VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU
Nárožní 2600/9a, 158 00 Praha 5

DIPLOMOVÁ PRÁCE

Vysoká škola ekonomie a managementu
info@vsem.cz / www.vsem.cz

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

NÁZEV DIPLOMOVÉ PRÁCE/TITLE OF THESIS
Návrh transformace implementovaného GDPR do procesního řízení vybrané organizace

TERMÍN UKONČENÍ STUDIA A OBHAJOBA (MĚSÍC/ROK)
Říjen / 2023

JMÉNO A PŘÍJMENÍ STUDENTA / STUDIJNÍ SKUPINA
Bc. Simona Beneš Kyjovská / KEMMA05

JMÉNO VEDOUCÍHO DIPLOMOVÉ PRÁCE
Ing. Radka Vaníčková, Ph.D., MBA

PROHLÁŠENÍ STUDENTA
Odevzdáním této práce prohlašuji, že jsem zadanou diplomovou práci na uvedené téma vypracoval/a samostatně a že jsem ke zpracování této diplomové práce použil/a pouze literární prameny v práci uvedené. Jsem si vědom/a skutečnosti, že tato práce bude v souladu s § 47b zák. o vysokých školách zveřejněna, a souhlasím s tím, aby k takovému zveřejnění bez ohledu na výsledek obhajoby práce došlo. Prohlašuji, že informace, které jsem v práci užil/a, pocházejí z legálních zdrojů, tj. že zejména nejde o předmět státního, služebního či obchodního tajemství či o jiné důvěrné informace, k jejichž použití v práci, popř., k jejichž následné publikaci v souvislosti s předpokládanou veřejnou prezentací práce, nemám potřebné oprávnění. Datum a místo: 1.9.2023 Kolín

PODĚKOVÁNÍ
Ráda bych tímto poděkovala vedoucí diplomové práce Ing. Radce Vaníčkové Ph.D., MBA za metodické vedení a odborné konzultace, které mi poskytla při zpracování diplomové práce. Ráda bych poděkovala i všem zaměstnancům organizace XY, kteří projevili součinnost při probíhajících výzkumech. V neposlední řadě patří poděkování mé rodině, za jejich podporu.

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

SOUHRN

1. Cíl práce:

Primárním cílem diplomové práce je tvorba návrhu projektu transformace implementovaného GDPR do procesního řízení organizace. Sekundárními cíli je zhodnocení současného stavu dodržování povinností integrovaných s GDPR ve prospěch vybrané organizace s identifikací jednotlivých procesů, ve kterých dochází ke zpracovávání osobních údajů napříč organizací.

2. Výzkumné metody:

V teoreticko-metodologické části práce byla využita literární rešerše na základě komparace odborných textů citovaných autorů tuzemských a zahraničních zdrojů včetně právních předpisů, směrnic, interních zdrojů a dat, nařízení a ostatních pramenů. Empirická data a výsledky byly získány z interních zdrojů v souladu s formulací výzkumných otázek a cílů a použitých vědecko-výzkumných analýz. V analytické části byly využity tyto metody: kvalitativní a kvantitativní výzkum, polostrukturovaný rozhovor, dotazníkové šetření, analýza interních dokumentů, komparace dat a výsledků, metoda syntézy a dedukce, datový audit, GAP analýza. Význam a přínos GAP analýzy umožnil vymezení rozsahu projektu a predikci jednotlivých projektových činností pro realizaci návrhu projektu.

3. Výsledky výzkumu/práce:

Polostrukturovaný rozhovor poukázal na nedostatky v plnění požadavků vyplývajících z GDPR. Toto zjištění bylo potvrzeno rozborem interních dokumentů a komparací s informacemi získanými z teoretické části práce, které potvrdily absenci vnitřních předpisů ochrany osobních údajů a školení zaměstnanců. Dotazníkové šetření mezi zaměstnanci odhalilo mezery v bezpečnostních a právních procesech. Datovým auditem a s podporou GAP analýzy byly identifikovány slabá místa mezi plánovaným a reálným stavem souladu s GDPR v nastavených procesech organizace. Nedostatky odhalily nekompletní záznamy o činnostech zpracování osobních údajů, absenci zpracovatelských smluv, školení zaměstnanců, nastavení interních procesů ochrany dat, nízkou implementnost právních a legislativních předpisů a nedostatečné plnění funkce pověřence pro ochranu osobních údajů. Rozsah návrhu projektu pro zajištění souladu s GDPR byl vymezen v 16 činnostech, mezi nimiž je: zajištění adekvátního pověřence pro ochranu osobních údajů, zamezení nadbytečného vyžadování nezákonných a nadbytečných osobních údajů či revize interních předpisů. Délka projektu byla naplánována na 72 dnů, resp. 52 pracovních dnů v kalendářních roce s celkovými náklady 47 850 Kč. Na základě získaných výsledků lze projekt realizovat a jeho cíl projektových aktivit byl úspěšný.

4. Závěry a doporučení:

Závěrem konstatuji, že cíl práce byl naplněn, návrh projektu byl implementován do směrnic vnitřních předpisů organizace. Tímto dochází k zajištění adekvátního pověřence pro ochranu osobních údajů, nastavení procesů a interních předpisů k zabezpečení a ochraně osobních údajů. V průběhu práce byly zodpovězeny jednotlivé výzkumné otázky. Druhá hypotéza byla potvrzena částečné z důvodu probíhající realizace projektu. Ekonomická přidaná hodnota projektu představuje návrat vložených nákladů na školení, sociální hodnotu přináší společenský užitek pro lidi a hospodárnost vynaložených prostředků je zajištěna udržitelností projektu v přesahu zavedených procesů, které připouští nové vstupy v budoucnosti. Potenciál práce spočívá v orientaci na účelnost vydaných nákladů do projektu a na efektivnost nastavených procesů z hlediska využívaných zdrojů při zpracovávání osobních údajů.

KLÍČOVÁ SLOVA

Osobní údaj, implementace, GDPR, projekt, školství

VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Nárožní 2600/9a, 158 00 Praha 5

SUMMARY

1. Main objective:

The primary goal of the master´s thesis is to create a proposal for a project that transforms the implemented GDPR into the process management of the organization. The secondary goals include an assessment of the current state of compliance with GDPR-related obligations for the benefit of the chosen organization, along with the identification of individual processes involving the processing of personal data across the organization.

2. Research methods:

In the theoretical-methodological part of the work, literary research was employed through a comparison of expert texts cited by both domestic and foreign authors, including legal regulations, directives, internal resources and data, regulations and other sources. Empirical data and results were obtained from internal sources in accordance with the formulation of research questions and objectives, as well as the applied scientific research analyses. In the analytical part, the following methods were utilized: qualitative and quantitative research, semi-structured interviews, questionnaire surveys, analysis of internal documents, data and results comparison, synthesis and deduction method, data audit and GAP analysis. The significance and contribution of the GAP analysis enabled the delineation of the project scope and the prediction of individual project activities for the implementation of the project proposal.

