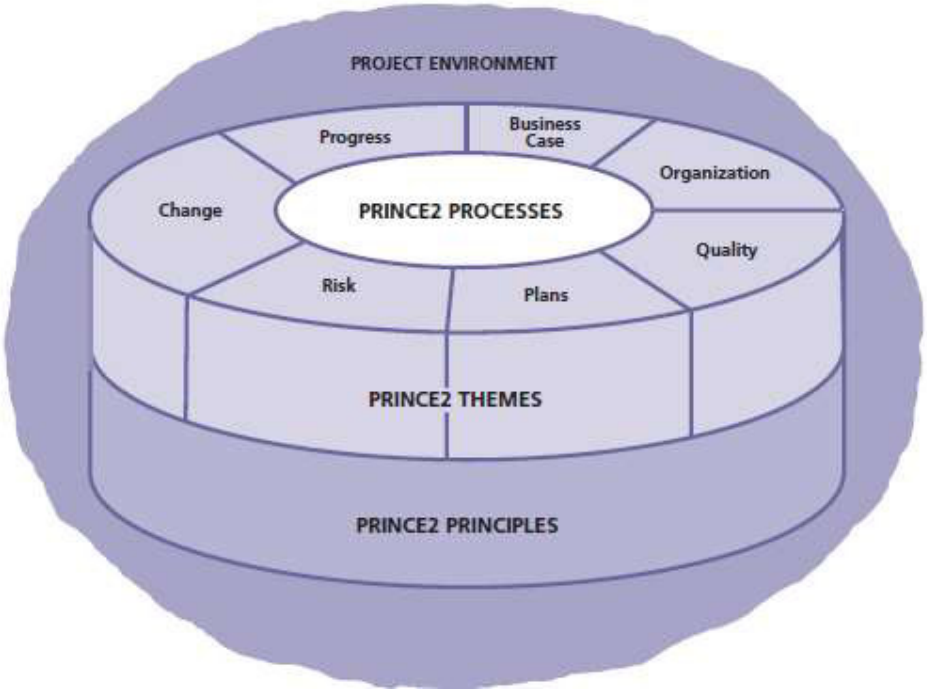
Princip kladoucí důraz na pochopení produktů, které mají být vytvořeny, a kritéria, na základě, kterých budou akceptovány z hlediska kvality. Účelem principu je například zajistit, že na projektu se provádí pouze ty práce, které přímo přispívají k vytvoření produktu, dále pomáhá řídit nekontrolované změny prostředním jejich

podmíněné akceptace, díky nimž také snižuje riziko nespokojenosti uživatelů. (AXELOS, 2017)

7) Přizpůsobení PRINCE2 prostředí projektu

Standard je přizpůsobován projektovému prostředí například na základě velikosti, složitosti a důležitosti projektu, schopnostem týmu a rizikům, díky tomu je jeho použití nezávislé na typu projektu, území nebo kultuře. V této práci je standard přizpůsoben zejména velikosti organizace, kdy jsou ku příkladu sjednoceny projektového role, avšak v takové míře, kterou standard umožňuje, aby nedocházelo ke střetu zájmů. (AXELOS, 2017)

Obrázek 3 - Struktura PRINCE2



Zdroj: Managing Succesful Projects with PRINCE2

Projektové prostředí

Metoda PRINCE2 není striktně definovaná metoda, ale flexibilní rámec, který lze snadno přizpůsobit nezávisle na typu či velikosti projektu, organizaci, geografii nebo kultuře.

Témata

Jedná se o aspekty projektového řízení, které musí být pravidelně průběžně řešeny v průběhu celého projektu. Sedm témat vysvětluje specifické zacházení, které vyžaduje PRINCE2 pro různé disciplíny v rámci řízení projektů a jejich nezbytnost.

1) **Business case (obchodní případ)** – odpověď na otázku PROČ?
2) **Organization (organizace)** – odpověď na otázku KDO?
3) **Quality (kvalita)** – odpověď na otázku CO?
4) **Plans (plány)** – odpovědi na otázky JAK? JAK MOC? KDY?
5) **Risks (rizika)** – odpověď na otázku CO KDYŽ?
6) **Change (změna)** – odpověď na otázku JAKÝ JE DOPAD?
7) **Progress (pokrok)** – odpovědi na otázky KDE JSME NYNÍ? KAM SMĚŘUJEME? MĚLI BYCHOM SE O TO STARAT?

Procesy

Jedná se o sled kroků v průběhu životního cyklu projektu, od zahájení projektu až po jeho ukončení. Každý proces poskytuje kontrolní seznam doporučených činností, produktů a souvisejících odpovědností.

1) Iniciace projektu
2) Zahájení projektu
3) Řízení projektu
4) Kontrola
5) Řízení dodávky produktu
6) Řízení přechodů mezi etapami
7) Uzavření projektu (AXELOS, 2017)

3.3 Evropské nařízení GPDR

GDPR (neboli General Data Protection Regulation) představuje právní rámec ochrany osobních údajů, který je platný ve všech členských státech Evropské unie. Účelem tohoto právního rámce je hájit práva občanů Evropské unie a zamezit neoprávněnému používání těchto dat a osobních údajů.

GDPR vstoupilo v účinnost dne 25. května 2018 a v České republice tak nahradilo tehdejší právní úpravu Směrnici 95/46/ES a také zákon č. 101/2000 Sb., o ochraně osobních údajů. Práva a povinnosti, které zákon definoval byly nahrazeny právy a povinnostmi plynoucími z Obecného nařízení. (Úřad pro ochranu osobních údajů, 2017)

Hlavní změny, které přináší Obecné nařízení GDPR jsou:

1. Nové pojetí odpovědnosti Správce v souvislosti se zajištěním a dokládáním souladu s nařízením GDPR;
2. Standardizované nástroje jako
    a. Kodexy chování,
    b. Osvědčení,
    c. Povinnost vést záznamy o činnostech zpracování za účelem napomoct správci zajistit a prokázat soulad s nařízením,
    d. Povinnost jmenovat pověřence pro ochranu osobních údajů (Data Protection Officer, dále jen DPO);
3. Přístup založený na riziku zpracování osobních údajů, na jehož základu jsou pak definovány různé povinnosti pro jednotlivé správce;
4. Posílení práv Subjektu údajů, včetně vzniku práva na přenositelnost;
5. Definování pravidel pro přenos údajů mimo členské státy EU. (Úřad pro ochranu osobních údajů, 2017)

3.3.1 Základní pojmy

Osobní údaj

Za osobní údaj se považuje jakákoli informace o fyzické osobě, která je identifikována nebo identifikovatelná.

Identifikovatelná fyzická osoba je osoba, u které lze provést nepřímou identifikaci prostřednictvím odkazu na určitý identifikátor, kterým může být například jméno, IP adresa,

telefonní číslo nebo prostřednictvím zvláštních prvků (např. fyzická, genetická, psychická, ekonomická, společenská, kulturní nebo fyziologická identita této osoby) (Nezmar, 2017)

Zpracování osobních údajů

„Zpracováním se rozumí jakákoliv operace nebo soubor operací, která je prováděna s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“ (Žůrek, 2017 str. 30)

Subjekt údajů

Fyzická osoba, které se týkají osobní údaje je dle GDPR subjektem údajů. Za subjekt údajů může být považována pouze fyzická osoba, nikoli právnická. Údaje o právnické osobě nejsou vnímány jako osobní údaje. (Nezmar, 2017)

Profilování

Profilováním je označováno jakékoli automatizované zpracování osobních údajů, které je prováděno za účelem hodnocení vybraných osobních aspektů, které se vztahují k fyzické osobě. Na základě těchto aspektů lze analyzovat a odhadnout další aspekty fyzické osoby, například její ekonomickou situaci, pracovní výkon, zdravotní stav, osobní preference, zájmy, spolehlivost, zvyky nebo i určit současné místo osoby včetně jejího pohybu.

Pseudonymizace

Proces, při kterém jsou osobní údaje zpracovávány tak, aby už nemohlo dojít k jejich přiřazení ke konkrétnímu subjektu údajů. Přiřazení by v tuto chvíli mohlo proběhnout jen za pomocí doplňujících informací, které jsou uloženy odděleně na jiném místě za pomoci dodržování technických a organizačních opatření. (Nezmar, 2017)

Třetí strana

„Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.“ (Žůrek, 2017 str. 31)

3.3.2 Právní tituly (zákonnost zpracování)

V současné době díky nařízení GDPR je možné zpracování osobních údajů pouze za předpokladu, že je přítomen alespoň jeden právní titul (viz níže):

1. **Plnění právní povinnosti**
    - Správce osobních údajů má ze zákona povinnost zpracovávat osobní údaje po dobu stanovenou příslušným zákonem (například archivace záznamů o zaměstnancích)
2. **Plnění smlouvy**
    - Zpracování osobních údajů je nutné pro plnění smluvního závazku
3. **Ochrana životně důležitých zájmů fyzické osoby**
    - Zpracování osobních údajů za účelem ochrany životně důležitých zájmů fyzické osoby
4. **Výkon veřejné moci nebo splnění úkolu v rámci veřejného zájmu**
    - Zpracování osobních údajů ve veřejném zájmu nebo při výkonu veřejné moci, jímž je správce osobních údajů pověřen
5. **Souhlas se zpracováním osobních údajů**
    - Subjekt údajů může udělit Správci osobních údajů souhlas se zpracováním osobních údajů pro jeden nebo více určitých účelů.
6. **Oprávněný zájem**
    - Zpracování osobních údajů za účelem oprávněného zájmu správce nebo třetích stran, vyjma situací, kdy základní práva a svobody subjektů údajů nebo jejich zájmy mají přednost. (Žůrek, 2017)

3.3.3 Souhlas se zpracováním osobních údajů

Souhlas se zpracováním osobních údajů by z pohledu správce měl být poslední možností pro zpracování osobních údajů.

Podmínky k vyjádření souhlasu:

1) Správce musí být schopen prokázat, že mu byl skutečně udělen souhlas se zpracováním osobních údajů daného subjektu údajů;
2) V případě, že souhlas je součástí jiného dokumentu, tak musí být patřičně oddělen od tohoto dokumentu, aby bylo zřejmé, že fyzická osoba poskytla souhlas se zpracováním svých osobních údajů vědomě;
3) Subjekt údajů může využít své právo a souhlas odvolat;
4) V případě posouzení skutečnosti, zda souhlas byl udělen svobodně, je nutné zohlednit skutečnost, zda dané zpracování osobních údajů je nad rámec nutnosti pro plnění smlouvy. (Úřední věstník Evropské unie, 2016)

Souhlas dítěte se zpracováním osobních údajů

Podmínkou, aby byl udělený souhlas zákonný je minimální věková hranice dítěte nejméně 16 let, v ostatních případech je nutné mít souhlas zákonného zástupce dítěte. Členské státy evropské unie však mohou věkovou hranici upravit, avšak ne níže než na věk 13 let.

Správce pro ověření splnění této podmínky vynaloží s ohledem na dostupnou technologii dostatečné úsilí. (Úřední věstník Evropské unie, 2016)

3.3.4 Zvláštní kategorie osobních údajů

Za účelem zvýšení ochrany osobních údajů fyzických osob byla definována zvláštní kategorie osobních údajů (tzv. „citlivé osobní údaje“). Jedná se o takové typy údajů, které mohou při jejich neoprávněném zpracování vést k poškození subjektu údajů, například mu mohou zasahovat do jeho soukromí nebo vést k ohrožení jiných jeho práv jako je zákaz či diskriminace.

Díky tomu musí probíhat zpracování osobních údajů této kategorie při zvýšené ochraně, která je především spjata se stanovením zvláštních právních důvodů na základě, kterých může zpracování dat probíhat, dále vzniká povinnost vést záznamy o činnostech zpracování osobních údajů a v případě jejich rozsáhlého zpracování je nutné provedení posouzení vlivu na jejich ochranu.

V případě, že hlavní činností správce je právě rozsáhlé zpracování tohoto typu údajů, tak správci vzniká povinnost ustanovení pověřence pro ochranu osobních údajů (DPO). (Žůrek, 2017)

„Zvláštní kategorií osobních údajů se podle čl. 9 odst. 1 Obecného nařízení rozumí osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, o zdravotním stavu, sexuálním životě a sexuální orientaci fyzické osoby. Za zvláštní kategorii osobních údajů se považují i genetické a biometrické údaje, avšak pouze pokud jsou zpracovávané za účelem jedinečné identifikace fyzické osoby.“ (Žůrek, 2017 str. 50)

Rodné číslo naopak není považováno za citlivý osobní údaj.

Genetické údaje

Jedná se o údaje popisující zděděné či získané genetické znaky identifikované fyzické osoby.

Biometrické údaje

Osobní údaje o fyzických nebo fyziologických znacích nebo znacích chování fyzické osoby umožňující či potvrzující její jedinečnou identifikaci (otisk prstu, zobrazení obličeje).

Údaje o zdravotním stavu

Osobní údaje, které se týkají tělesného či duševního zdraví určité fyzické osoby, do této kategorie dále spadají i údaje o poskytnutí zdravotních služeb, které mohou popisovat zdravotní stav (například popis zdravotního stavu, údaje o prodělaných nemocech). (Úřední věstník Evropské unie, 2016)

3.3.5 Subjekt údajů a jeho práva

Spolu s GDPR dostaly fyzické osoby v Evropské unii nová práva v rámci ochrany svých osobních údajů.

Právo být informován

Právo se vztahuje k povinnosti správce poskytnout na žádost subjektu údajů pravdivé informace o tom, jak se zpracovávají jeho osobní údaje.

Tabulka 1 - Povinně sdělované informace

Povinně sdělované informace	Zdroj údajů	
	Subjekt údajů	Jiný zdroj
Kontaktní a identifikační údaje Správce a DPO	x	x
Informace o účelu zpracování OÚ a právní titul	x	x
Jaký je oprávněný zájem správce nebo třetí strany		x
Kategorie OÚ		x
Další příjemci/zpracovatelé OÚ subjektu údajů	x	x
Přenos dat mimo EU	x	x
Archivační doba OÚ včetně kritérií	x	x
Poskytnutí informace o jeho právech	x	x
O možnosti odstoupit od smlouvy (pokud je to možné)	x	x
O možnosti podání stížnosti dozorovému úřadu	x	x
Zdroj OÚ		x
Zda poskytnutí OÚ je na základě smlouvy, zákonné povinnosti včetně hrozících následků při jejich neposkytnutí	x	
Zda dochází k automatizovanému rozhodovaní a profilování včetně stanovení významu a důsledků	x	x

Zdroj: GDPR: Praktický průvodce implementací

Poskytnutí informace o zpracovávání osobních údajů nesmí být zpoplatněno, musí být psány jasně a srozumitelně (především, pokud jsou sdělovány dětem), dále musí mít stručnou, jasnou a srozumitelnou formu včetně snadné dostupnosti.

Pokud jsou údaje získány přímo od subjektu údajů, tak informace musí být poskytnuta okamžitě bez zbytečného odkladu, v případě, že jsou údaje získány z jiných zdrojů, tak správce musí poskytnout informace v přiměřené lhůtě, ne však déle než 1 měsíc. Dále v případě poskytnutí údajů třetí straně je nezbytné tuto informaci subjektu údajů sdělit před předáním údajů. (Nezmar, 2017)

Právo na přístup

Fyzická osoba má právo přístupu ke svým osobním údajům, aby mohla ověřit, že zpracování jeho osobních údajů je zákonné na základě některého z právních titulů. Správce osobních údajů je povinen poskytnout subjektu údajů po jeho ověření totožnosti kopii s informacemi o zpracování včetně typu zpracovávaných údajů bezplatně. Avšak ve chvíli, kdy se žádost opakuje bez opodstatněného důvodu může Správce požadovat poplatek ve výši jeho administrativních nákladů na úkol. Odpověď na žádost musí dle nařízení proběhnout ve lhůtě do 1 měsíce, Správce může požádat o prodloužení lhůty o další dva měsíce, pokud

je vyřízení úkolu složité a časově náročné. Pokud Správce není schopen žádost vyřídit, musí v tomto případě uvědomit subjekt údajů o důvodu nevyřízení včetně jeho informování o právu podat stížnost dozorovému úřadu. (Nezmar, 2017)

Právo na opravu

V případě nepřesných nebo neúplných údajů, může subjekt údajů požádat o jejich opravu.

Právo na výmaz

Právo na výmaz je také často označováno, jako právo být zapomenut a umožňuje subjektu údajů podat žádost o výmaz jeho osobních údajů i v případě existence dalšího přesvědčivého důvodů dalšího zpracování. Správce je povinen zajistit výmaz údajů i u zpracovatelů třetích stran, pokud existuje za předpokladu, že to nevyžaduje vynaložení nepřiměřeného úsilí.

Toto právo lze uplatnit pouze za následujících okolností:

1) Osobní údaje už není třeba zpracovávat za účelem, kvůli kterému byly původně shromážděny a zpracovávány;
2) Subjekt údajů odvolá svůj souhlas se zpracováním (v případě, že zpracování bylo založeno na tomto právním titulu a neexistuje jiný právní titul);
3) Při vznesení námitky proti zpracovávání osobních údajů a Správce nemá jiný oprávněný zájem data zpracovávat (oprávněným zájmem může být pracovněprávní vztah);
4) Zpracování osobních údajů bylo protiprávní;
5) U dětí nebyl udělen souhlas zákonného zástupce;
6) Existuje povinnost údaje vymazat na základě Unijního práva nebo práva členského státu.

Odmítnutí žádosti na výmaz osobních údajů subjektů údajů může být v případě existence jiného zákonného účelu zpracování. (Nezmar, 2017)

Právo na omezení zpracování

Omezení zpracování osobních údajů spočívá v tom, že Správce při omezení může pouze uchovávat údaje bez následného zpracování.

Omezit zpracování lze za níže uvedených důvodů:

1) Ze strany subjektu údajů byla zpochybněna přesnost zpracovávaných údajů (omezení platí do ověření přesnosti);
2) Při vznesení námitky proti zpracování;
3) Při protiprávním zpracování, kdy subjekt údajů nepožaduje výmaz údajů, ale jich omezení;
4) Pro správce údajů už údaje nejsou potřebné, ale subjekt údajů je vyžaduje např. kvůli obhajobě svých právních nároků. (Nezmar, 2017)

Právo na přenositelnost dat

Podstatou práva je umožnění a usnadnění přenosu osobních údajů, aby subjekt údajů mohl přenést a využívat své údaje pro vlastní účely.

Údaje budou poskytnuty žadateli ve strukturované elektronické podobě např. CSV, XLS, XML.

Toto právo lze využít za následujících okolností:

1) Subjekt údajů sám údaje poskytl správci;
2) Zpracování osobních údajů je založeno na plnění smlouvy nebo poskytnutého souhlasu, a
3) Dochází k automatizovanému zpracování v informačním systému.

Pokud správce nemá automatický proces, který mu umožní jednoduše data ze systému exportovat, tak není jeho povinností vynaložit nepřiměřené úsilí k jejich shromáždění a přenosu. (Nezmar, 2017)

Právo na podání stížnosti či námitky

Subjekt údajů má právo kdykoli podat stížnost nebo námitku proti zpracování jeho osobních údajů, prováděné na základě právního titulu, kdy:

1) je nezbytné zpracování pro dokončení úlohy, která je ve veřejném zájmu nebo za účelem výkonu veřejné moci, kdy správce je tímto úkolem pověřen;
2) správce nebo třetí strana má oprávněný zájem pro zpracování osobních údajů subjektu údajů;
3) Pokud důvodem zpracování údajů je přímý marketing, tak při podání námitky musí správce okamžitě zastavit takové zpracování. (Žůrek, 2017)

Právo spojené s automatizovaným rozhodováním včetně profilování

Jedná se o právo nebýt součástí automatizovaného zpracování, které má za následek právní či obdobné účinky vůči subjektu údajů.

Automatizované zpracování je možné jen za předpokladu, že je to nezbytné k uzavření či plnění smlouvy mezi fyzickou osobou a správcem (např. banky a ověřování bonity klienta).

Při automatizovaném zpracování osobních údajů zvláštní kategorie, je nezbytné mít souhlas fyzické osoby nebo tak musí být činěno ve veřejném zájmu, s tím však je nutné zavést vhodný systém opatření, které zajistí práva, svobody a oprávněné zájmy subjektů údajů. (Žůrek, 2017)

3.3.6 Zásady nařízení GDPR

Evropské nařízení o ochraně osobních údajů definovalo šest zásad, na které lze hledět jako na seznam nejvíce důležitých povinností, které by správci osobních údajů měli dodržovat pro zajištění souladu s nařízením.

1. Zásada zákonného, korektního a transparentního zpracování;
2. Zásada účelového omezení;
3. Zásada minimalizace údajů;
4. Zásada dodržování přesnosti;
5. Zásada omezení uložení;
6. Zásada zachování integrity a důvěrnosti při zpracovávání osobních údajů.

Dále však z nařízení vyplývají další zásady, které se týkají:

1. Správcovi odpovědnosti za zpracovávaná data;
2. Správcovi povinnosti prokázat soulad s nařízením;
3. Zajištění bezpečnosti údajů;
4. Zvýšeného důrazu na přenos dat mimo EU.

(Nezmar, 2017)

3.3.7 Správce a Zpracovatel osobních údajů

Správce osobních údajů

Správce je hlavní subjekt v rámci zpracovávání osobních údajů, neboť bez jeho existence by vůbec nemohlo k této činnosti docházet, protože právě správce určuje, pomocí jakých prostředků bude zpracovávání osobních údajů probíhat včetně určení účelů.

Dle nařízení je správce jakákoli fyzická nebo právnická osoba, agentura, orgán veřejné moci nebo jakýkoli jiný subjekt, jenž sám či případně společně s jinými subjekty stanovuje účel zpracování osobních údajů včetně použitých prostředků. Správce vystupuje jako hlavní adresát v rámci povinnosti k GDPR a jeho funkce není závislá na jeho právní formě či statusu, ale na tom, že naplňuje hlavní znaky zpracování.

Povinnosti jsou na každého správce kladeny různě, neboť je zde aplikován přístup založený na riziku, které zpracování přináší. Na základě této diference je nezbytné, aby každý správce kladl důraz na správné pochopení povinností, které mu v jeho pozici z nařízení plynou. Odpovědnosti se nelze zbavit ani přenesením zpracování na zpracovatele osobních údajů, protože správce je neustále zodpovědný za dodržování souladu s nařízením včetně dodržování souladu jeho pověřených zpracovatelů. (Žůrek, 2017)

Společní správci

Ačkoli v nařízení není o společných správcích detailnější ustanovení, tak společní správci mohou existovat. Vyznačují se zejména tím, že stanovují společně mezi sebou účely a prostředky. Pro společné správce je nezbytné, aby si mezi sebou definovali soubor odpovědností.

Když si představíme tento vztah v praxi, tak se bude jednat o situaci, kdy na projektu více subjektů zpracovává osobní údaje. (příklad: vyhlášení soutěže automobilky mezi dealery). (Žůrek, 2017)

Zpracovatel osobních údajů

Zpracovatel je správcem určený subjekt, který má za úkol zpracovávat správcem svěřené osobní údaje o subjektech údajů předem dohodnutým způsobem. Zpracovatel sám neurčuje účely nebo prostředky zpracovávání osobních údajů. Ačkoli se jedná o zprostředkovaný subjekt, který zpracovává osobní údaje pro správce, tak i v tomto případě

musí být zpracovatel v souladu s nařízením GDPR a je to zároveň povinností správce, aby tuto skutečnost ohlídal a zpravidla smluvně zajistil včetně stanovení incident managementu pro případ porušení ochrany osobních údajů. (Žůrek, 2017)

3.3.8 Zabezpečení osobních údajů

Jedním z hlavních předpokladů k dosažení souladu s GDPR je nezbytné mít řádně zabezpečené osobní údaje, a to jak ze strany správce osobních údajů, tak i všech jeho zpracovatelů.

GDPR přesně nedefinuje jednotné požadavky na systém zabezpečení osobních údajů, neboť mezi správci je v mnoha směrech velká odlišnost, ať už z hlediska velikosti subjektu, jeho prostředků i typu zpracovávaných osobních údajů atp.

Systém zabezpečení osobních údajů je založen na přístupu zohledňující rizika zpracování a každý správce je povinen zabezpečit osobní údaje takovým způsobem, který poskytuje řádnou ochranu při zohlednění používané techniky, finančních zdrojů, dále účely zpracovávání osobních údajů včetně jejich rozsahu, povahy a kontextu, možná rizika, která plynou ze zpracování a které mohou ohrozit práva a svobody subjektů údajů. (Nezmar, 2017)

Za vhodná technická a organizační opatření se považují například:

- Provádět šifrování údajů a jejich pseudonymizaci;
- Schopnost zajištění bezpečnosti, dostupnosti, integrity a důvěry používaných systémů;
- Zajištění záloh osobních údajů pro případ vzniku fyzického nebo technického incidentu, aby byla zajištěna jejich dostupnost včetně snadného přístupu;
- Zavedení systému pravidelných testů, které budou posuzovat a hodnotit zavedená technická a organizační opatření;
- Zavedení mechanismů sledující možné neoprávněné přístupy do systémů nebo zvláštních činností v síti (možné využití logů);
- Provedení penetračních testů (zejména klíčových systémů).

(Nezmar, 2017)

3.3.9 Posouzení vlivu na ochranu osobních údajů

Obecné nařízení GDPR zavedlo nový nástroj, který má posuzovat, jestli zpracování osobních údajů může vysoce ohrozit práva a svobody subjektů údajů. Tento nástroj je nazván Posouzení vlivu na ochranu osobních údajů neboli také test DPIA (Data Protection Impact

Assessment). Zejména se jedná o takové zpracování. které svým rozsahem, povahou, kontextem či účelům může být považováno za rizikové nebo jsou při něm využívány nové technologie. (PRIVAZYPLAN, 2018)

Pro účely posouzení, zda je nutné provést DPIA vydal Úřad pro ochranu osobních údajů příručku pro sebehodnocení správce osobních údajů z hlediska rizikovosti zpracování. Sebehodnocení se skládá z deseti kritérií zpracování, které je dále rozčleněno do třech způsobů zpracování osobních údajů, které nabývají hodnot kritické hodnoty, významné hodnoty a nízké hodnoty s popisky jednotlivých případů zpracování. Správce na základě těchto kritérií přiřadí své zpracování k těmto hodnotám.

10 kritérií pro sebehodnocení

1. Zpracování osobních údajů zahrnuje monitorování subjektů údajů;
2. Zpracování údajů, které umožňují přímou identifikaci a/nebo těch, které mají vysoce osobní povahu pro subjekty údajů;
3. Zpracování údajů, jenž může subjekty údajů vystavit ohrožení z okolního prostředí;
4. Zpracování velkého rozsahu osobních údajů;
5. Zpracování, které zahrnuje monitorování veřejně přístupných prostor;
6. Zpracování osobních údajů, které mohou subjekty údajů ovlivnit v omezeném rozsahu;
7. Zpracování osobních údajů, které jsou veřejně přístupné;
8. Zpracování osobních údajů, využívající složité nebo pokročilé technické infrastruktury či platformy;
9. Zpracování osobních údajů jinými správci či zpracovateli;
10. Zpracování osobních údajů prostřednictvím nových technologických či organizačních řešení.

Systém vyhodnocení výsledků:

- pokud dvě a více odpovědí jsou v kritických hodnotách, tak musí správce zpracovat DPIA;
- pokud jedna odpověď je v kritických hodnotách a alespoň pět se jich nachází ve významných hodnotách, tak opět musí správce zpracovat DPIA.
  (ÚOOÚ, 2018)

3.3.10 Předávání osobních údajů mimo EU

Předávání osobních údajů je také forma zpracování osobních údajů, které je však nezbytné věnovat vyšší pozornost, protože v zemích mimo EHP fungují jiné přístupy k ochraně osobních údajů a s tím jsou spojena různá rizika pro subjekty údajů. Předáváním osobních údajů však není myšleno pouze předání údajů správcem v jedné zemi, zpracovateli, který se nachází v zemi mimo Evropskou unii, ale je tím také myšleno i zpřístupnění těchto údajů.

Aby nedocházelo k situacím, kdy by se správce osobních údajů chtěl cíleně zbavit zodpovědnosti za požadavky, které klade nařízení GDPR tím, že si za zpracovatele vybere instituci, která se nenachází na území EHP, tak je podmínkou správce používat jen takové zpracovatele osobních údajů, které jsou v souladu s GDPR nařízením nebo jejich úroveň ochrany osobních údajů byla uznána Evropskou unií, jako dostatečná úroveň a zároveň poskytují dostatečné záruky, zejména ve smyslu uplatnění práv subjektů údajů.

Takovým příkladem můžou být například společnosti na území USA, které jsou součástí tzv. Privacy Shield. (Žůrek, 2017)

4 Charakteristika podniku

Vybraná společnost je fintechový startup zabývající se poskytováním platebních služeb. Na českém trhu působí od roku 2017 jako licencovaný poskytovatel platebních služeb malého rozsahu, kde nabízí produkt pro fyzické a právnické osoby ve formě platební platformy využívající inovativní technologii blockchainu pro odesílání a příjem plateb, což klientům umožňuje provádět mezinárodní platby i mimo EHP s okamžitým zprocesováním namísto běžných 3-5 pracovních dnů. Dále poskytují klasické bankovní účty, směnné operace, vydávání debetních platebních karet a obchodování s kryptoměnami, které lze použít i pro charitativní účely.

Cílovými segmenty společnosti jsou však především malé a střední podniky a fyzické osoby působící v České republice, Polsku, Maďarsku, Slovenské republice a ve Velké Británii.

Organizační struktura

Společnost v současné době zaměstnává 7 zaměstnanců a pro své projekty využívá ve velké míře služby externích agentur a freelancerů. Interní zaměstnanci jsou na pozicích (viz níže na grafu organizační struktury).

Obrázek 4 - Organizační struktura společnosti

	interní zaměstnanec na plný úvazek
	externí zaměstnanec
	zaměstnanec na zkrácený úvazek

Zdroj: Vlastní zpracování

Projektové řízení v organizaci

V organizaci není vytvořena samostatná projektová kancelář, která by určovala metodické postupy pro řízení projektů nebo stanovila konkrétní standard řízení projektů. V současné době se společnost pokouší osvojit si řízení projektů pomocí mezinárodně uznávaného projektového standardu PRINCE2.

5 Vlastní práce – Projekt implementace GDPR

5.1 Předprojektová fáze

V předprojektové fázi byl definován základní cíl projektu, rozsah, časové ohraničení a předpokládané náklady prostřednictvím mandátu projektu (Project mandate), který byl odeslán ředitelem společnosti projektovému manažerovi.

Tabulka 2 - Project mandate

Project mandate	
Projektový manažer:	Martin Valeš
Cíl projektu:	Analyzovat současný stav společnosti z hlediska zpracování osobních údajů, identifikovat činnosti, rozsah zpracování, naplnění základních požadavků kladených Obecným nařízením GDPR.
Důvody pro projekt	- zákonná povinnost dosažení souladu organizace s nařízením GDPR - snížení rizika poškození dobrého jména společnosti a renomé - odstranění rizika spojeného s udělením pokuty společnosti za nedodržování souladu - mít data pod kontrolou (systematická evidence)
Rámcová doba projektu a náklady	2 měsíce 50 000 Kč rozpočet na právní služby

Zdroj: Vlastní zpracování

5.1.1 Project brief

Na základě obdrženého dokumentu Project mandatu byl vypracován iniciační dokument Project brief, který rozšiřuje Project mandate o hrubý návrh Business casu, kde jsou definovány důvody projektu, očekávané přínosy, nevýhody, časová náročnost, odhadnuté náklady, zhodnocení investice a hlavní rizika projektu.

Tabulka 3 - Project brief

Project brief	
Projektový manažer:	Martin Valeš
Definice projektu:	Projekt je zaměřen na implementaci požadavků Obecného nařízení GDPR v rámci organizace.
Cíl projektu:	Cílem projektu je analýza současného stavu manipulace s osobními údaji, zjištění slabých či kritických míst, která nejsou v souladu s nařízením a zajistit vytvoření základní dokumentace pro nabytí souladu, tj. například Směrnice o ochraně osobních údajů, informační memorandum, metodika vyřizování požadavků subjektů údajů.
Outline Business case	
Důvody pro projekt	- zákonná povinnost dosažení souladu organizace s nařízením GDPR - snížení rizika poškození dobrého jména společnosti a renomé - odstranění rizika spojeného s udělením pokuty společnosti za nedodržování souladu - mít data pod kontrolou (systematická evidence)
Očekávané přínosy	- vytvoření registru činností s detailním popisem o zpracování osobních údajů - vytvoření jednotné metodiky pro řešení žádostí subjektů a systému zpracování osobních údajů - posílení dobrého jména společnosti
Očekávané nevýhody	- žádné

Časová náročnost	- 2 měsíce
Náklady	50 000 Kč rozpočet na právní služby
Zhodnocení investice	odvrácení hrozící pokuty v závislosti na míře závažnosti poručení nařízení až do výše: - 10 000 000 EUR (nebo až do 2% celosvětového ročního obratu podniku) - 20 000 000 EUR (nebo až do 4% celosvětového ročního obratu podniku)
Hlavní rizika	- neochota zaměstnanců poskytovat veškeré informace o zpracování osobních údajů - pasivní přístup zaměstnanců k povinnostem nařízení - nedodržování korektních postupů
Popis produktu projektu	- vytvoření Směrnice o ochraně osobních údajů - vytvoření Informačního memoranda na internetové stránky společnosti - vytvoření Metodiky řízení výkonu práv subjektů
Projektový přístup	- v projektu bude zapojena externí advokátní kancelář, která bude revidovat soulad podniknutých kroků s nařízením - dále budou kvůli malému počtu zaměstnanců spojeny určité projektové role, avšak v povoleném rozsahu, který umožňuje PRINCE2, aby nedocházelo ke střetu zájmů

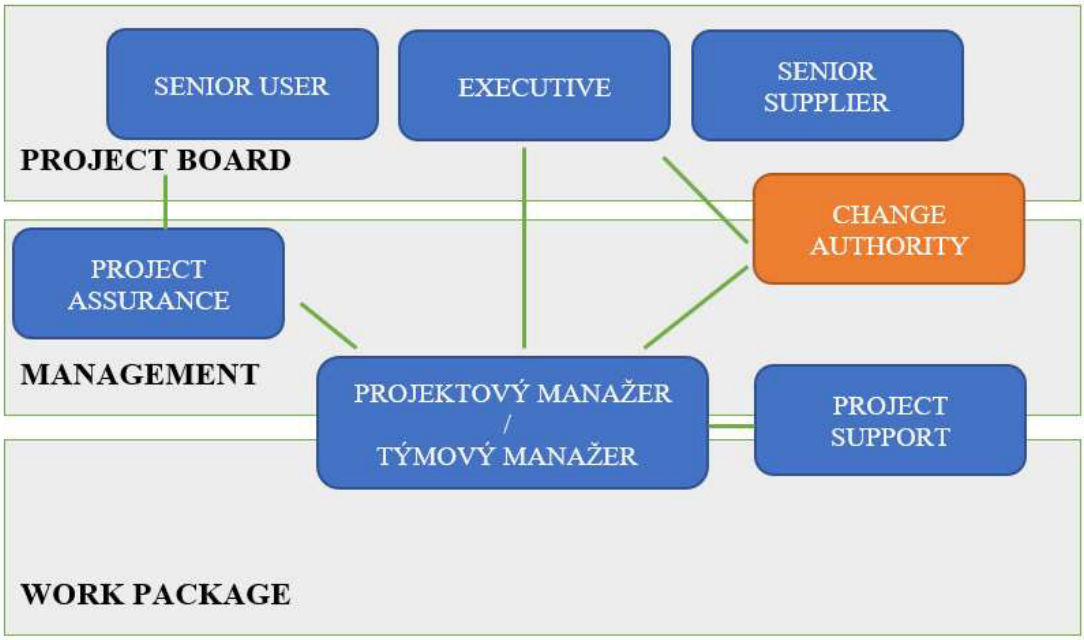
Zdroj: Vlastní zpracování

Organizační struktura projektu

Pro účely projektu a v návaznosti na velikost a strukturu vybrané společnosti muselo dojít k přizpůsobení funkční organizační struktury projektu, kdy došlo ke spojení určitých rolí, avšak v takovém rozsahu, jaký umožňuje tailoring projektového standardu PRINCE2, aby nedocházelo ke střetu zájmů jednotlivých rolí.