3. Result of research:

The semi-structured interview highlighted deficiencies in meeting the requirements arising from GDPR. This finding was corroborated by analyzing internal documents and comparing them with information obtained from the theoretical part of the work, which confirmed the absence of internal regulations for personal data protection and employee training. A questionnaire survey among employees revealed gaps in security and legal processes. Through data auditing and with the support of GAP analysis, weak points were identified between the planned and actual state of GDPR compliance within the organization´s established processes. The deficiencies unveiled incomplete records of personal data processing activities, the absence of data processing agreements, employee training, establishment of internal data protection processes, low implementation of legal and legislative regulations, and inadequate fulfillment of the Data Protection Officer´s role. The scope of the project proposal for achieving GDPR compliance was outlined in 16 activities, including ensuring an adequate Data Protection Officer, preventing excessive collection of unlawful and unnecessary personal data, and revising internal regulations. The project duration was planned for 72 days, or 52 working days in the calendar year, with total costs of 47,850 CZK. Based on the obtained results, the project can be implemented, and its aim of project activities was successful.

4. Conclusions and recommendation:

In conclusion, I ascertain that the goal of the work has been achieved: the project proposal has been implemented into the internal regulations of the organization. This ensures the provision of an adequate Data Protection Officer, the establishment of processes and internal regulations for securing and safeguarding personal data. Throughout the work, individual research questions have been addressed. The second hypothesis has been confirmed partially due to the ongoing project implementation. The economic added value of the project represents a return on the invested costs for training, the social value brings societal benefits for people, and the efficiency of resources expended is ensured by the sustainability of the project beyond established processes, allowing for new inputs in the future. The potential of the work lies in focusing on the purposefulness of costs allocated to the project and the effectiveness of established processes in terms of resource utilization during personal data processing.

KEYWORDS

Personal data, implementation, General Data Protection Regulation, project, education

JEL CLASSIFICATION

K00 General, K19 Other, K39 Other

Vysoká škola ekonomie a managementu
Nárožní 2600/9a, 158 00 Praha 5

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jméno a příjmení:	Bc. Simona Kyjovská
Studijní program:	Ekonomika a management (Ing.)
Studijní skupina:	KEMMA05
Název DP:	Návrh transformace implementovaného GDPR do procesního řízení vybrané organizace
Zásady pro vypracování (stručná osnova práce):	1 Úvod 2 Teoreticko-metodologická část 2.1 GDPR a povinnosti organizace 2.2 Integrace GDPR do procesního řízení 2.3 Metodika práce 3 Analytická část 3.1 GDPR v dílčích procesech organizace 3.2 Návrh projektu změnového řízení 3.3 Vyhodnocení výsledků a přínosů 4 Závěr
Seznam literatury: (alespoň 4 zdroje)	• DUMAS, M., LA ROSA, M., REIJERS, H. A., MENDLING, J. *Fundamentals of Business Process Management*. Germany: Springer Berlin Heidelberg, 2018. 527 s. ISBN 978-3-662-56509-4. • FOULSHAM, M., HITCHEN, B., DENLEY, A. *GDPR: how to achieve and maintain compliance*. New York: Routledge, Taylor & Francis Group, 2019. 211 s. ISBN 978-0-429-44997-0. • JANEČKOVÁ, E. *GDPR: řešení problémů v praxi škol*. 1. vyd. Praha: Grada, 2020. 352 s. ISBN 978-80-271-1354-5. • ŠVECOVÁ, L., VEBER, J. *Produkční a provozní management*. Praha: Grada, 2021. 344 s. ISBN 978-80-271-4621-5.
Harmonogram:	• Zpracování cílů a metodiky do 15. 04. 2023 • Zpracování teoretické části do 15. 05. 2023 • Zpracování výsledků do 31. 07. 2023 • Finální verze do 01. 09. 2023
Vedoucí práce:	Ing. Radka Vaníčková, Ph.D., MBA

prof. Ing. Milan Žák, CSc.
rektor

V Praze dne 01. 04. 2023

Prof. Ing. Milan Žák CSc.
Digitálně podepsal Prof. Ing. Milan Žák CSc.
DN: cn=Prof. Ing. Milan Žák CSc., c=CZ, o=Vysoká škola ekonomie a managementu, a.s., givenName=Milan, sn=Žák, serialNumber=ICA - 10393535

Obsah

1 Úvod 1
2 Teoreticko-metodologická část práce 4
2.1 GDPR a povinnosti pro organizace 4
2.2 Integrace GDPR do procesního managementu 15
2.3 Metodika práce 20
3 Analytická část práce 24
3.1 GDPR v procesech organizace 24
3.2 Návrh projektu pro změnové řízení 39
3.3 Vyhodnocení výsledků a jejích přínosů 46
4 Závěr 54
Literatura 57
Seznam příloh I

Seznam zkratek

CPM	Critical Path Method, metoda kritické cesty
DPIA	Posouzení vlivu na ochranu osobních údajů
DPO	Data Protection Officer, Pověřenec pro ochranu osobních údajů
ESG	Enviromental, Social, Governance
EU	Evropská unie
GDPR	nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
PZH	Jednoduchá bodová polokvantitativní metoda (pravděpodobnost, závažnost, hodnotitelé)
ÚOOÚ	Úřad pro ochranu osobních údajů

Seznam diagramů

Diagram 1: Organizační struktura 24
Diagram 2: Hlavní procesy organizace XY 31
Diagram 3: Hlavní procesy organizace rozšířené o počty činností s osobními údaji 32
Diagram 4: Hlavní procesy organizace rozšířené o využívané systémy a datové toky 33
Diagram 5: Síťový graf činností projektu 43

Seznam tabulek

Tabulka 1: Vyhodnocení souladu stanovených a plněných povinností v organizaci XY 25
Tabulka 4: Výhody a nevýhody interních a externích DPO 28
Tabulka 7: Přehled činností projektu 39
Tabulka 9: Ganttův diagram činností projektu doplněný o zdroje a časové rezervy 43
Tabulka 10: Analýza rizik návrhu projektu 44
Tabulka 11: Kalkulace nákladů návrhu projektu 45

1 Úvod

Ochrana osobních údajů se dotýká každého jednotlivce i organizací po celém světě. Jedná se o součást lidských práv a svobod a její význam by neměl být podceňován. Jak již ze samotného pojmu vypovídá, primárním cílem je ochrana, a to všech osobních údajů, které se vztahují ke konkrétním osobám. Je možné říct, že celá tato oblast vznikla pro fyzické osoby a jejím primárním účelem je jejich ochrana a prevence před možným poškozením. Svými právy i povinnostmi se ochrana osobních údajů týká jak fyzických, tak právnických osob a v mnoha zemích je pod záštitou zákona.