Společnost je kategorizována jako malá společnost do 50 zaměstnanců, a tudíž zde vrcholový management společnosti a Executive projektu zastává jedna osoba, kterým je jednatel společnosti, a proto není nad Project boardem v níže uvedeném schématu vyobrazen vrcholový management. Dále došlo ke spojení funkce projektového a týmového manažera, který také zastává jedna osoba a v poslední řadě Project board zastává role Project Assurance, Change Authority a Project Support.

Obrázek 5 - organizační struktura projektu



Zdroj: Vlastní zpracování

Tabulka 4 - Rozdělení rolí

Executive	Jednatel společnosti	
Senior User	Produktový manažer	
Senior Supplier	Právník	
Project Manager	Projektový manažer	Martin Valeš
Team Manager	Projektový manažer	Martin Valeš
Project Assurance	Project Board	
Project Support	Project Board	
Change Authority	Project Board	

Zdroj: Vlastní zpracování

Popis rolí

Tabulka 5 - Popis projektových rolí

Role	Popis role
Executive	Určuje projektového manažera, schvaluje zadání projektu a strukturu projektového týmu, schvaluje přístup k řízení komunikace v projektu.
Senior User	Definuje a ověřuje požadavky a očekávání uživatelů.
Senior Supplier	Poskytuje zdroje dodavatele. Informuje o požadavcích nařízení.
Project Manager	Připravuje a aktualizuje řízení komunikace. Navrhuje, přezkoumává a aktualizuje strukturu projektového týmu. Plánuje a zapojuje zainteresované strany. Definuje projektové role.
Team Manager	Řídí členy projektového týmu. Poskytuje poradentství projektovému týmu a zajišťuje účast zainteresovaných stran na projektu.
Project Assurance	Poskytuje poradentství při výběru projektového týmu a zapojení zainteresovaných stran. Zajištuje vhodný přístup řízení komunikace a kontroluje jeho uskutečnění.
Project Support	Poskytuje administrativní podporu projektovému týmu.
Change Authority	Schvaluje a připomínkuje návrhy na změny v projektu.

Zdroj: Vlastní zpracování

Reference: Project mandate

5.1.2 Lessons Log

Za účelem naplnění principu Lessons learned byl vypracován dokument Lessons Log, který bude sloužit projektovému manažerovi k zaznamenávání událostí, které měly na projekt pozitivní nebo negativní vliv a společnost je může v budoucnu použít jako poučení pro příští projekty.

Název projektu	**Projekt implementace GDPR nařízení**				
Datum:	2.1.2019	Release		Draft/Final	Draft
Autor:	Projektový manažer				
Vlastník:	Projektový manažer				
Klient:	Společnost				

Revizní historie				
Datum revize	**Předchozí datum revize**	**Souhrn změn**	**Priorita změn**	**Schválil**

Zaznamenaná poučení					
ID	**Oblast**	**Popis**	**Dopad na projekt**	**Plynoucí doporučení**	**Datum zápisu a jméno pracovníka**

5.1.3 Daily Log

Pro zaznamenání otevřených bodů nebo jiných významných skutečností či událostí v projektu, pro které neexistují samostatné registry byl vytvořen dokument Daily Log neboli deník projektového manažera.

Název projektu:	**Projekt implementace GDPR nařízení**				
Datum:	2.1.2019	Release		Draft/Final	Draft
Autor:	Projektový manažer				
Vlastník:	Projektový manažer				
Klient:	Společnost				

Revizní historie				
Datum revize	**Předchozí datum revize**	**Souhrn změn**	**Priorita**	**Schválil**

Seznam otevřených bodů				
Datum	**Popis problému, akce, události**	**Zodpovědná osoba**	**Cílové datum**	**Výsledek**

5.2 Iniciační fáze

V iniciační fázi dojde k rozšíření projektové dokumentace, která vznikla v předprojektové fázi, kde byly vydefinovány základní požadavky na projekt včetně prvotních odhadů pracnosti a finanční náročnosti projektu. Dále byla definována struktura

zainteresovaných stran projektu s využitím tailoringu podle PRINCE2. Dokumentace v iniciační fázi se bude zejména soustřeďovat na plánování projektu.

Hlavními dokumenty v této fázi jsou:

1. **PID (Project Initiation Documents)**,
2. **Kontrolní plán přínosů (Benefits Review Plan)**
3. **Registry kvality, problémů a rizik**

5.2.1 Project Initiation Documents

PID se skládá z:

- **a.** Strategie řízení komunikace (Communications Management strategy)
- **b.** Strategie řízení konfigurace (Configuration Management strategy)
- **c.** Strategie kvality (Quality strategy)
- **d.** Strategie rizik (Risk strategy)
- **e.** Business case
- **f.** Projektový plán
  - **i.** popis produktu
  - **ii.** směrný plán
- **g.** Stanovení rolí projektového týmu

5.2.1.1 Strategie řízení komunikace

Strategie řízení komunikace zajišťuje, že v projektu implementace GDPR nařízení jsou všechny zainteresované strany projektu informovány o veškerých relevantních informací o projektu. Projektový manažer je zodpovědný za efektivní komunikaci v projektu.

Nástroje a techniky

Systém Bitrix24

Hlavním komunikačním nástrojem mezi zainteresovanými stranami je softwarový nástroj Bitrix24, kde jsou zaznamenány veškeré úkoly projektu, včetně stanovení jejich finálních termínů, popisu, odpovědné osoby, participantů a nahlížejících osob.

E-mailová komunikace

Do každé emailové komunikace týkající se projektu implementace GDPR nařízení bude do kopie zprávy přidán projektový manažer. V případě přiřazení vysoké priority dané zprávě, bude přidán také ředitel společnosti.

Veškeré dokumenty vzniklé v projektu se budou ukládat do:

- sdílené složky na serveru společnosti \\název_serveru\společnost\GDPR
- Bitrix24, který bude také využit jako dočasné úložiště souborů, které jsou ve fázi editace a připomínkování

Reporting: pravidelné porady každé pondělí 10:00 – 11:30

Kontaktní osoby třetích stran

Tabulka 6 - kontaktní osoby třetích stran

Role	Kontaktní osoba	Telefon	E-mail
Právník – AK XXX	JUDr. Karel Novák	+420 111 222 333	pravnik@akxxx.cz
IT specialista	Marek Novotný	+420 222 444 555	it@xxx.cz

Zdroj: Vlastní zpracování

Potřebné informace vůči zainteresovaným stranám

Tabulka 7 - informační potřeby

Zainteresovaná strana	Předávané informace	Přijímané informace	Příjemce informace	Frekvence komunikace	Forma komunikace
Projektový manažer	stav projektu informace o úkolech	změnové požadavky průběh úkolů	Project board členové týmu	týdenní / ad-hoc ad-hoc	Email, porada Email, porada
Členové týmu	průběh úkolů	požadavky pro úkol	projektový manažer	týdenní / ad-hoc	Email, porada
Project board	změnové požadavky	stav projektu	projektový manažer	týdenní / ad-hoc	Email, porada

Zdroj: Vlastní zpracování

5.2.1.2 Strategie řízení konfigurace

Strategie řízení konfigurací má za úkol odpovědět na témata:

- uložení projektových produktů (kde a jak)
- zabezpečení produktů
- schválení změn produktů (kdo schvaluje, jakou formou)

Uložení a zabezpečení produktů

Úložiště souboru (tj. produktů projektu) se nachází na interním serveru společnosti, případně v systému Bitrix24, kde dochází k editaci a připomínkování dokumentů. Bližší informace jsou k dispozici v komunikační strategii.

Veškeré dodané dokumenty (produkty) budou uloženy v elektronické, editovatelné podobě do příslušného adresáře. Externí strany, které nemají přístup na server společnosti, zašlou finální verzi dokumentu elektronicky emailem projektovému manažerovi.

Pro odesílání dokumentů je zakázáno používat jakékoli volně přístupné internetové úložiště, jako je např. www.ulozto.cz a podobné služby.

Změna konfigurace produktů

Změna konfigurace produktů podléhá přímému schválení Project boardu a to výhradně písemnou formou.

5.2.1.3 Strategie kvality

Kontrola kvality

Produkty vytvořené v rámci projektu budou kontrolovány z hlediska kvality pomocí předem vytvořených checklistů, které budou vycházet z detailního popisu produktů.

Checklist bude tvořen souborem otázek a odpovědí typu ano/ne, kdy pro akceptaci vytvořeného produktu je nutné, aby na všechno otázky bylo odpovězeno ano.

V případě, že produkt nebude schválen, musí být veškeré informace o průběhu kontroly a zjištěných nedostatků zaznamenáno do seznamu otevřených bodů (daily log), a do registru kvality (viz níže).

Tabulka 8 - Registr kvality

ID	Produkt	Metoda měření kvality	Vytvořil	Zkontroloval	Schválil	Datum kontroly	Výsledek

Zdroj: Vlastní zpracování

5.2.1.4 Strategie řízení rizik

Stanovení strategie řízení rizik musí pokrývat minimální požadavky, které klade projektový standard PRINCE2, tj.:

1. definice způsobu identifikace a ohodnocení rizik, jak jsou naplánovány a realizovány reakce na řízení rizik a jak je řízení rizik komunikováno v rámci životního cyklu projektu;
2. posouzení, zda by identifikovaná rizika mohla mít významný dopad na podnikové odůvodnění (princip neustálého zdůvodňování projektu);
3. role a odpovědnosti při řízení rizik;
4. vytvoření a aktualizace registru rizik;

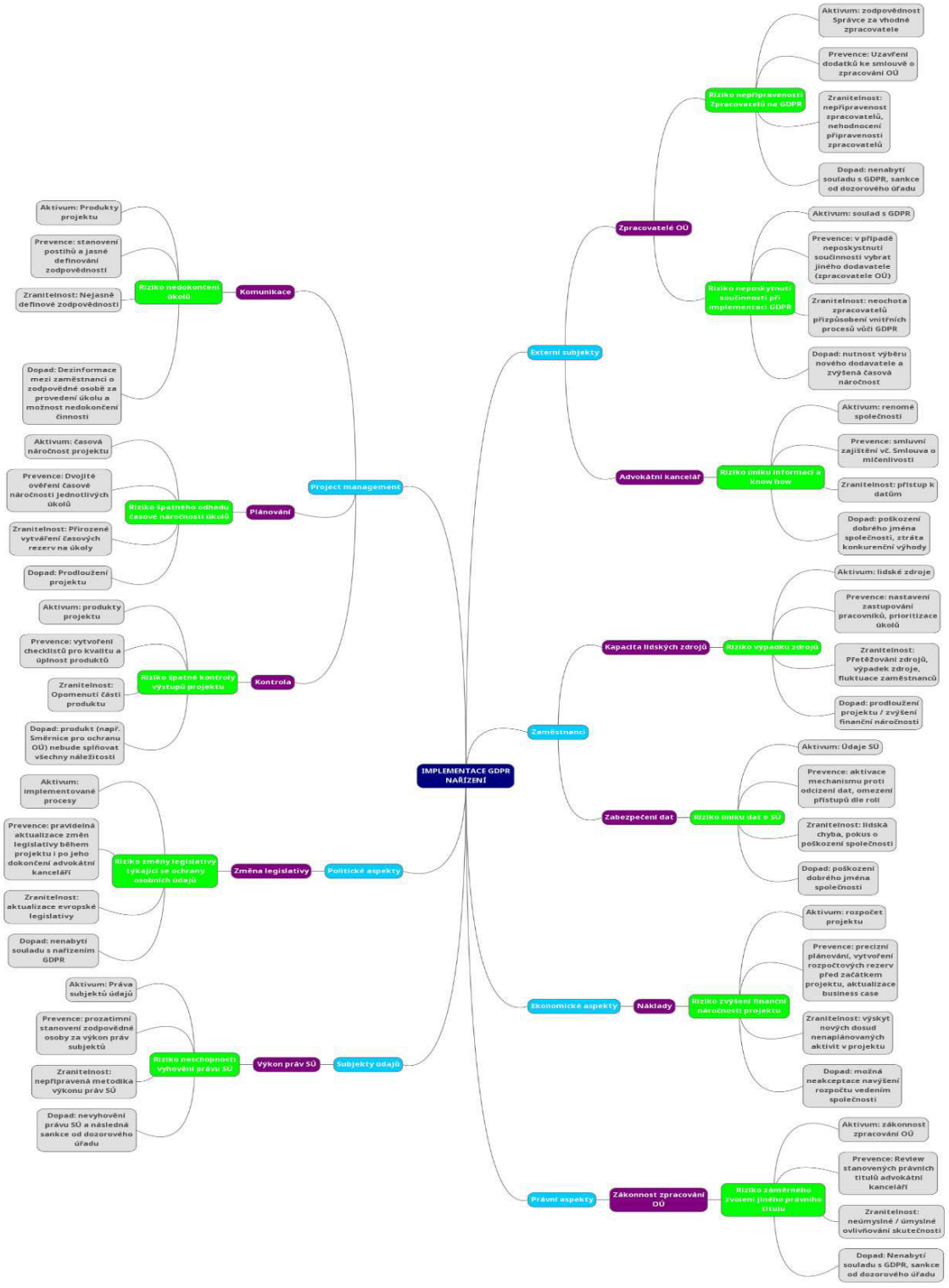
5. definice systému zajištění aktuálního registru rizik;
6. zaznamenání získaných zkušeností z řízení rizik v projektu (princip lessons learned).

Identifikace rizik

K identifikaci rizik bude využita metoda brainstormingu, kde budou nejprve definovány obecné hrozby, které budou detailně dekomponovány na konkrétní rizika a RBS (Risk Breakdown Structure) ke grafickému znázornění a základní kategorizaci dle kritických míst projektu.

Úvodní identifikace rizik proběhla před začátkem projektu v rámci mimořádné schůzky, kde byla vytvořena celková dokumentace PID a registry. Schůzky, a tedy i identifikace rizik se zúčastnily všechny zainteresované strany projektu.

Obrázek 6 - RBS



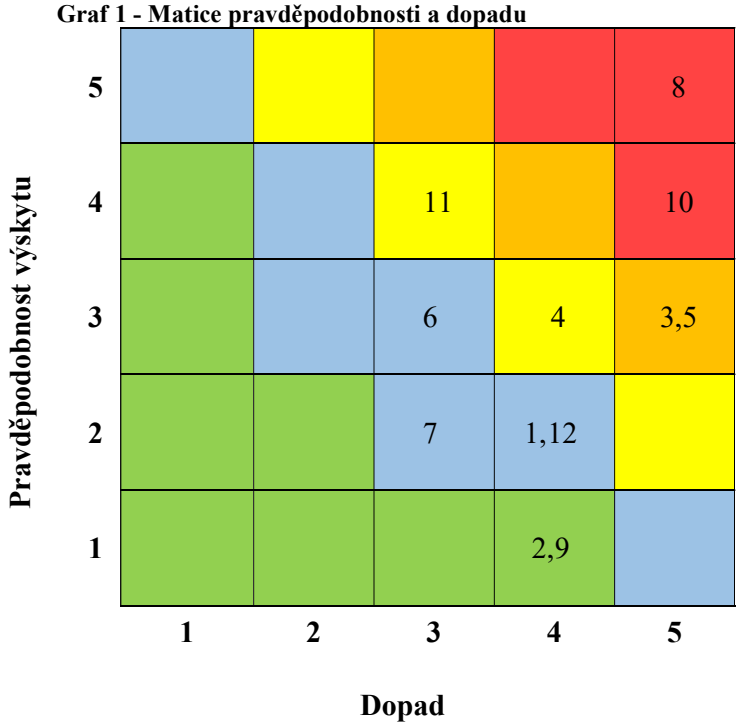
Zdroj: Vlastní zpracování

Ohodnocení rizik

Stanovená rizika budou podrobena kvantitativní analýze, ze které budou určena „Očekávané hodnoty rizik“ (dále jen OHR).