Každá osoba disponuje údaji a daty, na základě, kterých může dojít k jejich identifikaci. Jinak řečeno osobními údaji jsou obecně označována ta data, díky kterým jsou ostatní schopni danou osobu identifikovat. Ač by se mohlo zdát, že každý jedinec má své osobní údaje zcela pod kontrolou, nemusí tomu být vždy tak. Je důležité vyzdvihnout, že osobní údaje jsou běžně poskytovány různým institucím, a mnohdy si to lidé ani neuvědomují. Příkladem může být založení věrnostní karty v kamenném obchodě, vyzvednutí zásilky u přepravní společnosti, zaslání životopisu na zveřejněnou nabídku práce nebo sepsání reklamačního protokolu pro zakoupený produkt. Ve všech uvedených příkladech jsou předávány osobní údaje, které jsou dále zpracovávány společnostmi. Ne vždy však lze zpracování osobních údajů ovlivnit, v některých případech jako jsou údaje zaměstnanců, studentů dané školy či pacientů, stanovuje přímo zákon povinnost konkrétním organizacím zpracovávat osobní údaje těchto osob.

Za osobní údaje jsou obecně považovány základní identifikační a kontaktní údaje jednotlivců, mezi osobní údaje se však zařazují i fotografické a audiovizuální záznamy, IP adresa, informace o politických názorech i genetické a biometrické údaje, tento souhrn značí pouze krátký výčet. Některé z údajů mohou být dokonce natolik citlivé, že jejich zneužití může jedince značně poškodit. I to je jeden z důvodů, proč jsou osobní údaje chráněny legislativou. Ochrana osobních údajů je oblast, která se dostala do povědomí i po právní stránce méně orientované populaci zejména díky General Data Protection Regulation neboli nařízení GDPR. Toto nařízení nabylo účinnosti v květnu roku 2018 a vztahuje se na celou Evropskou unii. Jedním z důvodů vzniku GDPR bylo posílit práva osob v případě neoprávněného zacházení s jejich osobními údaji. Vzhledem k pokroku a neustálému vývoji bylo nutné právní ochranu přizpůsobit současné době. Avšak osobní údaje a jejich ochrana měly své zastoupení v právních předpisech již mnohem dříve. O tom vypovídá i Listina základních práv a svobod nebo zákon č. 101/2000 Sb., o ochraně osobních údajů. Jak již bylo zmíněno, legislativa udává povinnost veřejným i soukromým institucím ve vybraných případech zpracovávat osobní údaje osob a bez ohledu na tuto povinnost instituce mohou zpracovávat osobní údaje i nad stanovený rámec, pokud s tím daná osoba souhlasí. K tomu se váže dodržování určitých podmínek pro zpracovávání osobních údajů. Každý, kdo zpracovává osobní údaje musí dodržovat související právní předpisy, řídit se danými povinnostmi a respektovat práva osob, o nichž jsou osobní údaje zpracovávány. S příchodem nařízení GDPR se výčet povinností rozšířil a s tím i hrozba možných sankcí za jejich nedodržení. Za nejvýznamnější nově vzniklé povinnosti je uváděno zajištění pověřence pro ochranu osobních údajů a vedení záznamů o činnostech zpracování. Aby organizace naplňovaly soulad s ustanovením GDPR, musí zároveň dbát zásad, které z nařízení vyplývají. Zmiňované zásady komplexně vypovídají, že správce údajů smí zpracovávat pouze nezbytné osobní údaje po vymezenou dobu.

Organizace nemusí být na problematiku GDPR samy, zvlášť pokud množství jimi zpracovávaných osobních údajů je rozsáhlé a různorodé. To může být případ i vzdělávacích institucí, které zpracovávají osobní údaje nejen svých zaměstnanců, ale i studentů a případně zákonných zástupců. Mnoho firem nabízí své služby v podobě přenesení některých povinností v rámci GDPR na ně, poskytují pomoc s implementací nebo vystupují v roli konzultanta

pro tuto oblast. Pričemž v některých případech sami zřizovatelé u svých organizací prosazují outsourcování dané služby. V současné době mají organizace nespočet možností, kde adekvátní informace získat, přesto může být GDPR pro některé z nich stále relativně čerstvým tématem. Ačkoli GDPR již vešlo v platnost a organizace by se měly řídit stanovenými povinnostmi, neznamená to, že tomu tak je ve skutečnosti. Některé organizace mohou i nevědomě porušovat GDPR. Jedním z klíčových problémů organizací jsou podcenění významu daného nařízení, jeho neznalost nebo nedostatečné seznámení s ním. O tom vypovídá upozorňění ÚOOÚ (2019), které odkazuje na nadbytečné vyžadování souhlasů ve školství, jenž značí chybné chápání souhlasu se zpracováním osobních údajů. Podstatnou skutečnost představuje neustálý vývoj technologií, díky kterým jsou osobní údaje zpracovávány. To přináší v první řadě riziko nedostatečného zabezpečení a s tím souvisejícího zneužití osobních údajů. Na nutnost zabezpečení systémů také odkazuje ÚOOÚ (2020) a jako příklad uvádí situaci, kdy se studentovi střední školy podařilo vniknout do systému školy a pozměnit některé údaje. Neustálý vývoj technologií tak směřuje k potřebě pravidelného posuzování souladu s GDPR.

Povinnosti, které správcům osobních údajů vyplývají z GDPR nestačí pouze mít v paměti, ale pro úspěšné plnění je stěžejní jejich integrace do interních procesů. K jejich začlenění je třeba přistupovat důkladně, o tom svědčí i množství zdrojů, které se věnují implementaci GDPR do procesního řízení organizací. Například Nezmar (2017, s. 533-538) v tomto ohledu přináší postup, jak implementaci uchopit a vymezuje ji v několika krocích. Pakliže firmy uskutečnění integraci GDPR do jejich procesů, nelze automaticky předpokládat, že vše proběhlo v pořádku a daná právnická osoba je v souladu s ustanovením GDPR. Pokud dojde k identifikaci nedostatků nebo mezer v plnění stanovených povinností, je nutné přijmout opatření a napravit požadovaný stav. V každém případě je stěžejní sjednat nápravu, a to, pokud možno, v co nejkratším čase. Na základě rozsahu nedostatků a porušení zabezpečení ochrany osobních údajů nařizuje GDPR správcům subjektů údajů přijmout i další nezbytné kroky, kterými je posouzení nahlášení skutečnosti ÚOOÚ a subjektům údajů. Přičemž představuje-li odhalený nesoulad s GDPR velký rozsah, doporučuje se k celé situaci přistupovat z pohledu projektu a danou skutečnost řídit jako projekt změnového řízení s vytyčením zdrojů i časového harmonogramu.