Stanovení OHR bude vypočteno prostřednictvím matice pravděpodobnosti a dopadu (Probability Impact Grid). Pro určení pravděpodobnosti a dopadu rizika byla zvolena stupnice 1-5, kdy 1 znamená nízkou míru pravděpodobnosti / dopadu rizika na projekt.

Graf 1 - Matice pravděpodobnosti a dopadu



Zdroj: Vlastní zpracování

Tabulka 9 - Legenda Matice pravděpodobnosti a dopadu

Hodnota OHR	Významnost rizika
1-4 b	Malá
5-9 b	Střední
10-14 b	Vysoká
15-19 b	Velmi vysoká
vyšší rovno 20 b	Kritická

Zdroj: Vlastní zpracování

Registr rizik

Výstupem identifikace rizik je Registr rizik, kde jsou pravidelně zaznamenávány a aktualizovány identifikovaná rizika. Níže je uvedena předpřipravená struktura, která vznikla v rámci mimořádné schůzky, kde byl definován k rizikům dopad a výskyt. Kompletní registr rizik je uveden v příloze č.1 této práce.

Tabulka 10 - Registr rizik s definovanými dopady a výskyty rizik

ID	Odpovědná osoba	Popis	Scénář	Dopad	Výskyt	OHR
1	Právník	Riziko nepřipravenosti zpracovatelů na GDPR	Námi vybraní zpracovatelé nejsou v souladu s GDPR (nebylo kontrolováno ani smluvně zajištěno)	4	2	8
2	Finanční manažerka	Riziko neposkytnutí součinnosti při implementaci GDPR	Zpracovatel odmítne podepsat dodatek ke smlouvě o zpracovávání osobních údajů.	4	1	4
3	Projektový manažer	Riziko úniku informací a know-how	Externí zaměstnanci vynesou know-how společnosti	5	3	15
4	Ředitel	Riziko výpadku zdrojů	Zaměstnanec podá výpověď / nebude moct pracovat z důvodu nemoci	4	3	12
5	Ředitel	Riziko úniku dat o subjektu údajů	Zaměstnanci zveřejní / smažou údaje SÚ	5	3	15
6	Projektový manažer	Riziko zvýšení finanční náročnosti projektu	Při projektu budou nalezeny další nezbytné aktivity pro nabytí souladu s GDPR.	3	3	9
7	Právník	Riziko záměrného zvolení jiného právního titulu	Pracovník zvolí jiný typ právního titulu, aby mohl pokračovat ve zpracování osobních údajů.	3	2	6

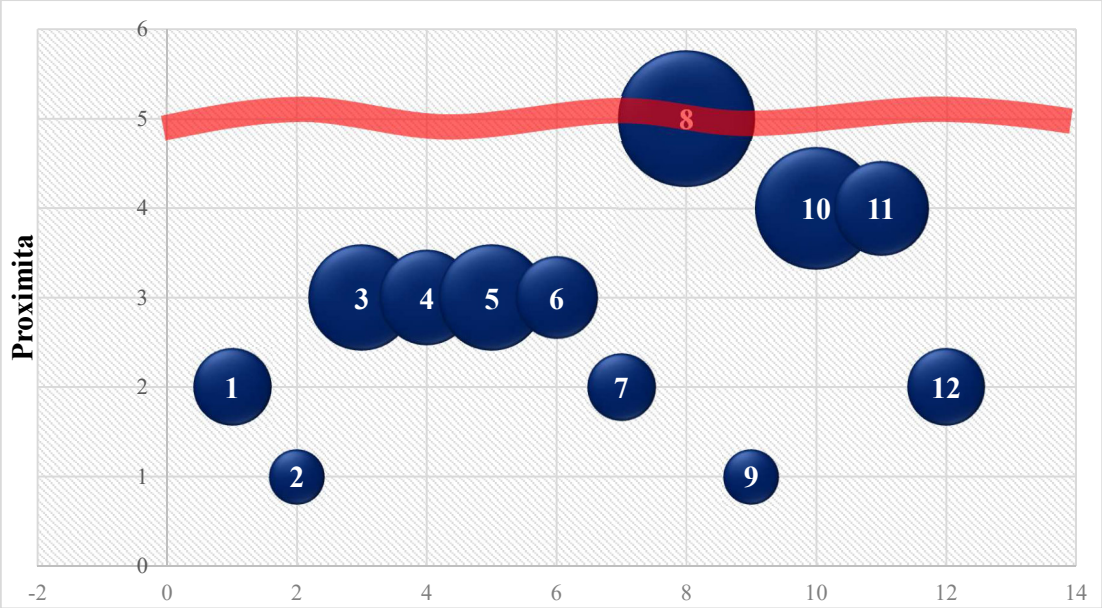
8	Ředitel	Riziko neschopnosti vyhovění právu subjektu údajů	Subjekt údajů chce uplatnit své právo, ale společnost nemá nastavenou metodiku pro výkon, tj. nedokáže např. shromáždit veškeré informace či není stanovený řešitel.	5	5	25
9	Právník	Riziko změny legislativy týkající se ochrany osobních údajů	EU nebo Úřad pro ochranu osobních údajů vydá aktualizaci podmínek zpracování osobních údajů.	4	1	4
10	Projektový manažer	Riziko špatné kontroly výstupů projektu	Vzniklá dokumentace neobsahuje nezbytné prvky.	5	4	20
11	Projektový manažer	Riziko špatného odhadu časové náročnosti úkolů	Dochází k časovým prodlevám, projekt nabírá zpoždění.	3	4	12
12	Projektový manažer	Riziko nedokončení úkolů	Pro daný úkol není stanovená odpovědná osoba.	4	2	8

Zdroj: Vlastní zpracování

Risk appetite společnosti

Na základě identifikace a kvantitativního vyjádření OHR dochází ke stanovení Risk appetitu společnosti na jednotlivá rizika. Pro jeho stanovení je využit bublinkový graf, kde jsou rizika graficky znázorněna. Osa x představuje blížící se výskyt rizik neboli jejich proximitu. Čím blíže je určité riziko ve formě bubliny u hladiny, tím dříve by mělo být riziko řešeno.

Graf 2 - Bublinkový graf



Zdroj: Vlastní zpracování

Obranné strategie řízení rizik

Společnost se rozhodla v rámci řízení rizik v projektu využít pouze 3 obranné strategie, kdy není zahrnuta obranná strategie „Vyhnutí se“, kdy je nutné provedení změny stylu práce či projektových aktivit, protože charakter identifikovaných rizik tuto obranou strategii neumožňuje.

Použité strategie

- *Přijetí rizika:* riziko má nízké OHR a vynaložené úsilí na jeho eliminaci by převyšovalo hodnotu ztráty
    - rizika s ID 2 a 9 = společnost nebude vynakládat kroky vedoucí k jeho eliminaci z důvodu velmi nízké pravděpodobnosti jejich výskytu.

- *Omezení rizika:* U rizik bude redukován jejich pravděpodobnost výskytu prostřednictvím preventivních opatření, které jsou blíže specifikované v Registru rizik, který je uveden v příloze č. 1 této práce.
    - Riziko č. 10, které se již nachází mezi riziky s kritickou významností bude též zařazeno do strategie Omezení rizika, protože není možné se této činnosti vyhnout. Jako prevence bude zejména použit checklist, který podléhá kontrole a schválení vedením společnosti.
- *Přenesení rizika:* Zodpovědnost za riziko je přenesena na jiný subjekt.
    - Riziko č. 8 – bude prozatímně přeneseno na Právníka, neboť ve společnosti zatím není nastaven přesný postup řízení výkonu práv subjektů údajů a mohlo by tak dojít k hrubému porušení nařízení GDPR ještě před dokončením projektu.

Tabulka 11 - Rozdělení rizik dle přidělených strategií

Významnost rizika	Strategie	Rizika	Poznámka
Malá	Přijetí	2,9	
Střední	Omezení	1,6,7,12	
Vysoká	Omezení	4,11	
Velmi vysoká	Omezení	3,5	
Kritická	Omezení, Přenesení	8, 10	

Zdroj: Vlastní zpracování

5.2.1.5 Business case

V předprojektové fázi byl vytvořen Outline business casu, který bude použit pro vytvoření první úplné verze Business case.

Business case	
Název projektu:	Implementace GDPR nařízení
Odpovědná osoba:	Martin Valeš
Sponzor projektu:	Ředitel společnosti
Verze:	1.0
Cíl projektu	Cílem projektu je analýza současného stavu manipulace s osobními údaji, zjištění slabých či kritických míst, která nejsou v souladu s nařízením a zajistit vytvoření základní dokumentace pro nabytí souladu, tj. například Směrnice o ochraně osobních údajů, informační memorandum, metodika vyřizování požadavků subjektů údajů.
Důvody pro projekt	- zákonná povinnost dosažení souladu organizace s nařízením GDPR - snížení rizika poškození dobrého jména společnosti a renomé - odstranění rizika spojeného s udělením pokuty společnosti za nedodržování souladu - mít data pod kontrolou (systematická evidence)
Možnosti projektu	1) nedělat nic 2) vynaložit úsilí pro dosažení souladu s GDPR nařízením
Očekávané přínosy	- vytvoření registru činností s detailním popisem o zpracování osobních údajů - vytvoření jednotné metodiky pro řešení žádostí subjektů a systému zpracování osobních údajů - posílení dobrého jména společnosti
Očekávané nevýhody	- alokace zaměstnanců na projekt a omezení jejich kapacit pro standardní úkony
Časová náročnost	- 32 dní (22.10.2018 – 4.12.2018)

Náklady	246 220 Kč (z toho 110 400 Kč rozpočet na právní služby)
Zhodnocení investice	odvrácení hrozící pokuty v závislosti na míře závažnosti poručení nařízení až do výše: - 10 000 000 EUR (nebo až do 2% celosvětového ročního obratu podniku) - 20 000 000 EUR (nebo až do 4% celosvětového ročního obratu podniku)
Hlavní rizika	- riziko nepřipravenosti zpracovatelů na GDPR - riziko neposkytnutí součinnosti při implementaci GDPR - riziko úniku informací a know-how - riziko výpadku zdrojů - riziko úniku dat o subjektech údajů - riziko zvýšení finanční náročnosti projektu - riziko záměrného zvolení jiného právního titulu - riziko neschopnosti vyhovění právu subjektu údajů - riziko změny legislativy týkající se ochrany osobních údajů - riziko špatné kontroly výstupů projektu - riziko špatného odhadu časové náročnosti úkolů - riziko nedokončení úkolů
Popis produktů projektu	- vytvoření Směrnice o ochraně osobních údajů - vytvoření Informačního memoranda na internetové stránky společnosti - vytvoření Metodiky řízení výkonu práv subjektů - vytvoření Registru záznamů o činnostech zpracování OÚ - vzor dodatku ke smlouvě o zpracování OÚ se zpracovateli - vytvoření vnitřního předpisu IT bezpečnosti
Projektový přístup	- v projektu bude zapojena externí advokátní kancelář, která bude revidovat soulad podniknutých kroků s nařízením

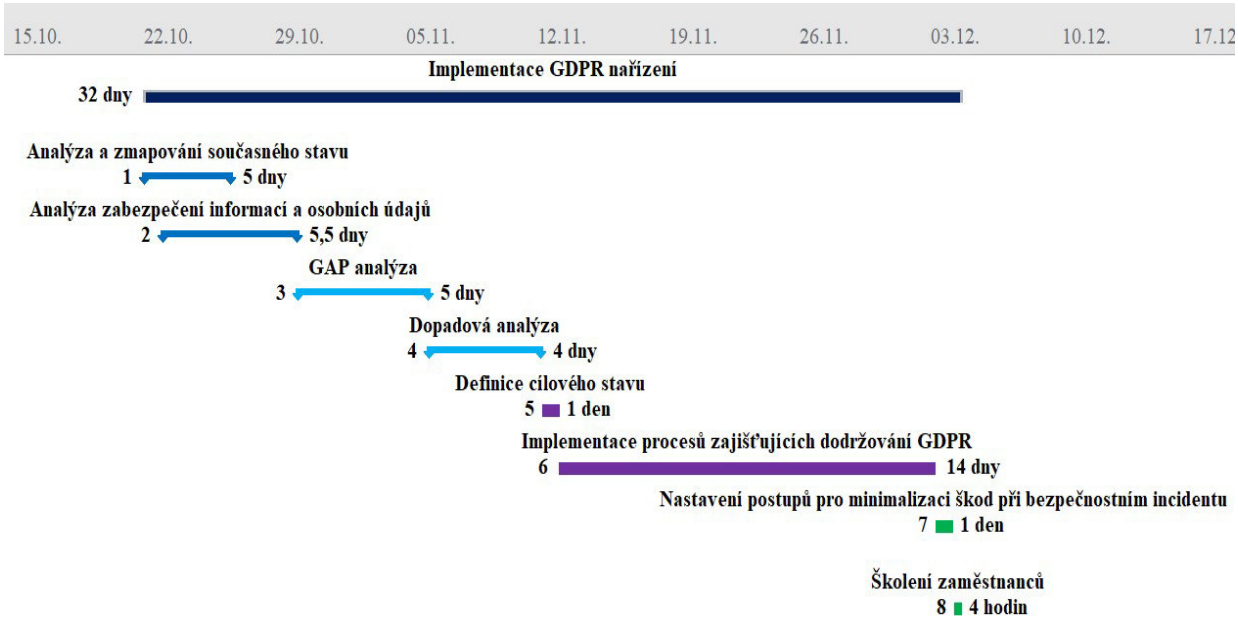
	- dále budou kvůli malému počtu zaměstnanců spojeny určité projektové role, avšak v povoleném rozsahu, který umožňuje PRINCE2, aby nedocházelo ke střetu zájmů		
Zvolená možnost rozsahu projektu (1,2)	2	Schválil:	Ředitel společnosti (Sponzor projektu)
		Datum:	15.10.2018

Zdroj: Vlastní zpracování

5.2.1.6 Projektový plán

V rámci plánování projektu byl vytvořen Ganttův diagram směrného plánu projektu, kde jsou zobrazeny projektové úkoly s délkami trvání. Z důvodu vyšší přehlednosti grafu jsou zobrazeny pouze hlavní úkoly, které však v sobě zahrnují dílčí úkoly, které jsou blíže specifikované na obrázku č. 9 – Soupis projektových úkolů.

Obrázek 7 - Směrný plán projektu



Zdroj: Vlastní zpracování

Náklady na projektové úkoly vycházejí z hodinových sazeb lidských zdrojů, které jsou blíže popsány v obrázku č. 8 (viz níže).

Obrázek 8 - Náklady na lidské zdroje

Název zdroje	Náklady	Práce	Standardní sazba
Projektový manažer	25 760,00 Kč	92 hodin	280,00 Kč/hod.
Právník	110 400,00 Kč	92 hodin	1 200,00 Kč/hod.
Asistentka	12 800,00 Kč	80 hodin	160,00 Kč/hod.
IT specialist	30 600,00 Kč	68 hodin	450,00 Kč/hod.
Finanční manažerka	18 900,00 Kč	67,5 hodin	280,00 Kč/hod.
Produktový manažer	14 560,00 Kč	52 hodin	280,00 Kč/hod.
Ředitel společnosti	14 000,00 Kč	28 hodin	500,00 Kč/hod.
Business analyst	12 600,00 Kč	84 hodin	150,00 Kč/hod.
Fakturantka	6 600,00 Kč	40 hodin	165,00 Kč/hod.

Zdroj: Vlastní zpracování

Směrný plán projektu počítá s délkou trvání celého projektu v rozsahu 32 dnů a 8 hlavních projektových úkolů. Celková doba trvání projektu je delší kvůli malému počtu pracovníků, kdy muselo dojít k vyrovnání zdrojů, aby nedocházelo k jejich přetížení.

Například lidský zdroj „Právník“ se podílí na činnostech 6.3, 6.4, 6.5. a poté na činnosti 7, kdy muselo dojít k posunutí začátků činností.

Obrázek 9 - Soupis projektových úkolů

Kód WBS	Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci	Názvy zdrojů	Náklady
	Implementace GDPR nařízení	**32 dny**	**22.10.2018**	**04.12.2018**			**246 220,00 Kč**
1	**Analýza a zmapování současného stavu**	**5 dny**	**22.10.2018**	**26.10.2018**			**13 140,00 Kč**
1.1	Identifikace míst, kde dochází ke zpracování OÚ	2 dny	22.10.2018	23.10.2018		Asistentka	2 560,00 Kč
1.2	Revize vydaných přístupů a oprávnění v rámci intranetu	1 den	22.10.2018	22.10.2018		IT specialist	3 600,00 Kč
1.3	Identifikaci nástrojů ke zpracování OÚ	1 den	24.10.2018	24.10.2018		Asistentka; Business analyst; Finanční manažerka	4 580,00 Kč
1.4	Zmapování základních činností, které se s daty provadí	2 dny	25.10.2018	26.10.2018		Business analyst	2 400,00 Kč
2	**Analýza zabezpečení informací a osobních údajů**	**5,5 dny**	**23.10.2018**	**30.10.2018**			**6 020,00 Kč**
2.1	Revize zabezpečení serveru a cloudových řešení	1 den	23.10.2018	23.10.2018	3	IT specialist	3 600,00 Kč
2.2	Revize zabezpečení fyzických dokumentů	0,5 dny	30.10.2018	30.10.2018	1	Asistentka;Fakturantka;Produktový manažer	2 420,00 Kč
3	**GAP analýza**	**5 dny**	**30.10.2018**	**06.11.2018**	**1;6**		**38 800,00 Kč**
3.1	Revize podnikové dokumentace	2 dny	30.10.2018	01.11.2018		Asistentka;Business analyst;Finanční manažerka;Projektový manažer	13 920,00 Kč
3.2	Revize smluv	2 dny	01.11.2018	05.11.2018	10	Právník	19 200,00 Kč
3.3	Revize stávajích Souhlasů se zpracováním OÚ	1 den	05.11.2018	06.11.2018	10;11	Produktový manažer	2 240,00 Kč
3.4	Předávání dat mimo EU	1 den	05.11.2018	06.11.2018	10;11	Business analyst	1 200,00 Kč
3.5	Soupis požadavků	1 den	05.11.2018	06.11.2018	10;11	Projektový manažer	2 240,00 Kč
4	**Dopadová analýza**	**4 dny**	**06.11.2018**	**12.11.2018**			**28 160,00 Kč**
4.1	Kontrola nutnosti provedení DPIA	1 den	06.11.2018	07.11.2018	9	Projektový manažer	2 240,00 Kč
4.2	Stanovení a posouzení rizik pro podnik	2 dny	07.11.2018	09.11.2018	16	Finanční manažerka; Produktový manažer; Projektový manažer; Ředitel společnosti	21 440,00 Kč
4.3	Stanovení rizik plynoucí pro subjekty údajů	1 den	09.11.2018	12.11.2018	16	Produktový manažer; Projektový manažer	4 480,00 Kč
5	**Definice cílového stavu**	**1 den**	**12.11.2018**	**13.11.2018**	**1;6;9;15**	Projektový manažer	**2 240,00 Kč**
6	**Implementace procesů zajišťujících dodržování GDPR**	**14 dny**	**14.11.2018**	**04.12.2018**	**19**		**125 920,00 Kč**
6.1	Vytvoření registru záznamů o činnostech zpracování OÚ	4 dny	14.11.2018	20.11.2018		Asistentka;Business analyst;Fakturantka;IT specialist	29 600,00 Kč
6.2	Revize registru záznamů o činnostech zpracování OÚ	2 dny	20.11.2018	22.11.2018	23	Finanční manažerka;Projektový manažer	8 960,00 Kč
6.3	Vytvoření metodického pokynu pro výkon práv subjektů údajů	4 dny	14.11.2018	20.11.2018		Právník	38 400,00 Kč
6.4	Vytvoření Směrnice pro ochranu osobních údajů	2 dny	20.11.2018	22.11.2018		Právník	19 200,00 Kč
6.5	Vytvoření vnitřního předpisu IT bezpečnosti	2 dny	30.11.2018	04.12.2018		Právník;IT specialist	26 400,00 Kč
6.6	Vytvoření a vyplnění registru evidovaných souhlasů a informačního memoranda	1,5 dny	14.11.2018	15.11.2018		Produktový manažer	3 360,00 Kč
7	**Nastavení postupů pro minimalizaci škod při bezpečnostním incidentu**	**1 den**	**04.12.2018**	**05.12.2018**	**22**	Právník; Finanční manažerka; Projektový manažer; Ředitel společnosti	**18 080,00 Kč**
8	**Školení zaměstnanců**	**4 hodin**	**05.12.2018**	**05.12.2018**	**29**	Všichni zaměstnanci	**13 860,00 Kč**

Zdroj: Vlastní zpracování

5.2.1.7 Popis produktu

Směrnice o ochraně osobních údajů

Účelem produktu Směrnice o ochraně osobních údajů je vytvoření vnitřního předpisu společnosti, kterým se jsou všichni zaměstnanci společnosti povinni řídit v souvislosti s veškerým zpracováním osobních údajů a její nedodržování je bráno jako hrubé porušení pracovních povinností. Směrnice má za účel definovat přesná práva a povinnosti zaměstnancům při zpracování osobních údajů subjektů údajů, tj. například v jaké formě, rozsahu a na základě jakého právního titulu mohou zpracovávat osobní údaje, dále definuje typy osobních údajů a k nim příslušné požadavky na zajištění bezpečnosti.

Obsah dokumentu:

- definice základních pojmů;
- vymezení účelu a působnosti směrnice;
- práva a povinnosti při zpracování osobních údajů;
- požadavky na zabezpečení osobních údajů;
- odpovědná osoba za korektní zpracování osobních údajů;
- definice formy a rozsahu povinného školení zaměstnanců;
- zásady správného počínání s daty;
- datum počátku účinnosti směrnice.

Formát dokumentu:

- elektronický dokument vytvořený v MS Word s možnou pozdější editací.

Požadované dovednosti na vývoj:

- právní znalost v oblasti ochrany osobních údajů, tj. znalost zákona č. 101/2000 Sb., o ochraně osobních údajů a Obecného nařízení GDPR;
- praktická zkušenost s implementací GDPR nařízení.

Odpovědnost za kvalitu

- JUDr. Karel Novák (autor);
- Projektový manažer (kontrola – checklist).

Metodický pokyn pro výkon práv subjektů údajů

Účelem Metodického pokynu pro výkon práv subjektů údajů je zejména definování procesu, který bude aplikován v případě obdržení žádosti na uplatnění práva subjektů údajů. V dokumentu budou uvedeny a vysvětleny práva subjektů údajů včetně požadavků, které musí být splněny, aby mohlo dojít k uplatnění práva.

Obsah dokumentu

- definice základních pojmů;
- účel a působnost metodiky;
- detailní vysvětlení jednotlivých práv subjektů údajů;
- definice požadavků nezbytných pro jejich uplatnění;
- stanovení přesného procesu zpracování požadavku subjektu údajů;
- uvedení požadavků na vyřízení žádosti ze strany správce;
    - maximální lhůta pro vyřízení
    - kdy může dojít k neuplatnění práva
    - forma odpovědi
    - kdy může dojít k zpoplatnění vyřízení žádosti
- stanovení komunikačních kanálů;
- způsob identifikace a verifikace subjektu údajů;
- stanovení odpovědností;
- způsob evidence žádostí;
- vzor žádosti a odpovědi na žádost;
- proces ohlašování případů porušení zabezpečení;

Formát dokumentu

- elektronický dokument vytvořený v MS Word s možnou pozdější editací;
- užití grafických prostředků pro vizualizaci procesů (předdefinované nástroje MS Word, případně užití sofistikovaného nástroje např. MS Visio)

Požadované dovednosti na vývoj:

- právní znalost v oblasti ochrany osobních údajů, tj. znalost zákona č. 101/2000 Sb., o ochraně osobních údajů a Obecného nařízení GDPR;

- praktická zkušenost s implementací GDPR nařízení.

Odpovědnost za kvalitu

- JUDr. Karel Novák (autor)
- Projektový manažer (kontrola – checklist)

Registr záznamů o činnostech zpracování osobních údajů

Účelem dokumentu Registru záznamů o činnostech zpracování osobních údajů je vytvoření jednotné strukturované evidence činností, při kterých dochází ke zpracování osobních údajů. Registr bude zejména využit v případě nutnosti poskytnutí součinnosti dozorovému úřadu při prokazování dodržování souladu s obecným nařízením GDPR.

Každá činnost v registru obsahuje detailní informace o rozsahu a opodstatnění zpracování (viz „Obsah dokumentu“ níže).

Obsah dokumentu

- identifikátor činnosti;
- popis činnosti;
- účel zpracování;
- právní titul;
- nástroje pro zpracování;
- forma zabezpečení;
- informace o případném dalším zpracovateli osobních údajů;
- forma přenosu dat;
- informace o přenosu dat mimo EU;
- typy zpracovávaných osobních údajů;

Formát dokumentu

- elektronický dokument vytvořený v MS Excel s možnou pozdější editací.

Požadované dovednosti na vývoj

- detailní znalost interních procesů
- základní povědomí o požadavcích GDPR na Registru záznamů

Odpovědnost za kvalitu

- Autor: Asistentka, Business analytik, Fakturantka, IT specialista
- Kontrola: Právník – JUDr. Karel Novák (písemné potvrzení správnosti)

Informační memorandum

Účelem dokumentu je naplnění informační povinnosti vůči subjektům údajům, kde jsou uvedeny jejich práva a možnosti jejich uplatnění vůči správci osobních údajů včetně uvedení komunikačních kanálů a lhůt pro vyřízení. Vytvořený dokument bude vyvěšen na webových stránkách společnosti.

Obsah dokumentu

- účel dokumentu;
- popis účelu zpracování osobních údajů;
- uvedení příslušných právních titulů;
- informace o rozsahu zpracovávaných údajů;
- informace o předávání údajů třetím stranám;
- definice práv subjektů údajů plynoucích z Obecného nařízení;
- komunikační kanály;
- lhůty pro vyřízení.

Formát dokumentu

- elektronický dokument vytvořený v MS Word s možnou pozdější editací.

Požadované dovednosti na vývoj:

- právní znalost v oblasti ochrany osobních údajů, tj. znalost zákona č. 101/2000 Sb., o ochraně osobních údajů a Obecného evropského nařízení GDPR;
- praktická zkušenost s implementací GDPR.

Odpovědnost za kvalitu

- JUDr. Karel Novák (autor)
- Projektový manažer (kontrola – checklist)

Vzor dodatku ke smlouvě o zpracování osobních údajů

Účelem Dodatku ke smlouvě o zpracování osobních údajů je vytvoření základní šablony, která bude v současnosti i v budoucnu uzavírána mezi společností jako správcem a třetími stranami, které jsou v rolích zpracovatelů. Hlavním posláním dokumentu je uplatnění povinnosti správce zaručit soulad jím vybraných zpracovatelů osobních údajů s nařízením GDPR.

Obsah dokumentu

- definice základních pojmů;
- vymezení stran správce a zpracovatele osobních údajů;
- vymezení povinností obou stran;
- stanovení schvalovacího procesu pro možné větvení zpracovatelů;

Formát dokumentu

- elektronický dokument vytvořený v MS Word s možnou pozdější editací.

Požadované dovednosti na vývoj:

- právní znalost v oblasti ochrany osobních údajů, tj. znalost zákona č. 101/2000 Sb., o ochraně osobních údajů a Obecného evropského nařízení GDPR;
- praktická zkušenost s tvorbou smluv

Odpovědnost za kvalitu

- JUDr. Karel Novák (autor)
- Projektový manažer (kontrola – checklist)

Vnitřní předpis IT bezpečnosti

Účelem vnitřního předpisu IT bezpečnosti je stanovení pravidel pro používání ICT zaměstnanci z hlediska bezpečnosti.

Obsah dokumentu

- definice základních pojmů;
- vymezení struktury IT prvků společnosti;
- vymezení odpovědností (zajištění dodržování předpisu, správa IT);
- vymezení preventivních opatření (např. pro případ výpadku elektrického proudu).

Formát dokumentu

- elektronický dokument vytvořený v MS Word s možnou pozdější editací.

Požadované dovednosti na vývoj:

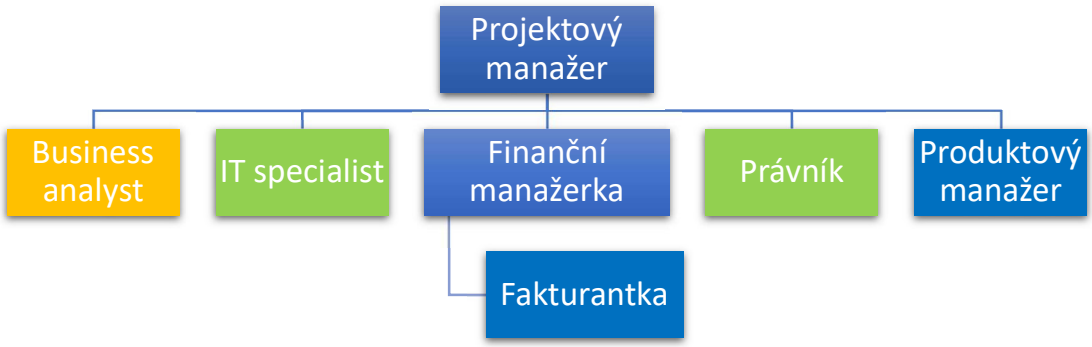
- znalost IT struktury společnosti.

Odpovědnost za kvalitu

- Správce IT (autor)
- Ředitel společnosti (kontrola – checklist)

5.2.1.8 Stanovení rolí projektového týmu

Obrázek 10 - Složení týmu



Zdroj: Vlastní zpracování

5.2.2 Plán přezkoumání přínosů (Benefits Review Plan)

Plán přezkoumání přínosů bude použit k určení, jakým způsobem a kdy může dojít k provedení měření dosažení očekávaných přínosů.

Plán zahrnuje aktivity, které jsou potřebné pro konkrétní ověření očekávaných benefitů a může dojít k jeho aktualizaci během projektu.

Tabulka 12 - Plán přezkoumání přínosů

ID	Popis benefitu	Vlastník	Měření		Zdroje potřebné k ověření
			Jak	Kdy	
1	Ucelený registr s detaily o zpracování osobních údajů, který bude sloužit jako nástroj pro dokazování souladu společnosti s nařízením GDPR	Jednatel	Vizuální kontrola	Ihned po dokončení tvorby registru	Registr záznamů o činnostech zpracování OÚ Checklist kvality registru
2	Nastaven jednotný proces pro výkon práv subjektů údajů	Jednatel	Vizuální kontrola	Ihned po dokončení	Metodika splňuje body checklistu a je zařazena mezi vnitřní předpisy společnosti
3	Posílení dobrého jména společnosti	Jednatel	Evidence bezpečnostních incidentů a požadavků SÚ (nulová tolerance bezpečnostních incidentů, kterým nešlo předejít prevencí)	1x ročně	Záznamy o vzniklých bezpečnostních incidentech a požadavků subjektů údajů

Zdroj: Vlastní zpracování

5.3 Řízení projektu

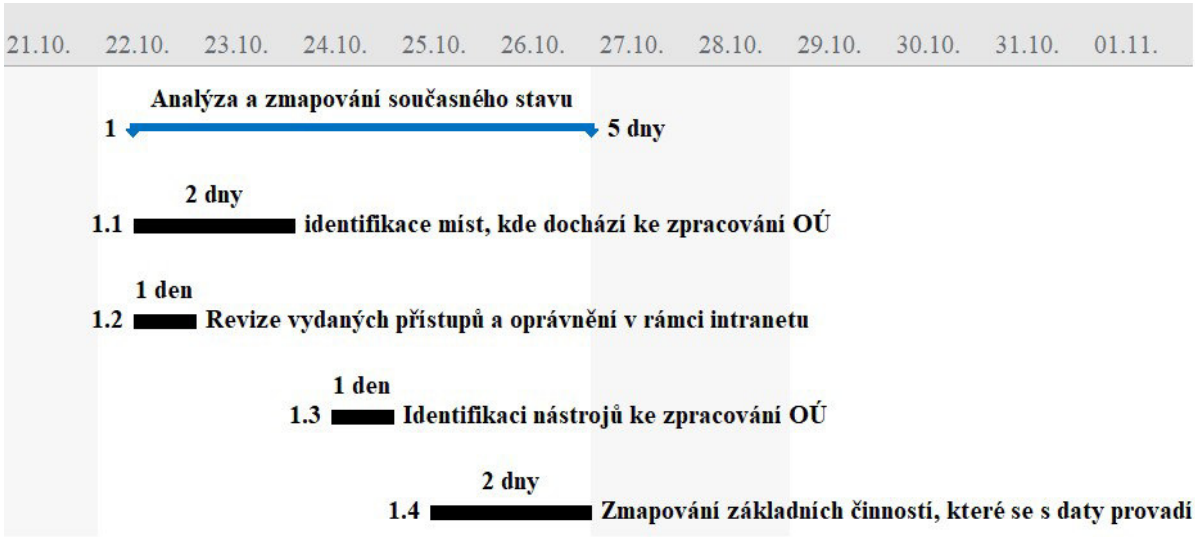
Za účelem řízení a kontroly průběhu projektu byl projekt rozdělen do milníků, které reprezentují ve WBS hlavní projektové činnosti, tj.

1. Analýza a zmapování současného stavu;
2. Analýza zabezpečení informací a osobních údajů;
3. GAP analýza;
4. Dopadová analýza;
5. Definice cílového stavu;
6. Implementace procesů zajišťujících dodržování GDPR;
7. Nastavení postupů pro minimalizaci škod při bezpečnostním incidentu.

5.3.1 Analýza a zmapování současného stavu

První milník projektu se při dekompozici hlavní projektové činnosti skládá ze 4 konkrétních dílčích úkolů (viz níže obrázek č. 10).