Primárním cílem diplomové práce je tvorba návrhu projektu transformace implementovaného GDPR do procesního řízení organizace. Sekundárními cíli je zhodnocení současného stavu dodržování povinností integrovaných s GDPR ve prospěch vybrané organizace s identifikací jednotlivých procesů, ve kterých dochází ke zpracovávání osobních údajů napříč organizací. V souladu se stanovenými cíli práce došlo k formulaci výzkumných otázek:

1. Jakým způsobem jsou uplatňovány povinnosti vyplývající z GDPR v organizaci?
2. Je využití externího DPO pro danou organizaci efektivnější než tuto činnost delegovat na některého ze zaměstnanců?
3. Jaký je vztah mezi současně nastaveným systémem ochrany osobních údajů v organizaci a přístupem zaměstnanců k tomuto systému?
   a) Mají zaměstnanci potřebné informace k systému zabezpečení a ochrany osobních údajů v organizaci?
   b) Přistupují celistvě k nastavenému systému?
   c) Dbají zaměstnanci na dostatečné zabezpečení a ochranu osobních údajů před jejich neoprávněným zpřístupněním cizím osobám?
4. Jaké povinnosti je nutné revidovat ve stávajícím systému ochrany osobních údajů v organizaci potřebných k naplnění souladu s GDPR?

Dále došlo ke stanovení 2 hypotéz:

1. Pokud organizace neprovádí pravidelné kontroly outsourcovaných služeb, nemůže se spoléhat na důkladné plnění povinností integrovaných s GDPR.
2. Pokud organizace zjistí nedostatečné plnění povinností vyplývajících z GDPR, je schopna vlastními silami provést nápravu.

Tyto předpokládané výroky budou v rámci práce potvrzeny, nebo vyvráceny.

2 Teoreticko-metodologická část práce

Tato kapitola je rozdělena do tří částí, první podkapitola se věnuje stručnému vhledu do problematiky GDPR, povinnostem, které z ní vyplývají pro organizace a právům subjektů údajů. Následující druhá část se zaměřuje na integraci GDPR do procesního managementu organizace. V závěru je samotná podkapitola vyhrazena výzkumným metodám, které jsou v diplomové práci využity, viz kapitola 2.3 Metodika práce.

2.1 GDPR a povinnosti pro organizace

Z důvodu relativně stále nové problematiky jsou na úvod této podkapitoly stručně ozřejmeny základní pojmy a příslušná legislativa vztahující se k GDPR. Velká pozornost je věnována povinnostem, které se vztahují ke správcům osobních údajů, avšak pro ucelený pohled nebyla opomenuta ani práva subjektů údajů, kterým je věnována samostatná subkapitola.

2.1.1 Základní pojmy a legislativa

Jak popisuje Janečková (2020, s. 33-44) každá informace o identifikované nebo identifikovatelné fyzické osobě je osobním údajem a mezi základní identifikátory osobních údajů řadí jméno, příjmení, datum narození a rodné číslo. Rodné číslo však rozporuje Nonnemann (2018, s. 24), neboť jej považuje za specifický údaj, který je upraven v zákoně č. 133/2000 Sb., a který má při zpracování rodného čísla přednost, zároveň však nevylučuje omezené nakládání s tímto údajem v souladu s uvedenou legislativou. Zároveň Janečková (2020, s. 40-42) předpokládá, že někdy správce údajů ani nenapadne, že by údaj, který zpracovává představoval osobní údaj nebo naopak některé údaje mohou vyvolat pochybnosti, a v této souvislosti dále mezi osobní údaje zařazuje: telefonní číslo, emailovou a IP adresu. Nonnemann (2018, s. 20) tento výčet osobních údajů ještě rozšiřuje o další příklady: adresa bydliště, korespondenční adresa, číslo bankovního účtu, platební morálka, údaje o předchozích nákupech a dodává, že osobním údajem je vše, co je k dané osobě evidováno. Janečková (2020, s. 43-45) i Nonnemann (2018, s. 21-22) poukazují na kategorii zvláštních osobních údajů, které jsou mnohem citlivější, jejich zpracování představuje větší zásah do soukromí dané osoby a je potřeba jim věnovat zvýšenou ochranu. Přesný výčet zvláštních kategorií osobních údajů je uveden v článku 9 GDPR. Tuto oblast Janečková (2020, s. 43-49) završuje vyjádřením k odvětví školství, kde dochází ke zpracování velkého množství osobních údajů žáků, zákonných zástupců, zaměstnanců i dalších osob, avšak jak je upozorněno, mnoho údajů podléhá zpracování na základě školského zákona, zákona č. 561/2004 Sb.

Janečková (2020, s. 53-56) vysvětluje, že bez ohledu na právní formu je správcem osobních údajů každý subjekt, který určuje účel a prostředky zpracování osobních údajů. V tomto ohledu Nonnemann (2018, s. 28) zmiňuje například zaměstnavatele, kteří jsou správci osobních údajů svých zaměstnanců za účely stanovenými pracovněprávními předpisy, dále popisuje dvě možnosti, a to že správce sám rozhodne o tom, zda bude osobní údaje zpracovávat, nebo mu to uloží zvláštní zákon, jak vyplývá z již uvedeného příkladu se zaměstnavateli. Janečková (2020, s. 53-56) doplňuje, že školy představují správce, kteří budou vždy určeny zákonem, dále upozorňuje, že zpracování osobních údajů provádí správce sám, nebo může využít zpracovatele. Richter (2021) využívá pro zpracovatele jednoduchou definici a to, že se jedná o subjekt, který zpracovává pro správce osobní údaje. Za typické zpracovatele Nonnemann (2018, s. 29) považuje externí archiv, externí mzdové účetní či bezpečnostní agenturu. Podobně Nezmar (2017, s. 113-117) popisuje, že zpracovatel se od správce liší tím, že provádí pouze takové operace, kterými byl od správce pověřen. V souvislosti s problematikou GDPR se užívá další významný pojem, a to subjekt údajů. Frýbová a kol. (2019, s. 16) komentují, že subjektem údajů není právnická, ale výhradně fyzická osoba, k níž se vztahují osobní údaje, a v případě škol se jedná o žáky, zákonné zástupce nebo zaměstnance. Janečková (2020, s. 69-73) k pojmu

subjektu údajů dodává, že i osobní údaje fyzických osob podnikajících jsou považovány za údaje spadající pod ochranu GDPR.

Zpracování osobních údajů Janečková (2020, s. 70-76) komentuje jako operaci, činnost nebo soubor operací, kterou správce s osobními údaji provádí s jasným účelem a systematicky, pod tento pojem řadí tyto operace s osobními údaji: shromáždění, zaznamenání, uložení, vyhledání, uspořádání, šíření, nahlédnutí, použití, zkombinování, seřazení, omezení, výmaz i jejich zničení. Stejný zdroj dodává, že zpracování osobních údajů končí v momentě, kdy dané osobní údaje přestávají existovat. Porušení zabezpečení osobních údajů Nonnemann (2018, s. 136) vysvětluje jako porušení zabezpečení, jehož následkem je náhodné nebo protiprávní zničení, změna, ztráta nebo neoprávněné poskytnutí či zpřístupnění uložených nebo jinými způsoby zpracovávaných osobních údajů. V souvislosti s touto definicí se věnuje Janečková (2020, s. 77-83) detailnímu rozboru pojmů protiprávní a neoprávněné zpracování a specifikuje je jako zpřístupnění osobních údajů příjemcům, kteří nemají právo na přístup nebo jinou formu zpracování těchto údajů. Stejný zdroj vyzdvihuje několik typů, které považuje za nejčastější porušení zabezpečení osobních údajů ve školských zařízeních a mezi ně řadí ztrátu a odcizení dokumentů, zaslání osobních údajů v emailové komunikaci nebo jejich zpřístupnění prostřednictvím dopisu dalším třetím osobám či neoprávněný přístup osoby do databází.

Fialová a kol. (2020, s. 11) připomíná, že EU vytvořila veřejnoprávní systém ochrany osobních údajů na základě Směrnice Evropského parlamentu a rady č. 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volným pohybem těchto údajů (dále jen „Směrnice č. 95/46/ES), tímto EU reagovala na rozsáhlé množství generovaných dat o jednotlivých osobách, kdy jedinci často neměli ani možnost zjistit strukturu a rozsah informací, které jsou o nich zpracovávány. Janečková (2020, s. 19-24) v souvislosti s uvedenou Směrnicí č. 95/46/ES doplňuje, že tato právní úprava předcházela GDPR a členské státy měly tuto směrnici promítnout do svých právních řádů, v ČR se této problematice věnoval zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, avšak tento zákon byl zrušen a postupně došlo k jeho nahrazení zákonem č. 110/2019 Sb., o zpracování osobních údajů, který již v souladu s GDPR specifikuje některé oblasti. Předchozí legislativa, jak upozorňuje Nonnemann (2018, s. 12-13), nedokázala pojmout současný vývoj technologií a představovala roztříštěnost právních úprav v rámci jednotlivých členských států EU, přičemž GDPR právní úpravu sjednocuje a lze implementovat na jakékoliv zpracování osobních údajů bez ohledu na příslušnou technologii. GDPR nepředstavuje jediný dokument, který se vztahuje k ochraně a bezpečnosti osobních údajů, to naznačuje již zmiňovaný zákon č. 110/2019 Sb., o zpracování osobních údajů, nebo zákon č. 89/2012 Sb., občanský zákoník, kde § 84 - § 90 se věnují podobě člověka a soukromí včetně uvedení výjimek. Janečková (2020, s. 22-24) dále poukazuje na novelu zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, která se dotýká i škol a školských zařízení.

Jak uvádí Janečková (2020, s. 946-949) dozor nad dodržování GDPR v České republice vykonává ÚOOÚ a Nonnemann (2018, s. 113) upozorňuje na drakonické sankce, kterým jsou organizace vystaveny. Za klíčovou kompetenci v tomto ohledu Nezmar (2017, s. 5-9) považuje znalost dodržení předpisů GDPR včetně praktického aplikování nařízení za přijatelných cenových podmínek. Článek 58 GDPR popisuje nápravné pravomoci dozorového úřadu, mezi kterými je zařazeno mimo správní pokuty i upozornění na porušení nařízení či udělení napomenutí, nemusí se tedy vždy jednat o udělení sankcí. Janečková (2020, s. 971-974) výši sankcí také označuje za příliš vysokou, avšak poukazuje na článek 83 GDPR, dle kterého si členské státy mohou stanovit pravidla pro ukládání správních pokut orgánům veřejné moci a veřejným subjektům. K tomu se vztahuje v rámci ČR § 62 zákon č. 110/2019 Sb., o zpracování osobních údajů, který uvádí, že bude upuštěno od udělení sankcí orgánům veřejné moci a veřejným subjektům, a v tomto ohledu MŠMT (2017) doplňuje, že tímto orgánem může

být škola, ačkoli upuštění od pokuty neznamená, že nedošlo k porušení práv nebo porušení jiného právního předpisu.

2.1.2 Povinnosti správců údajů

Jak uvádí Janečková (2020, s. 87-89), Frýbová a kol. (2019, s. 5) i Nezmar (2017, s. 211-215) organizace mají spravovat osobní údaje podle zásad ochrany osobních údajů a soubor těchto zásad je stanoven GDPR. Frýbová a kol. (2019, s. 5) komentuje, že celé GDPR podléhá těmto zásadám, jenž představují nejvýznamnější povinnosti, které udávají správcům, jak zpracovávat osobní údaje. Důležitý význam těmto zásadách přiklání i Nonnemann (2018, s. 31), který považuje za nezbytné, aby pověřenec pro ochranu osobních údajů se v těchto pravidlech uměl orientovat a podle toho poskytovat potřebné poradenství správci a zpracovateli osobních údajů. Janečková (2020, s. 87-134) blíže představuje hlavní zásady, které při zpracování osobních údajů jsou správci i zpracovatelé povinni respektovat a těmito zásadami jsou: zákonnost a transparentnost zpracování, minimalizace údajů, účelové omezení, přesnost a omezení uložení údajů, bezpečnost a integrita dat, doložitelná odpovědnost za soulad s GDPR. Výčet těchto zásad uvádí v podobném znění i Nezmar (2017, s. 211-215) avšak oproti Janečkové (2020, s. 87-134) navíc uvádí i povinnost prokazování a mezinárodní transfery. Jednotlivé zásady budou blíže rozebrány.

Zásada: Zákonnost, korektnost, transparentnost

Janečková (2020, s. 87-94) popisuje, aby bylo možné zpracovávat osobní údaje, je správce povinnen nalézt alespoň jeden z níže uvedených důvodů a tyto důvody musí být specifické, transparentní a korektní. Těmito důvody, resp. podmínkami jsou:

- udělení souhlasu se zpracováním osobních údajů;
- zpracování je nezbytné pro splnění smluvního závazku;
- zpracování je nezbytné pro zpracování právní povinnosti;
- zpracování je nezbytné pro ochranu životně důležitých zájmů;
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce.

V případě nenalezení zákonného důvodu nebo jeho pominutí je podle Janečkové (2020, s. 87-91) správce povinen tyto osobní údaje zlikvidovat. Nonnemann (2018, s. 32) upozorňuje, že v případě nedoložení existence právního důvodu ke zpracování je považováno toto zpracování od začátku za nelegální a správci může být nařízena likvidace všech souvisejících uložených a zpracovaných osobních údajů. Naproti tomu se vyjadřuje Nezmar (2017, s. 234-235), pokud zpracování odpovídá tomu, co subjekt údajů odsouhlasil, lze to považovat za transparentní, a korektnost vystihuje popis zpracování, které subjekt údajů odsouhlasil. Nezmar (2017, s. 229-233) dále uvádí, že správce údajů musí informovat subjekt údajů o tom, jaké informace jsou o něm zpracovávány a toto informování musí být předáno jasným, srozumitelným a jednoduchým jazykem. S tím souhlasí Voigt, Bussche (2017, s. 88) a dodávají i možnost využití vizualizace v případě potřeby, dále doplňují, že informace mohou být předávány v elektronické podobě v rámci webových stránek. Nezmar (2017, s. 229-233) poukazuje také na nutnost, informovat subjekt údajů ještě před shromažďováním osobních údajů nebo před případnými následnými změnami, a tímto informováním je zajištěno transparentnosti.