Obrázek 11 - Ganttův diagram prvního milníku



Zdroj: Vlastní zpracování

Analýza a zmapování současného stavu společnosti v rámci zpracování osobních údajů je nezbytným vstupem pro vytvoření GAP analýzy, kde jsou zjištěny nedostatky současného stavu proti ideálnímu stavu, kdy je společnost tzv. GDPR Compliance.

1.1 Identifikace míst, kde dochází ke zpracování OÚ

První aktivita spočívá ve stanovení konkrétních míst, kde jsou data fyzicky nebo elektronicky uložena. Na tuto aktivitu byla alokována asistentka ředitele společnosti, protože je ve společnosti od počátku a měla by mít největší přehled o aktivitách a místech, kde dochází ke zpracování osobních údajů. Zároveň nedochází k velkému zatížení rozpočtu projektu, protože má nižší MD sazbu než manažeři společnosti.

Tabulka 13 - Úložiště dat

Typ úložiště	Popis	Uložená data
Fyzické	Kniha návštěv	Informace o návštěvách: jméno, příjmení, kontaktní údaje (telefon, email) a datum návštěvy
Fyzické	Trezor	Smlouvy s klienty, zaměstnanci a třetími stranami
Fyzické	Uzamykatelná skříň	Šanony s údaji o zaměstnancích (účetní údaje, komunikace se zaměstnanci, klienty a třetími stranami)
Elektronické	Server společnosti	Veškeré držené dokumenty jsou také uchovávány na serveru společnosti (skeny smluv, uložená komunikace, fotografie…)
Elektronické	Bitrix24	Údaje o zaměstnancích (jméno, příjmení, pozice, kontaktní údaje, docházkový systém, fotografie)
Elektronické	Osobní PC zaměstnanců	emailová komunikace, koncepty smluv

Zdroj: Vlastní zpracování

1.2 Revize vydaných přístupů a oprávnění v rámci intranetu

Revizí vydaných přístupů a oprávnění v rámci intranetu mělo být zjištěno, do jakých oblastí, a tedy složek intranetu mají určití zaměstnanci přístup. Výstupem této revize je níže uvedená tabulka č. 14, kde jsou uvedeni jednotliví zaměstnanci a informace o tom, zda mají neomezený přístup do dané oblasti intranetu, není tím však myšleno, že nemají žádný přístup, ale tak, že jejich přístup je omezen pouze do takových adresářů, které jsou nezbytné pro výkon jejich funkce.

Tabulka 14 - Přístupy v rámci intranetu

Zaměstnanec	Typ zaměstnance	FIN	PM	Údaje o zaměstnancích	Informace o klientech
Ředitel	Interní	ANO	ANO	ANO	ANO
Asistentka	Interní	NE	ANO	NE	ANO
Projektový manažer	Interní	NE	ANO	NE	NE
Produktový manažer	Interní	NE	NE	NE	ANO
Finanční manažerka	Interní	ANO	NE	ANO	ANO
Business analytik	Interní	NE	ANO	NE	ANO
Fakturantka	Interní	ANO	NE	ANO	ANO
IT specialista	Externí	ANO	ANO	ANO	ANO
Vývojář	Externí	NE	NE	NE	NE
PPC/SEO specialista	Externí	NE	NE	NE	NE
Marketingový specialista	Externí	NE	NE	NE	NE
Účetní	Externí	ANO	NE	ANO	NE

Zdroj: Vlastní zpracování

Ukončení této činnosti proběhlo dříve, než bylo plánováno. Původní očekávaná náročnost byla 1 MD, ale bylo na ní vyčerpáno jen 0,5 MD.

1.3 Identifikace nástrojů ke zpracování OÚ

Po identifikování míst, kde dochází ke zpracování osobních údajů došlo k úplné identifikaci nástrojů, které se podílejí na zpracování. V rámci této identifikace se musely také zjistit, jak manuální, tak elektronické nástroje, neboť za zpracování osobních údajů je považována jakákoli manipulace s daty fyzických osob. Například kopírování či skenování pracovních smluv je bráno z pohledu GDPR také jako zpracování osobních údajů.

Na této činnosti se podílela asistentka, business analytik a finanční manažerka, kteří museli projít své pravidelné pracovní úkony a vyjmenovat nástroje, které používají a dochází při nich ke zpracování osobních údajů fyzických osob.

Zároveň asistentka a business analytik museli oslovit ostatní kolegy o poskytnutí těchto informací a vytvořit ucelený soubor nástrojů.

Seznam nástrojů:

- MS Office;
- Adobe Acrobat;
- Google kalendář;
- Bitrix24;
- Backend internetového bankovnictví;
- Účetní systém;
- Tiskárna.

1.4 Zmapování základních činností, které se s daty provádí

Zmapováním základních činností, kdy dochází ke zpracování osobních údajů vznikne základní katalog činností, který bude vstupem pro vytvoření jednoho z hlavních projektových produktů Registru záznamů o činnostech zpracování osobních údajů, proto je této činnosti věnována vysoká priorita.

Pro snížení nákladů na vytvoření katalogu byl tímto úkolem pověřen business analytik, který je ve společnosti na zkrácený úvazek a má i nižší MD sazbu. Plánovaná časová náročnost aktivity je 2 MD.

Kompletní katalog činností bude jako součást Registru záznamů o činnostech zpracování osobních údajů uveden v příloze č. 2.

Závěr prvního milníku

Pro ověření dokončení prvního milníku projektu implementace GDPR nařízení byl vytvořen checklist s otázkami. Projekt nenabírá zpoždění a byl ušetřen 0,5MD na činnosti 1.2.

Tabulka 15 - Checklist prvního milníku

Checklist	ANO / NE	Komentář
Jsou identifikována místa, kde dochází ke zpracování OÚ?	ANO	
Jsou revidovány přístupy a oprávnění na intranet?	ANO	
Jsou identifikovány nástroje ke zpracování OÚ?	ANO	
Je vytvořen úplný katalog činností, kde dochází ke zpracování OÚ?	ANO	

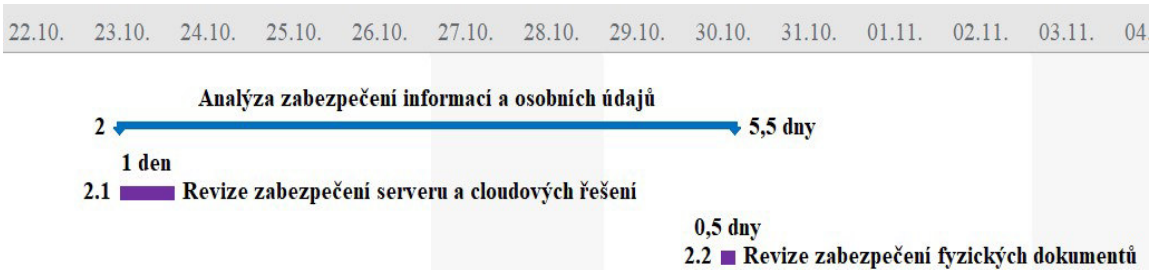
Nastala odchylka od plánu?	ANO	Činnost 1.2 byla dokončena v předstihu o 0,5MD

Zdroj: Vlastní zpracování

5.3.2 Analýza zabezpečení informací a osobních údajů

Úkolem správce IT bylo revidovat zabezpečení informací a osobních údajů v rámci nástrojů, které jsou buď poskytované prostřednictvím třetích stran a společnost je přímo nespravuje, tj. cloudová řešení nebo je k nim připojováno prostřednictvím internetu, tj. server společnosti, který může představovat potenciální riziko bezpečnostního incidentu.

Obrázek 12 - Ganttův diagram druhého milníku



Zdroj: Vlastní zpracování

2.1 Revize zabezpečení serveru a cloudových řešení

Zabezpečení serveru a cloudových řešení bylo vyhodnoceno zejména na základě parametru, kdy byl posuzován typ dat, které se v daném úložišti nachází, respektive, zda se zde vyskytují citlivé osobní údaje, které vyžadují přísnější opatření.

Cloudové řešení

Ve společnosti jsou používány 3 cloudové řešení:

1. Bitrix24
2. Backend internetového bankovnictví
3. Google kalendář

V cloudových řešeních Bitrix24 a Google kalendáři nedochází ke zpracování citlivých osobních údajů. Poskytovatel systému Bitrix24 zároveň deklaruje svým zákazníkům vysokou formu zabezpečení a připravenost na GDPR.

Cloudové řešení Google kalendář nepředstavuje žádnou hrozbu při porušení zabezpečení, neboť se zde maximálně vyskytují jména a příjmení subjektů údajů ve vytvořených záznamech. Nicméně i kdyby došlo k porušení zabezpečení, tak by nebylo možné přímo identifikovat konkrétní osobu.

Jediné možné riziko z hlediska zabezpečení představuje backendové řešení internetového bankovnictví, protože se zde vyskytují citlivé osobní údaje. Avšak i v tomto případě je poskytovatel smluvně zavázán k zajištění vysoké úrovně zabezpečení, kterou je povinen pravidelně testovat. Zároveň je smluvně zavázán odpovědností za každé vzniklé porušení zabezpečení a dodržování vnitřního souladu s GDPR nařízením.

Server společnosti

Server je adekvátně zabezpečen proti porušení zabezpečení dat a to například:

- fyzicky zabezpečen v uzamčené místnosti;
- omezení přístupů a práv jednotlivým uživatelům;
- zaznamenávání veškerých aktivit;
- šifrovaná data;
- funkční firewall a router;
- blokování datových toků mezi serverem a interní sítí.

Shrnutí zabezpečení

Cloudová řešení a server společnosti jsou dostatečně zabezpečena.

2.2 Revize zabezpečení fyzických dokumentů

Revize zabezpečení fyzických dokumentů se zejména týká archivovaných smluv, účetních dokumentů a údajů o zaměstnancích. Tímto úkolem byla pověřena asistentka, fakturantka a produktový manažer, protože mají přístup k potřebným oblastem.

Z revize vyplynulo, že veškeré citlivé dokumenty jsou uzamčeny v trezoru nebo uzamykatelných skříních a nebyl nalezen žádný výskyt nechráněných dokumentů, které by ohrožovaly bezpečnost dat subjektů údajů.

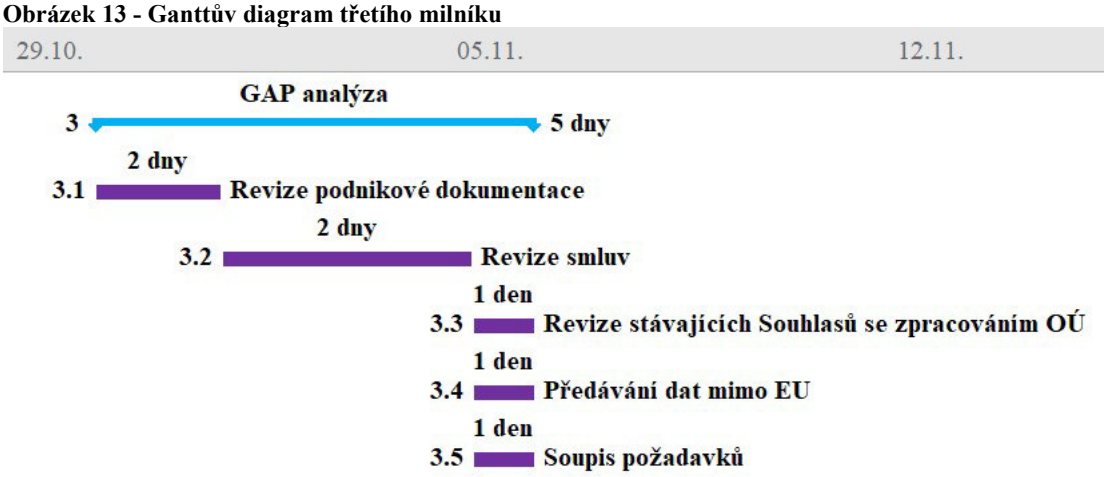
Shrnutí druhého milníku

Vše proběhlo podle plánu, nedošlo k odchylkám.

5.3.3 GAP analýza

GAP analýza neboli analýza rozdílů mezi požadovaným stavem a současným stavem připravenosti společnosti na GDPR nařízení. Aby bylo možné provést tuto analýzu smysluplně a objektivně, tak bylo nezbytné provést revizi aktuální podnikové dokumentace, smluv, Souhlasů se zpracováním OÚ, kdy bylo zejména nutné posoudit, zda souhlasy byly uděleny vědomě a nebyly například součástí smlouvy, protože takové souhlasy jsou z hlediska GDPR nařízení považovány za neplatné. Dále bylo potřeba zjistit, zda dochází k předávání osobních údajů mimo EU, neboť tam již GDPR není účinné a v poslední řadě na základě všech dřívějších poznatků vytvořit soupis požadavků neboli sepsat oblasti, kde se nacházejí odchylky od požadovaného stavu.

Obrázek 13 - Ganttův diagram třetího milníku



Zdroj: Vlastní zpracování

3.1 Revize podnikové dokumentace

Revizí podnikové dokumentace je myšlen průzkum všech vnitřních nařízení společnosti, kdy je nutné revidovat dokumentace všech podnikových oblastí a posoudit je ve vztahu ke zpracování a ochraně osobních údajů.

Revizí byl pověřen projektový manažer, finanční manažerka, business analytik a asistentka, při čemž bylo zjištěno, že společnost disponuje omezeným množstvím vnitřních nařízení, které bude potřeba vytvořit v blízké budoucnosti po skončení projektu implementace GDPR nařízení.

3.2 Revize smluv

Revizi smluv prováděl právník, který byl nejkompetentnější osobou pro tento účel a revize smluv trvala 2 MD.

3.3 Revize stávajících Souhlasů se zpracováním OÚ

Na tuto činnost byl alokován produktový manažer, protože zaštiťuje veškerou komunikaci směrem ke klientům, dále oblast marketingu a produktového managementu. Cílem revize bylo zjistit, jakým způsobem dochází ke sběru souhlasů se zpracováním osobních údajů, dále jakou mají formu a zda existuje ucelený přehled držených souhlasů.

Výstup:

- Forma: písemná (ucelený přehled zatím neexistuje)
- Zdroj: webový formulář, souhlas ve smlouvě (nyní již neplatný)

3.4 Předávání dat mimo EU

Business analytik provedl revizi veškerých smluv se zpracovateli a zároveň ověřil místo podnikání jednotlivých zpracovatelů, zda se nenacházejí mimo EU. Výsledkem bylo, že nedochází k přenosu dat mimo EU.

Samotná GAP analýza

Na základě dosud provedených aktivit byla provedena GAP analýza pomocí dotazníku s odpověďmi typu ano/ne, kdy úplného souladu je dosaženo zodpovězením všech otázek formou ano. Výstup GAP analýzy je zobrazen níže na obrázku č. 14.

3.5 Soupis požadavků

Po zodpovězení otázek ve formuláři GAP analýzy jsme získali přehled oblastí, které nejsou v souladu s nařízením GDPR, a tedy i soupis požadavků, které je potřeba splnit:

- Vytvořit Směrnici o ochraně osobních údajů;
- Vytvořit Registr záznamů o činnostech zpracování osobních údajů;
- Vytvořit Metodický pokyn pro výkon práv subjektů údajů;
- Vytvořit informační memorandum a vnitřní předpis IT bezpečnosti;
- Provést školení zaměstnanců.

Závěr třetího milníku: V rámci třetího milníku nedošlo ke změnám oproti projektovému plánu.