Ač se může zdát souhlas se zpracováním osobních údajů jednoznačný, zahrnuje mnoho specifických podmínek. Janečková (2020, s. 74-79) definuje souhlas jako svobodný, informovaný, konkrétní a jednoznačný projev vůle, kterým subjekt údajů dává svolení se zpracováním svých osobních údajů a zároveň upozorňuje, že mlčení, nečinnost nebo předem

zaškrtnuté políčko jako vyjádření souhlasu nestačí. Nonnemann (2018, s. 32-33) souhlas popisuje zejména po praktické stránce a uvádí, že není možné například poskytnutí další služby podmiňovat souhlasem se zpracováním osobních údajů pro další účely z hlediska marketingu, subjekt údajů musí sám aktivně údaje poskytnout a při udělení souhlasu musí být informován o tom, za jakým účelem, jakému správci a k jakým údajům dává souhlas. Jak komentují Frýbová a kol. (2019, s. 22) souhlas je kdykoliv odvolatelný, jeho odvolání musí být stejně jednoduché, jako jeho udělení a odvolání souhlasu znamená, že musí dojít k vyhledání a likvidaci všech osobních údajů, které byly na základě uděleného souhlasu zpracovávány. Melotíková (2020, s. 101) upozorňuje na zásadní problémy v otázce udělování souhlasů v rámci škol a v tomto ohledu i Frýbová a kol. (2019, s. 20) poukazují na skutečnost, že školy by měly využívat souhlas se zpracováním osobních údajů pouze tehdy, pokud nemohou využít jiný právní důvod. Také Denley a kol. (2019) doporučuje mít jiný právní základ pro zpracování osobních údajů než souhlas, společnosti by jej měly využívat jako poslední možnost, ačkoli připouští, že v některých případech je potřeba vyžádat udělení souhlasu. MŠMT (2017) přímo uvádí chybné příklady, kdy školy nadbytečně vyžadují souhlas, a těmito situacemi mohou být případy vyžadování souhlasu pro zveřejnění prací žáků v prostorách školy či zveřejnění jména a příjmení žáků účastnících se za školu soutěží. Na tuto problematiku poukazuje i Gembalová (2019), která informuje o závažnénm porušování GDPR v podobě nadbytečného vyžadování souhlasů se zpracováním osobních údajů, které se často děje ze strany škol, a školám doporučuje pravidelně přezkoumávat, za jakými účely osobní údaje zpracovávají a nezapomínat na posouzení, zda mezi školou a žákem nevzniká smlouva, na základě které dochází k právním důvodům zpracování. Podle stejného zdroje se smlouva může vztahovat například na předplatné stravného, družin, přihlašování na akce školy, poskytnutí přístupu do elektronické žákovské knížky i doložení potvrzení o bezinfekčnosti. ÚOOÚ (2019) uvádí, že běžným důvodem pro zpracování osobních údajů ve školství může být plnění smlouvy i plnění veřejného zájmu a ve svém upozornění se dotýká souhlasů, které se vztahují k dětem, respektive k jejich zákonnným zástupcům. V případě osobních údajů dětí článek 8 GDPR obsahuje podmínky týkající se souhlasu dítěte, je-li dítě mladší 16 let, musí souhlas vyjádřit nebo schválit zákonná osoba dítěte. Avšak stejný zdroj sděluje, že členské státy mohou pro uvedené účely tuto věkovou hranici snížit právním předpisem. V ČR je tato věková hranice snížena na 15 let, jak popisuje § 7 zákona č. 110/2019 Sb. zákon o zpracování osobních údajů, avšak vztahuje se pouze k nabídce služeb informační společnosti. K této problematice se vyjadřuje i Janečková (2020, s. 391-399) a podle ní nezletilí mladší 15 let nejsou způsobilí k udělení souhlasu, ten za ně musí poskytnout zákonný zástupce, zároveň odkazuje na ÚOOÚ a jeho přesvědčení, že žáci jsou od 15 let věku po řádném poučení schopni sami posoudit, zda chtějí škole udělit souhlas, aby mohly být jejich osobní údaje dále zpracovávány, přičemž by škola měla získávat souhlasy přímo od těchto žáků, avšak s informováním zákonných zástupců o zpracování takových údajů. V souvislosti s tím Melotíková (2020, s. 112) odkazuje na praxi škol, kdy s daným zpracováním osobních údajů souhlasí dítě, ale nesouhlasí s ním zákonný zástupce dítěte, v tomto případě je doporučováno najít shodu mezi dítětem a zákonným zástupcem, případně musí být vytvořen záznam o celé situaci. Stejný zdroj také klade důraz na srozumitelnou formulaci souhlasu, tak aby pro dítě bylo pochopitelné, čemu dává svůj souhlas.

Zásada: Účelové omezení

Janečková (2020, s. 111-113) i Voigt, Bussche (2017, s. 88-89) upozorňují, že zpracování osobních údajů může probíhat pouze za účelem, za kterým byly tyto údaje nasbírány a zpracování může probíhat pouze prostředky a způsoby, které jsou slučitelné s těmito účely. Nezmar (2017, s. 249-253) tuto zásadu přibližuje slovy, že od samého začátku musí být zřejmé, proč jsou údaje shromažďovány a jak s nimi bude nakládáno. Voigt, Bussche (2017, s. 88-89)

navíc v účelu zpracování vidí důležitou roli pro správce, neboť je nápomocen při určení dodržování zásad minimalizace, uložení i přesnosti údajů. Rozšířením či změnou účelu zpracování se zabývá Frýbová a kol. (2019, s. 7-8) i Nezmar (2017, s. 258-260) a poukazují na povinnost správce zohlednit, zda zpracování osobních údajů pro jiný účel je slučitelné s účely, pro které byly údaje původně shromážděny.

Zásada: Minimalizace údajů

Zásada minimalizace údajů navazuje na stanovení účelu a jak Janečková (2020, s. 114-116) i Voigt, Bussche (2017, s. 90) popisují, zpracování musí být relevantní, přiměřené a omezené pouze na nutný rozsah ke stanovenému účelu. Toto tvrzení potvrzuje Frýbová a kol. (2019, s. 8) i Nonnemann (2018, s. 42) a shodně doplňují, že správce musí být schopen prokázat proč pro daný účel zpracování potřebuje právě tyto shromažďované údaje. Jak dodává Frýbová a kol. (2019, s. 8) během zpracování může docházet ke změně potřebného rozsahu údajů, je tak důležité pravidelně přezkoumávat dané aspekty a nezpracovávat údaje, které již nejsou potřebné. Nezmar (2017, s. 297-305) tuto zásadu shrnuje tak, že správce by měl mít tolik informací, kolik potřebuje ke správnému naplnění cíle, ale ne více, navíc upozorňuje na citlivé osobní údaje, u kterých by obzvlášť mělo být uchováváno nebo shromažďováno pouze minimální množství potřebných informací.

Zásada: Přesnost údajů

Janečková (2020, s. 122-125) popisuje, že osobní údaje, které jsou zpracovávány musí být přesné a podle potřeby aktualizované, pakliže budou zpracovávány či shromaždovány nepřesné osobní údaje, je požadována jejich bezodkladná oprava či výmaz. V souvislostis s tím Frýbová a kol. (2019, s. 9) komentují, že musí být přijata veškerá rozumná opatření, aby údaje, které nejsou přesné, byly opraveny nebo vymazány a podobně jako Janečková (2020, s. 122-125) připouští, že správce by měl v přijatelné míře ověřovat přesnost údajů i v průběhu zpracování osobních údajů. Podle Nezmara (2017, 309-312) GDPR uznává, že tato zásada nemusí být praktický proveditelná, neboť kontrola správnosti všech položek osobních údajů, které organizace zpracovává nemusí být realizovatelná, a uvádí několik bodů, které má správce pro naplnění této zásady uskutečňovat a těmi jsou: realizace přiměřených kroků k zajištění přesnosti zpracováváných osobních údajů, zajištění jasného a nezpochybnitelného zdroje osobních údajů, důkladné zvážení vzniklých nejasností a problémů týkajících se přesnosti údajů, posouzení nutnosti a četnosti aktualizace informací. Nezmar (2017, s. 309-312) dále doplňuje, že GDPR jako nepřesné osobní údaje vnímá ty, které jsou zavádějící nebo nesprávné.

Zásada: Omezení uložení údajů

Janečková (2020, s. 126-128) uvádí, že správce může uchovávat osobní údaje pouze po dobu, po kterou trvá právní vztah, daná povinnost nebo po dobu trvání účelu, pro který jsou osobní údaje zpracovávány. Podobně tuto zásadu shrnuje Nezmar (2017, s. 332-342) a to tak, že osobní údaje nemají být uchovovány déle, než je to nezbytné, a upřesňuje, co tento princip znamená pro správce v praxi, a uvádí výčet několika povinností, podle toho organizace musí: kontrolovat dobu uchování osobních údajů, posuzovat účely, zajistit bezpečnou likvidaci či odstranění údajů, které již pro tyto účely nejsou potřebné, zajistit aktualizaci, archivaci nebo bezpečné smazání zastaralých informací. Dále Nezmar (2017, s. 335-342) doplňuje, že příliš brzké vyřazení potřebných údajů nebo naopak uchovávání osobních údajů po příliš dlouhou dobu má svá úskalí. Frýbová a kol. (2019, s. 9-10) upozorňují, že v případě nevyužití některé z podmínek, která dává možnost uchovávat údaje po delší dobu, než je nezbytné, musí dojít ke smazání nebo anonymizaci těchto údajů. K odstranění informací po uplynutí nezbytné doby se vyjadřuje i Nonnemann (2018, s. 43), který dodává, že anonymizace nebo smazání osobních údajů musí proběhnout ve všech systémech, ve kterých jsou zpracovávány, i v případné papírové evidenci. A jak poukazuje Janečková (2020, s. 126-128), v prostředí škol této zásadě

často dopomáhají spisové a skartační řády, případně je správce povinnen uchovávací dobu sám určit a za tuto stanovenou dobu nese odpovědnost.

Zásada: Bezpečnost údajů

K této zásadě Janečková (2020, s. 131-133) upozorňuje na nutnost zabezpečení osobních údajů před hrozbami uvnitř organizace i mimo ni a dodává, že zabezpečení se týká papírového i automatizovaného zpracování. Melotíková (2020, s. 104) odkazuje v souvislosti s vývojem techniky zejména na využívaní tzv. cloudových služeb, kdy správce je povinen zajistit dostatečnou úroveň ochrany osobních údajů. Na základě GDPR Frýbová a kol. (2019, s. 11) uvádí, že správce i zpracovatel mají zajistit s ohledem na účel zpracování, potencionální rizika i náklady vhodná organizační a technická opatření. Podobně i Nezmar (2017, s. 390-399) konstatuje dodržení souladu s tímto principem, a to tak, že bezpečnost v organizacích by měla být zajištěna tak, aby odpovídala povaze zpracovávaných osobních údajů, případně by mělo být zajištěno zabránění škodám nebo jejich minimalizaci v případě porušení bezpečnosti, dále by měla být stanovena osoba zodpovědná za zajištění bezpečnosti informací, dostatečné fyzické i technické zabezpečení by mělo být podpořeno kvalitně zpracovanými procesy a postupy včetně proškoleného personálu, organizace by měla být schopna rychle a efektivně reagovat na jakékoliv narušení bezpečnosti. Naproti tomu Nonnemann (2018, s. 44) vyzdvihuje zejména skutečnost, že GDPR neukládá povinnost organizacím ve využívání konkrétních opatření, které by musely zavádět. Ač Nezmar (2017, s. 406-420) považuje fyzické a technické zajištění bezpečnosti jako základ, nepředpokládá, že bude dostatečné, proto uvádí i další výčet opatření, kterým by organizace měly věnovat svou pozornost, mezi tato opatření zařazuje: zaměření na zvyšování povědomí o ochraně osobních údajů a budování firemní kultury v rámci bezpečnosti, pověření osoby odpovědné za vhodná bezpečností opatření, zajištění nejen základních školení o ochraně a zpracování osobních údajů, ale i průběžné kontinuální vzdělávání. Nezmar (2017, s. 406-428) také upozorňuje na nutnost zahrnutí do fyzické bezpečnosti i například kamerový systém, dohled nad pohybem návštěvníků, vstupní systém v podobě čipů, způsob nakládání s přenosnými zařízeními nebo likvidace papírového odpadu z kanceláří. Co se týče kybernetické bezpečnosti, stejný zdroj upozorňuje na: instalaci firewallu a antivirové kontroly, přijímaní automatických bezpečnostních aktualizací, nastavení heslové politiky, zálohování a šifrování elektronických informací, odstraňování uložených elektronických osobních údajů před likvidací a vyřazením počítačových technologií či intalaci nástroje proti spywaru. Na to, že ne vždy je dbáno na dostatečné zajištění bezpečnosti údajů odkazuje i ÚOOÚ (2020) ve svém vyjádření o porušování zabezpečení osobních údajů ze strany správců a dodává, že mnohdy není kladen důraz na heslovou politiku a hodnocení zabezpečení přístupů do interních systémů. Janečková (2020, s. 798-807) se zaměřuje spíše na zpracování osobních údajů zaměstnanci a doplňuje Nezmara (2017, s. 406-420) o k tomu příslušná opatření, uvádí například dostatek uzamykatelných prostor pro uložení dokumentů s osobními údaji, pravidlo „prázdného stolu“, kdy po odchodu ze zaměstnání jsou všechny dokumenty s osobními údaji uloženy v uzamykatelných skříních, vytvoření bezpečnostní dokumentace, se kterou budou zaměstnanci seznámeni, poučeni o jejich odpovědnosti, a která bude zdůrazňovat využívání informací výhradně k pracovním úkolům a upozorňovat zaměstnance na mlčenlivost o všech informacích, se kterými se seznámí v souvislosti s pracovní činností. Stejně jako Nezmar (2017, s. 422-428) i Janečková (2020, s. 798-807) se vyjadřuje ke kybernetické bezpečnosti a doplňuje některá opatření: před opuštěním výpočetní techniky dochází k odhlášení nebo uzamčení pracovní plochy, výpočetní technika je využívána pouze k pracovním činnostem a nejsou používány soukromé datové nosiče.