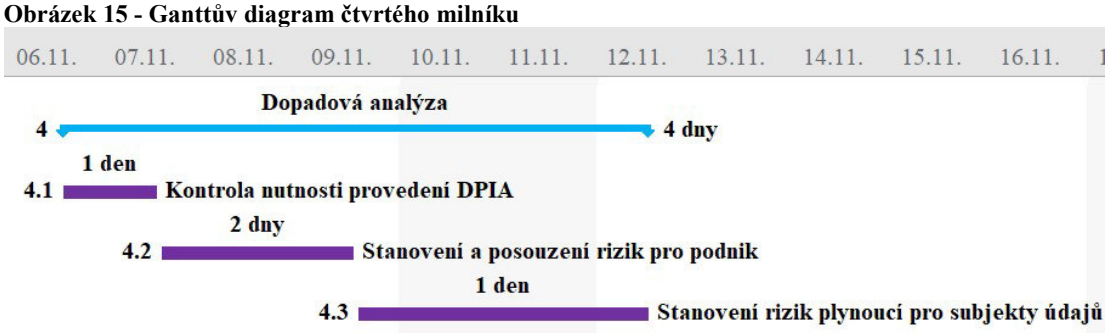
Obrázek 14 - GAP analýza

GAP analýza	ANO / NE	Komentář
Spravedlivé získání souhlasu se zpracováním osobních údajů:		
V době, kdy shromažďujeme informace o údajů, jsou informovány o způsobu použití těchto informací?	NE	Bude řešeno informačním memorandem
Jsou subjekty údajů informovány o zveřejňování nebo předávání jejich údajů třetím stranám ke zpracování?	NE	
Získali jsme souhlas subjektů údajů s jakýmkoli druhotným použitím jejich osobních údajů, protože jim to nemusí být zřejmé?	ANO	
Můžeme popsat naše postupy shromažďování údajů jako zákonné, korektní, spravedlivé a transparentní?	ANO	
Specifikace účelu:		
Je účel nebo účely, pro který uchováváme osobní informace dostatečně jasný a zřejmý?	ANO	
Jsou osoby, které již máme v naší databázi, také jasně srozuměny s tímto účelem?	NE	V případě souhlasu ne
Byla přidělena odpovědnost některému zaměstnanci za udržování přehledu všech souborů dat a účelů, který je s nimi spojen?	ANO	
Používání a zveřejňování informací:		
Existují definovaná pravidla týkající se používání a zveřejňování informací?	NE	Bude řešeno směrnicí o ochraně osobních údajů
Znají všichni zaměstnanci tato pravidla?	NE	
Jsou si subjekty údajů vědomy použití a zveřejnění svých osobních údajů? Byly by překvapeny, kdyby se o nic dozvěděly?	ANO	
Bezpečnost:		
Existuje seznam bezpečnostních opatření pro každý soubor dat nebo databázi?	NE	Bude řešeno vnitřním předpisem IT bezpečnosti
Je někdo zodpovědný za implementaci a přezkum těchto ustanovení?	NE	
Jsou tato opatření dostatečně vhodná pro citlivost osobních údajů, které uchováváme?	NE	
Jsou naše počítače a naše databáze chráněny hesly a šifrovány, pokud je to vhodné?	ANO	
Jsou naše počítače, servery a soubory bezpečně uzamčeny před neoprávněnými osobami?	ANO	
Přiměřenost, relevantnost a nezbytný rozsah:		
Shromažďujeme pouze informace, které nezbytně potřebujeme, a získáváme je spravedlivým a komplexním způsobem?	ANO	
Zkontrolovali jsme, zda všechny informace, které shromažďujeme, jsou relevantní a pouze nezbytného rozsahu pro náš oprávněný účel?	ANO	
Pokud by nás někdo požádal, abychom mu poskytli všechny informace, které o něm uchováváme, mohli bychom tak učinit?	NE	Bude řešeno Registrem záznamů a metodickým pokynem pro výkon práv SÚ
Existují politiky, zásady a procesy uchovávání, odmazávání, přístupu a pozastavení zpracování dat?	NE	Bude řešeno směrnicí o ochraně osobních údajů
Přesnost a aktuálnost:		
Kontrolujeme námi uchovávané údaje z hlediska přesnosti?	ANO	Každý uživatel je povinnen aktualizovat údaje v internetovém bankovnictví.
Víme, kolik z našich osobních údajů je časově citlivých, tj. pravděpodobně časem nepřesných, pokud nebudou aktualizovány?	ANO	
Máme zajištěnou stálou aktualizaci našich databází?	ANO	
Doba uchovávání:		
Existují jasná pravidla o tom, jaké informace a jak dlouho mají být uchovány?	NE	Vycházíme ze zákoné lhůty, ale není stanovena lhůta pro oprávněný zájem a souhlas. Bude upřesněno v Registru záznamů.
Jsme si jasně vědomi všech právních požadavků na uchování údajů pro určitou dobu? Například zákon o archivnictví, účetnictví apod.	ANO	V zákonem stanovených lhůtách ano.
Pravidelně odmazáváme data z našich databází, která již nepotřebujeme, jako jsou údaje týkající se bývalých zákazníků nebo zaměstnanců?	NE	Bude určena odpovědná osoba.
Máme politiku a zásady pro mazání osobních údajů, jakmile je účel, pro který jsme údaje získali, dokončen?	NE	
Právo na přístup:		
Byla určena osoba odpovědná za zpracování žádostí o přístup?	NE	Bude řešeno Metodickým pokynem pro výkon práv SÚ.
Existují jasné postupy pro řešení těchto žádostí?	NE	
Zaručují tyto postupy dodržování požadavků nařízení?	NE	
Registrace:		
Máme jasno v tom, zda potřebujeme být zaregistrováni u ÚOOÚ?	ANO	Nepotřebujeme být zaregistrováni.
Školení a vzdělávání:		
Znáte úroveň povědomí o ochraně osobních údajů ve své organizaci?	NE	Bude řešeno školením zaměstnanců na konci projektu.
Jsou si zaměstnanci vědomi svých odpovědností v oblasti ochrany osobních údajů - včetně požadavku důvěrnosti?	NE	
Je součástí vzdělávacího programu pro naše zaměstnance i oblast ochrany osobních údajů?	NE	
Jsou si všichni zaměstnanci vědomi své role?	NE	

Zdroj: Vlastní zpracování

5.3.4 Dopadová analýza

Obrázek 15 - Ganttův diagram čtvrtého milníku



Zdroj: Vlastní zpracování

4.1 Kontrola nutnosti provedení DPIA

Úřad pro ochranu osobních údajů vydal dokument s deseti kritérii pro obecné určení rizikovosti zpracování, a tedy i nutnosti provedení DPIA neboli Posouzení vlivu na ochranu osobních údajů. Ke každému kritériu jsou přiřazeny 3 příklady typů zpracování, které se nacházejí na škále „Kritické hodnoty“, „Významné hodnoty“ a „Nízké hodnoty“. Správce se na základě oněch třech příkladů přiřadí k jedné hodnotě, které odpovídá jeho styl zpracování osobních údajů.

Systém vyhodnocení výsledků:

- pokud dvě a více odpovědí jsou v kritických hodnotách, tak musí správce zpracovat DPIA;
- pokud jedna odpověď je v kritických hodnotách a alespoň pět se jich nachází ve významných hodnotách, tak opět musí správce zpracovat DPIA.

Tabulka 16 - posouzení provedení DPIA

ID	Kritérium	Hodnota
1	Zpracování osobních údajů zahrnuje monitorování subjektů údajů	Významná
2	Zpracování údajů, které umožňují přímou identifikaci a/nebo těch, které mají vysoce osobní povahu pro subjekty údajů	Kritická
3	Zpracování údajů, jenž může subjekty údajů vystavit ohrožení z okolního prostředí	Nízká
4	Zpracování velkého rozsahu osobních údajů	Nízká
5	Zpracování, které zahrnuje monitorování veřejně přístupných prostor	Významná
6	Zpracování osobních údajů, které mohou subjekty údajů ovlivnit v omezeném rozsahu	Významná
7	Zpracování osobních údajů, které jsou veřejně přístupné	Nízká
8	Zpracování osobních údajů, využívající složité nebo pokročilé technické infrastruktury či platformy	Nízká
9	Zpracování osobních údajů jinými správci či zpracovateli	Významná
10	Zpracování osobních údajů prostřednictvím nových technologických či organizačních řešení	Nízká

Zdroj: Úřad pro ochranu osobních údajů

Na základě výše uvedených odpovědí není nutné provádět DPIA. Proto činnosti 4.2 a 4.3, které byly původně plánovány ve směrném plány nebudou uskutečněny.

Závěr čtvrtého milníku

Dvě činnosti nebyly realizovány, projekt je v předstihu o 3 dny a došlo k finanční úspoře ve výši 25 920 Kč.

5.3.5 Definice cílového stavu

Projektový manažer má za cíl v rámci definice cílového stavu zhodnotit, zda v projektu došlo ke změnám ve směrném plánu, respektive jestli byly definovány nové aktivity, s nimiž nebylo původně počítáno a je nutné je provést. V takovém případě by muselo dojít k aktualizaci plánu a postoupení nových aktivit k dalšímu schválení Project boardu, který by musel schválit navýšení rozpočtu a časové prodloužení projektu.

Na základě dříve vytvořených analýz není nutné zavést další aktivity, které by měnily projektový plán. Na druhou stranu díky snížení náročnosti činností a vyřazením posledních dvou činností 4.2 a 4.3 dochází k předstihu vývoje projektu v porovnání se směrným plánem.

5.3.6 Aktualizace dokumentace

Po dokončení analýz dochází aktualizaci celkové projektové dokumentace, tj.:

- business case;
- registrů (kvality, rizik a problémů);
- projektového plánu;
- lessons log, daily log.

Aktualizace business case

V průběhu projektu dochází k aktualizaci business casu, kdy je vytvořena nová verze 2.0, která bude předložena vedení k dalšímu schválení a zdůvodnění účelu projektu. Uvnitř dokumentu níže jsou žlutě vyznačeny změny oproti původní verzi 1.0.

Tabulka 17 - Aktualizovaný business case (2.0)

Business case	
Název projektu:	Implementace GDPR nařízení
Odpovědná osoba:	Martin Valeš
Sponzor projektu:	Ředitel společnosti
Verze:	2.0
Cíl projektu	Cílem projektu je analýza současného stavu manipulace s osobními údaji, zjištění slabých či kritických míst, která nejsou v souladu s nařízením a zajistit vytvoření základní dokumentace pro nabytí souladu, tj. například Směrnice o ochraně osobních údajů, informační memorandum, metodika vyřizování požadavků subjektů údajů.
Důvody pro projekt	- zákonná povinnost dosažení souladu organizace s nařízením GDPR - snížení rizika poškození dobrého jména společnosti a renomé

	- odstranění rizika spojeného s udělením pokuty společnosti za nedodržování souladu - mít data pod kontrolou (systematická evidence)
Možnosti projektu	1) nedělat nic 2) vynaložit úsilí pro dosažení souladu s GDPR nařízením
Očekávané přínosy	- vytvoření registru činností s detailním popisem o zpracování osobních údajů - vytvoření jednotné metodiky pro řešení žádostí subjektů a systému zpracování osobních údajů - posílení dobrého jména společnosti
Očekávané nevýhody	- alokace zaměstnanců na projekt a omezení jejich kapacit pro standardní úkony
Časová náročnost	- 22,5 dní (22.10.2018 – 21.11.2018)
Náklady	218 500 Kč (z toho 110 400 Kč rozpočet na právní služby)
Zhodnocení investice	odvrácení hrozící pokuty v závislosti na míře závažnosti poručení nařízení až do výše: - 10 000 000 EUR (nebo až do 2% celosvětového ročního obratu podniku) - 20 000 000 EUR (nebo až do 4% celosvětového ročního obratu podniku)
Hlavní rizika	- riziko nepřipravenosti zpracovatelů na GDPR - riziko neposkytnutí součinnosti při implementaci GDPR - riziko úniku informací a know-how - riziko výpadku zdrojů - riziko úniku dat o subjektech údajů - riziko zvýšení finanční náročnosti projektu - riziko záměrného zvolení jiného právního titulu

	- riziko neschopnosti vyhovění právu subjektu údajů - riziko změny legislativy týkající se ochrany osobních údajů - riziko špatné kontroly výstupů projektu - riziko špatného odhadu časové náročnosti úkolů - riziko nedokončení úkolů		
Popis produktu projektu	- vytvoření Směrnice o ochraně osobních údajů - vytvoření Informačního memoranda na internetové stránky společnosti - vytvoření Metodiky řízení výkonu práv subjektů - vytvoření Registru záznamů o činnostech zpracování OÚ - vzor dodatku ke smlouvě o zpracování OÚ se Zpracovateli - vytvoření vnitřního předpisu IT bezpečnosti		
Projektový přístup	- v projektu bude zapojena externí advokátní kancelář, která bude revidovat soulad podniknutých kroků s nařízením - dále budou kvůli malému počtu zaměstnanců spojeny určité projektové role, avšak v povoleném rozsahu, které umožňuje PRINCE2, aby nedocházelo ke střetu zájmů		
Zvolená možnost rozsahu projektu (1,2)	2	Schválil:	Ředitel společnosti (Sponzor projektu)
		Datum:	12.11.2018

Zdroj: Vlastní zpracování

Aktualizace registrů, daily log a lessons log

V rámci dokumentace nedošlo ke změnám.

Aktualizace projektového plánu

V průběhu projektu docházelo k průběžnému monitoringu probíhajících změn, při kterém docházelo ke změnám v dobách trvání činností a také k odstranění zpočátku

plánovaných činností, které již nebylo nutné provést. Celková doba trvání projektu se zkrátila na 22,5 dní a zároveň došlo ke zlevnění projektu o 27 720 Kč.

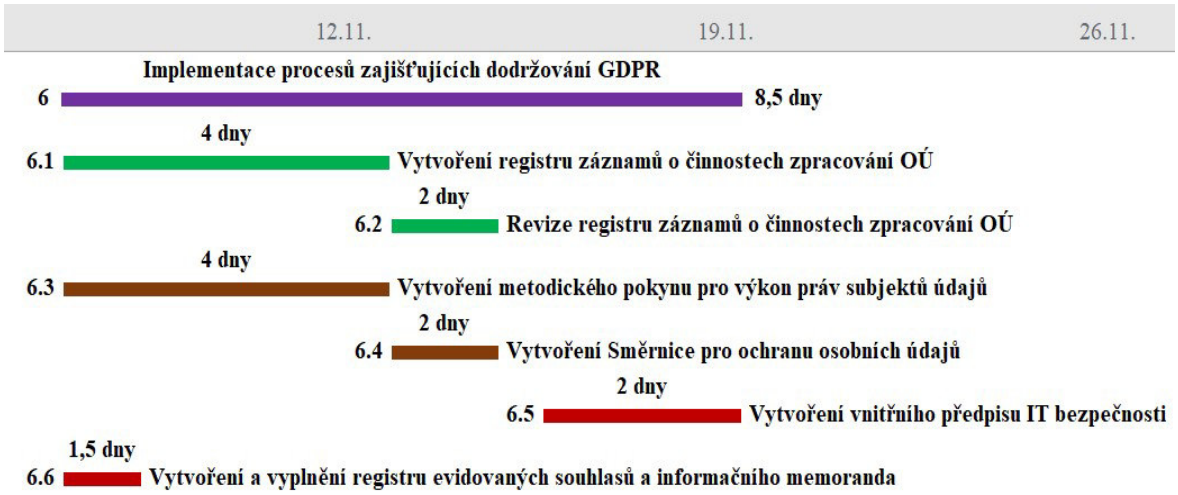
Obrázek 16 -Aktuální projektový plán

Zdroj: Vlastní zpracování

5.3.7 Implementace procesů zajišťujících dodržování GDPR

V této fázi projektu dochází již k přímé implementaci procesů zajišťující soulad s nařízením GDPR a zejména vytvoření základní dokumentace, jejíž účelem je prokázání souladu organizace dozorovému úřadu v případě kontroly.

Obrázek 17 - Ganttův diagram 6. milníku



Zdroj: Vlastní zpracování

6.1 Vytvoření registru záznamů o činnostech zpracování OÚ

Vytvoření registru záznamů o činnostech zpracování osobních údajů je jedním ze základních požadavků kladených nařízením GDPR. Pro jeho vytvoření byly plánovány 4 dny za účasti asistentky, business analytika, fakturantky a správce IT.

Registr musí obsahovat:

- ID činnosti;
- Název činnosti;
- Právní tituly;
- Účel zpracování;
- Vlastník činnosti;
- Informace o správcích a zpracovatelích osobních údajů;
- Kdo je subjekt údajů;
- Kdo má přístup k datům a jaká je forma zabezpečení;
- Seznam systému, ve kterých probíhá zpracování;
- Archivační a skartační lhůta osobních údajů;

- Informace o tom, zda dochází k přenosu dat mimo EU, v jaké formě a do jakých zemích;
- Informace, zda je zpracování osobních údajů zpracovatelem smluvně zajištěno;
- Jaké osobní údaje jsou zpracovávány;
- Informace, zda dochází ke zpracování citlivých osobních údajů.

Skutečná délka trvání této činnosti se z plánovaných 4 dnů prodloužila na 6 pracovních dní, protože asistentka a fakturantka byly indisponovány jinými pracovními úkoly, které přímo souvisely s náplní jejich práce. Zároveň, zde došlo k aplikaci studentova syndromu, kdy pracovní úsilí nebylo vynakládáno rovnoměrně, ale až u blížícího se termínu dokončení činnosti.

Dále se při tvorbě dokumentu vyskytl další problém, kdy zaměstnanci neznali archivační a skartační lhůty, které se váží k určitým kategoriím osobních údajů a právním titulům pro zpracování. Řešení tohoto problému bylo eskalováno na právníka, aby v rámci revize registru tyto údaje doplnil.

6.2 Revize registru záznamů o činnostech zpracování OÚ

Hlavním cílem revize registru záznamů o činnostech zpracování osobních údajů bylo zkontrolovat vhodnost přiřazení jednotlivých právních titulů k činnostem a na základě požadavku z činnosti 6.1 doplnit informace o archivačních a skartačních lhůtách.

Po revizi dokumentu ze strany právníka došlo ke kontrole kvality dokumentu prostřednictvím checklistu a následného zaznamenání do registru kvality.

Tabulka 18 - Checklist Registru záznamů o činnostech zpracování osobních údajů

Jsou doplněny následující informace?	ANO/NE
ID činnosti	ANO
Název činnosti	ANO
Právní titul	ANO
Účel zpracování	ANO
Vlastník činnosti	ANO
Informace o správcích a zpracovatelích osobních údajů	ANO
Kdo je subjekt údajů	ANO
Kdo má přístup k datům a jaká je forma zabezpečení	ANO

seznam systému, ve kterých probíhá zpracování	ANO
Archivační a skartační lhůta osobních údajů	ANO
Informace o tom, zda dochází k přenosu dat mimo EU, v jaké formě a do jakých zemích	ANO
Informace, zda je zpracování osobních údajů Zpracovatelem smluvně zajištěno	ANO
Jaké osobní údaje jsou zpracovávány	ANO
Informace, zda dochází ke zpracování citlivých osobních údajů	ANO

Zdroj: Vlastní zpracování

6.3 Vytvoření metodického pokynu pro výkon práv subjektů údajů

Účelem metodického pokynu pro výkon práv subjektů údajů je vytvoření jednotné metodiky, podle které se každý zaměstnanec společnosti bude řídit v případě obdržení takové žádosti. Bez existence pokynu by mohlo dojít k nevyřízení žádosti nebo by nebyla dodržena lhůta, která je nařízená GDPR nařízením.

Vytvořením metodického pokynu byl pověřen právník a nedošlo zde ke změně oproti projektovému plánu. Po obdržení finální verze dokumentu provedl projektový manažer kontrolu kvality pomocí checklistu (viz níže), a také byla kontrola zapsána do registru kvality. Vytvořený dokument je uveden v příloze č. 5 této práce.

Tabulka 19 - Checklist metodického pokynu pro výkon práv SÚ

Jsou doplněny následující informace?	ANO/NE
Předmět a rozsah působnosti dokumentu	ANO
Definice základních pojmů	ANO
Vymezení jednotlivých práv subjektů údajů	ANO
K jednotlivým právům jsou uvedeny příklady	ANO
Popis procesu vyřízení žádosti subjektu údajů	ANO
Komunikační kanály pro vyřízení žádostí	ANO
Proces identifikace a verifikace žadatele	ANO
Situace, kdy lze odmítnout žádost	ANO
Situace, kdy lze účtovat náklady za vyřízení žádosti	ANO
Definice lhůt pro vyřízení žádosti	ANO
Vzor Žádosti subjektu údajů	ANO
Vzor Odpovědi na žádost subjektu údajů	ANO

Zdroj: Vlastní zpracování

6.4 Vytvoření Směrnice o ochraně osobních údajů

Směrnice o ochraně osobních údajů je stěžejním dokumentem celé implementace nařízení GDPR, protože její kvalita a následné dodržování slouží zároveň jako prevence proti vzniku bezpečnostního incidentu ze strany zaměstnanců. Směrnice je uvedena v příloze č. 4 této práce.

Tabulka 20 - Checklist Směrnice o ochraně osobních údajů

Jsou doplněny následující informace?	ANO/NE
Definice základních pojmů	ANO
Role a odpovědnosti	ANO
Zásady zpracování osobních údajů	ANO
Fyzická bezpečnost	ANO
IT bezpečnost	ANO
Kontrolní mechanismy	ANO
Pravidelná školení zaměstnanců	ANO
Vedení a aktualizace záznamů o činnostech zpracování	ANO
Zpracovatelské vztahy	ANO
Pravidelná revize a aktualizace interních předpisů	ANO
Archivace a likvidace osobních údajů	ANO

Zdroj: Vlastní zpracování

6.5 Vytvoření vnitřního předpisu IT bezpečnosti

Vzhledem k podnikatelské činnosti společnosti, kdy k poskytování služeb klientům dochází prostřednictvím sofistikovaného softwaru ve formě internetového bankovnictví a komunikace uvnitř společnosti i mimo ni prochází skrze IT nástroje bylo nezbytné vytvořit vnitřní předpis IT bezpečnosti.

Kvalita vnitřního předpisu IT bezpečnosti byla posouzena též prostřednictvím checklistu (viz níže). Vnitřní předpis vzhledem k svému charakteru nebude v této práci uveřejněn.

Tabulka 21 - Checklist vnitřního předpisu IT bezpečnosti

Jsou doplněny následující informace?	ANO/NE
Informační systém a jeho zabezpečení	ANO
Role a odpovědnosti	ANO
Administrace přístupů a oprávnění	ANO
Definice základních podmínek pro práci s výpočetní technikou a daty	ANO
Pravidla používání elektronické pošty	ANO
Pravidla používání internetu	ANO
Ochrana osobních a citlivých OÚ v rámci informačního systému	ANO
Systém zálohování	ANO

Zdroj: Vlastní zpracování

6.6 Vytvoření a vyplnění registru evidovaných souhlasů a informačního memoranda

Při této činnosti produktový manažer zaznamenal do registru souhlasů veškeré souhlasy se zpracováním osobních údajů, které byly získány zejména prostřednictvím formuláře na webových stránkách společnosti.

Pro účely této diplomové práce nebude uveden kompletně vyplnění registr souhlasů, protože by tak došlo k porušení nařízení GDPR, neboť by šlo o zpracování osobních údajů bez právního titulu. Na obrázku č. 16 je zobrazen nevyplněná šablona registru.

Obrázek 18 - Registr souhlasů

Informace o subjektu údajů				Souhlasy se zpracováním OÚ			Propojení na Registr záznamů	
Jméno	Příjmení	Datum narození / RČ	Kontaktní údaje (adresa, email, tel.)	Datum udělení souhlasu	Datum odvolání souhlasu	Forma souhlasu	ID	Název činnosti

Zdroj: Vlastní zpracování

Vypracováním informačního memoranda byl též pověřen produktový manažer, protože byl pro tento účel nejkompetentnější osobou, neboť hlavní zdroj získávání souhlasů a následné zpracování osobních údajů je v jeho režii. Informační memorandum je uvedené v příloze č. 3 této práce.

Závěr šestého milníku

Při vytváření registru záznamů o činnostech zpracování osobních údajů došlo k prodloužení této činnosti o 2 dny, avšak nedošlo k prodloužení celkové doby trvání projektu. Náklady na činnost zůstaly konstantní.

5.3.8 Nastavení postupů pro minimalizaci škod při bezpečnostním incidentu a školení zaměstnanců

Na základě dohody mezi finanční manažerkou a právníkem bylo rozhodnuto, že nastavení postupů minimalizace škod při bezpečnostním incidentu bude ve formě rozšíření metodického pokynu pro výkon práv subjektů údajů, protože jsou tematicky přímo spjata. Tato část metodického pokynu nebude v této práci zveřejněna, protože se jedná o důvěrnou část dokumentu a vedení společností její zveřejnění neumožnilo.

Tabulka 22 - Checklist postupu minimalizace škod

Jsou doplněny následující informace?	ANO/NE
Sestava eskalačního týmu	ANO
Postup analýzy škod	ANO
Systém stanovení dopadu na subjekt údajů	ANO
Odpovědnost za vytvoření následné prevence do budoucna	ANO

Zdroj: Vlastní zpracování

Poslední aktivitou projektu bylo školení zaměstnanců právníkem v oblasti GDPR, které bylo zakončeno závěrečným testem a získáním certifikátu o absolvování školení.

Závěr sedmého a osmého milníku

Vše proběhlo podle projektového plánu.

5.3.9 Aktualizace registrů

V návaznosti na proběhlé změny v projektu a akceptací vytvořených projektových produktů dochází k aktualizaci registru kvality a lessons log.

Aktualizace lessons log

Pro uplatnění principu projektového standardu PRINCE2 lessons learned byly zaznamenány dvě události, které měly podstatný vliv na projekt. Ačkoli jedna činnost měla pozitivní dopad a druhá dopad negativní, tak obě byly zapříčiněny chybami v plánování, které by se v budoucnu neměly opakovat.

Tabulka 23 - Aktualizovaný lessons log

Revizní historie				
Datum revize	**Předchozí datum revize**	**Souhrn změn**	**Priorita změn**	**Schválil**
7.11.2018	-	Zápis poučení	malá	PM
15.11.2018	7.11.2018	Zápis poučení	malá	PM

Zaznamenaná poučení					
ID	**Oblast**	**Popis**	**Dopad na projekt**	**Plynoucí doporučení**	**Datum zápisu a jméno pracovníka**
1	Fáze analýzy	č. 4.2 a 4.3	Projekt v předstihu	Lépe posoudit systém analýz, aby nedocházelo k chybenému plánování	7.11.2018 Projektový manažer
2	Tvorba registru	Tvorba registru záznamů o činnostech zpracování	Prodloužení činnosti projektu	Vytvoření sankčního systému při nedodržení termínu a preventivní stanovení CPM	15.11.2018 Projektový manažer

Zdroj: Vlastní zpracování

Registr kvality

V registru kvality byly zaznamenány veškeré události schvalování projektových produktů. V rámci této evidence v projektu implementace GDPR nařízení nedocházelo k opakovaným schvalovacím procesům. Veškeré zaznamenané údaje jsou k dispozici v tabulce číslo 24 – Aktualizovaný registr kvality.

Tabulka 24 - Aktualizovaný registr kvality

ID	Produkt	Metoda měření kvality	Vytvořil	Zkontroloval	Schválil	Datum kontroly	Výsledek
1	Registr záznamů o činnostech zpracování OÚ	Checklist	Asistentka, Business analytik, Fakturantka, Správce IT	Finanční manažerka, Projektový manažer	Projektový manažer	19.11.18	Schváleno
2	Metodický pokyn pro výkon práv subjektů údajů	Checklist	Právník	Projektový manažer	Jednatel	13.11.18 20.11.18	Schváleno
3	Směrnice o ochraně osobních údajů	Checklist	Právník	Projektový manažer	Jednatel	15.11.18	Schváleno
4	Vnitřní předpis IT bezpečnosti	Checklist	Právník, Správce IT	Projektový manažer	Jednatel	19.11.18	Schváleno
5	Registr evidovaných souhlasů	Vizuální kontrola	Produktový manažer	Projektový manažer	Projektový manažer	8.11.18	Schváleno
6	Informačního memorandum	Checklist	Produktový manažer	Projektový manažer	Jednatel	8.11.18	Schváleno

Zdroj: Vlastní zpracování

6 Výsledky práce

V rámci uzavření projektu byla vypracována závěrečná zpráva o projektu, která v sobě zahrnuje nejdůležitější informace o průběhu projektu a zaměřuje se na čtyři důležité prvky, kterými jsou projektový plán, projektový tým, business case, akceptační proces, a nakonec řízení rizik. Zpracovaná závěrečná zpráva byla následně předána vedení společnosti.

6.1.1 Závěrečná zpráva o projektu

Projektový plán

V projektovém plánu došlo ke změnám v délkách trvání u dvou činností, a to u činnosti 1.2, kdy došlo k úspoře 0,5MD a snížení nákladů o 1 800 Kč a u činnosti 6.1 došlo naopak k prodloužení činnosti o dva dny a tím došlo ke zpoždění vypracování projektového produktu Registru záznamů o činnostech zpracování osobních údajů, čímž byla posunuta činnost jeho revize. Avšak prodloužení vytvoření produktu nemělo vliv na celkovou dobu trvání projektu a na nákladovou složku. Dále nebyly v projektu realizovány činnosti 4.2 a 4.3, které měly hodnotit rizika plynoucí pro společnost a subjekt údajů na základě provedení DPIA, které však nemuselo být realizováno na základě sebehodnocení prostřednictvím vydané metodiky dozorovým úřadem ČR. Díky zrušení těchto činnosti došlo ke zkrácení projektu o 3MD a snížení nákladů o 25 920 Kč. Projekt byl na základě výše uvedených změn dokončen o 13 dní dříve oproti plánovanému datu a došlo k úspoře nákladů v celkové výši 27 720 Kč.

Projektový tým

Projektový tým si vedl po většinu projektu velmi dobře, jediné pochybení nastalo při vytváření registru o činnostech zpracování osobních údajů, kdy díky projevu studentova syndromu a multitaskingu došlo k prodloužení této činnosti. Veškeré činnosti v projektu probíhaly v rámci standardní pracovní doby a nedocházelo k přesčasové práci.

Business case

V rámci aktualizace business casu došlo k snížení nákladů na projekt o 27 720 Kč, nedošlo však ke změnám v rozpočtu na právní služby, které byly jedním z požadavků. Dokument zůstal validní po celou dobu projektu.

Akceptační proces

Všechny projektové produkty byly akceptovány prostřednictvím checklistů a nedocházelo k opětovné akceptaci produktů či změnovým požadavkům.

Řízení rizik

Rizika nebyla v průběhu projektu zaznamenána a po dobu projektu nebyla nutná aktualizace registru rizik

7 Závěr

Hlavním cílem diplomové práce bylo provést popis a zhodnocení implementace GDPR nařízení ve vybrané společnosti, tak aby bylo dosaženo souladu s daným nařízením. Implementace byla provedena prostřednictvím projektového řízení, a to s využitím mezinárodně uznávaného projektového standardu PRINCE2, který zároveň poskytl autorovi potřebná vodítka pro vhodné vedení projektu.

Dílčími cíli této práce bylo vytvořit znalostní databázi z dokončeného projektu, která bude využita pro budoucí projekty, neboť současná úroveň projektového řízení ve firmě je teprve v začátcích. Dále vytvořit standardizovaný projekt implementace GDPR nařízení, který čtenář této práce může použít pro implementaci tohoto nařízení s ohledem na velikost jím vybrané společnosti a charakterem jejího podnikání.

V prvé řadě proběhlo mapování zpracování, tj. veškerých aktivit, kdy dochází k jakémukoli zpracování osobních údajů fyzických osob včetně definování používaných systémů ochrany těchto údajů, právních titulů a archivačních a skartačních dob. Z celkové analýzy současného stavu zpracování a GAP analýzy byl upřesněn projektový plán.

V průběhu projektu byl zjištěn nedostatek v kvalitě plánování projektu, kdy docházelo ke změnám v termínech dokončení činností. Ačkoli tři změny měly pozitivní dopad na projekt, díky nimž byl projekt zaprvé dokončen o 13 dní dříve a také došlo ke snížení nákladů o 27 720 Kč.

Tyto změny byly vyhodnoceny jako chybné plánování z nedostatku kompetentních lidských zdrojů společnosti, které by provedly dvoufázové ověření časové náročnosti aktivit. Kdyby však pro tyto účely byly využity externí služby, tak by se projektové náklady zcela jistě zvýšily a v porovnání s přidanou hodnotou by se jevily jako neúčelné.

Dále proběhla změna délky trvání činnosti, která prodloužila vypracování registru záznamů o činnostech zpracování osobních údajů, aniž by však prodloužila celkovou dobu trvání projektu nebo zvýšila náklady. Příčinou byl projev studentova syndromu a multitasking daného zdroje, kdy nejprve odložil zpracování úkolu na pozdější dobu a poté byl nucen se věnovat svým primárním úkolům plynoucí z jeho pozice ve společnosti.

8 Seznam použitých zdrojů

AXELOS. 2017. *Managing Successful Projects with PRINCE2™.* London : TSO, 2017. ISBN 978-0-11-331533-8.

Doležal, Jan, a další. 2012. *Projektový management podle IPMA.* Praha : Grada Publishing, a.s., 2012. ISBN 978-80-247-4275-5.

Doskočil, Radek. 2013. *Metody, techniky a nástroje řízení projektů.* Brno : Akademické nakladatelství CERM, s.r.o., 2013. ISBN 978-80-7204-863-2.

IPMA. 2017. *Mezinárodní standard projektového řízení podle IPMA ICB v.4.* místo neznámé : IPMA Czech Republic, 2017. ISBN 978-80-7326-286-0.

Maule, Pavel. 2004. SYSTÉMOVÁ INTEGRACE 3/2004. *Česká společnost pro systémovou integraci.* [Online] 1. Březen 2004. [Citace: 12. Březen 2019.] www.cssi.cz/cssi/system/files/all/SI_04_3_maule.pdf.

Nezmar, Luděk. 2017. *GDPR: Praktický průvodce implementací.* Praha : GRADA Publishing, a.s., 2017. ISBN 978-80-271-0668-4.

PM Consulting. 2019. ICB – IPMA® Competence Baseline. *www.pmconsulting.cz.* [Online] PM Consulting, 2019. [Citace: 1. Březen 2019.] https://www.pmconsulting.cz/pm-wiki/icb-ipma-competence-baseline/.

PRIVAZYPLAN. 2018. Článek 35 EU obecné nařízení o ochraně osobních údajů "Posouzení vlivu na ochranu osobních údajů". *Privacy-regulation.* [Online] Secure Data Service, 5. Září 2018. [Citace: 1. Březen 2019.] http://www.privacy-regulation.eu/cs/35.htm.

Řeháček, Petr. 2013. *Projektové řízení podle PMI.* Praha : Ekopress, 2013. ISBN 978-80-86929-90-3.

Svozilová, Alena. 2011. *Projektový management.* Příbram : Grada Publishing a.s., 2011. ISBN 978-80-247-3611-2.

ÚOOÚ. 2018. K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA). *Úřad pro ochranu osobních údajů.* [Online] 2018. [Citace: 1. Březen 2019.] https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=33193.

Úřad pro ochranu osobních údajů. 2017. GDPR (obecné nařízení). *ÚOOÚ.* [Online] Úřad pro ochranu osobních údajů, 2017. [Citace: 5. Říjen 2018.] https://www.uoou.cz/gdpr/ds-3938/p1=3938.

Úřední věstník Evropské unie. 2016. EUR-lex. *Eur-lex.europa.eu.* [Online] Úřední věstník Evropské unie, 27. Duben 2016. [Citace: 20. Prosinec 2018.] https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679.

Žůrek, Jiří. 2017. *Praktický průvodce GDPR.* [editor] Jitka Mgr. Bezoušková. Olomouc : Nakladatelství ANAG, 2017. ISBN 978-80-7554-097-3.

9 Přílohy