Zásada: Odpovědnost správce

Jak popisuje Frýbová a kol. (2019, s. 11), správce musí být schopen doložit, že dodržuje výše uvedené zásady a zpracování je prováděno v souladu s GDPR. Stejně tak Nezmar (2017,

s. 445-456) poukazuje na splnění stanovených zásad a shrnuje, že organizace musí prokázat skutečné plnění toho, co má teoreticky uvedeno v papírových pravidlech, jinak řečeno musí dokázat, že principy jsou začleněny do činnosti organizace. Nonnemann (2018, s. 47) přímo uvádí několik nástrojů, které slouží k dokládání souladu zpracování s požadavky a mezi tyto nástroje zařazuje: záznamy o činnostech zpracování, ověření a posouzení zpracovatele osobních údajů, náležitosti zpracovatelské smlouvy, Privacy by Design a Privacy by Default, DPIA, pravidla ohlašování případů porušení zabezpečení osobních údajů, stanovení pověřence pro ochranu osobních údajů a přihlášení ke kodexům a certifikátům. Naproti tomu Nezmar (2017, s. 453-456) v tomto ohledu zmiňuje dokumentaci týkající se například řízení rolí a odpovědností, školení a zvyšování povědomí, správy záznamů nebo řízení rizik.

Přestože jsou zásady zmiňovány v mnoha zdrojích, jejich výklad zůstává ve své hlavní podstatě shodný. Některé uváděné zdroje již naznačily, že na stanovené zásady navazují další povinnosti z toho vyplývající pro správce osobních údajů, ty však nejsou jednoznačně vymezeny. Například Nonnemann (2018, s. 63-109) uvádí výčet obecných povinností, které přináší GDPR a těmi jsou: záznamy o činnostech zpracování, ověřování zpracovatelů a zpracovatelská smlouva, záruky předávání údajů do zahraničí, záměrná a standardní ochrana osobních údajů, posouzení vlivu na ochranu osobních údajů, předchozí konzultace, řízení bezpečnostních incidentů, stanovení pověřence pro ochranu osobních údajů, kodexy a certifikáty. Nezmar (2017, s. 101) přistupuje k novým povinnostem obecněji a ač jeho výčet není tak rozsáhlý jako Nonnemanna (2018, s. 63-109), dodává, že s výjimkou záznamů o činnostech zpracování jsou ostatní povinnosti vázány na přítomnost rizika, tj. nemusí být povinné pro každého správce. Melotíková (2020, s. 101) se věnuje přímo GDPR ve školství a mezi povinnosti pro ně plynoucí zařazuje: zmapování procesů zpracovávajících osobní údaje v rámci školy, tzv. příprava pro záznamy o činnostech, kontrola smluv se zpracovateli, nastavení vnitřních procesů pro zacházení s osobními údaji, stanovení pověřence pro ochranu osobních údajů a informování o zpracování osobních údajů zvěřejněné na webových stránkách škol. Podobně Lock (2018) se zaměřuje na GDPR ve školách a oproti Melotíkové (2020, s. 101) vyzdvihuje zejména školení zaměstnanců. Vybrané povinnosti budou blíže specifikovány.

Záznamy o činnostech zpracování

Záznamy o činnostech zpracování osobních údajů podle Janečkové (2020, s. 400-402) představují podrobný popis zpracovávání údajů u daného správce nebo zpracovatele, jejich forma není stanovena, avšak evidence záznamů slouží k doložení souladu s GDPR. Frýbová a kol. (2019, s. 25) jednoznačně uvádějí, že školy mají povinnost vést záznamy o činnostech zpracování a minimální rozsah uváděných údajů představují: kontaktní údaje správce, údaje pověřence, účel zpracování, popis činnosti, kategorie subjektů údajů, popis kategorií osobních údajů, kategorie příjemců, předávání osobních údajů do třetích zemí, plánovaná lhůta pro výmaz osobních údajů, popis technických a organizačních bezpečnostních opatření. Jak dodává Janečková (2020, s. 403-407) záznamy mohou být rozšířeny i o další informace, a těmi může být například právní základ jednotlivých zpracování.

Ověření zpracovatele a zpracovatelská smlouva

Na základě GDPR Frýbová a kol. (2019, s. 51) uvádí, že zpracovatel by měl poskytovat dostatečné záruky zavedení vhodných organizačních a technických opatření na zpracování osobních údajů v souladu s GDPR. Podle Nonnemanna (2018, s. 68) disponuje správce možností přenést zpracování osobních údajů na dodavatele či zpracovatele a stejně jak uvádí Frýbová a kol. (2021, s. 51) dodává, že je v takovém případě správce povinen posoudit důvěryhodnost konkrétního zpracovatele. Nonnemann (2018, s. 68-69) doplňuje výběr nástrojů, které lze pro posuzování dodavatelů použít a těmito nástroji může být: ověření identity, majetkové struktury a délky existence zpracovatele, zjištění veřejně dostupných informací

i ověření existence negativních informací, certifikace zpracovatele v oblasti bezpečnosti dat, zpracovatel se hlásí k některému kodexu chování, spolupracuje při svém ověření, poskytuje správci veškerou potřebnou součinnost a nebrání se smluvnímu závazku k plnění všech povinností stanovených GDPR. V této souvislosti Nezmar (2017, s. 436-440) upozorňuje na skutečnost, že správce nese plnou odpovědnost za operace s osobními údaji provedené zpracovatelem a stejně jako Nonnemann (2018, s. 68) dodává, že správce v těchto případech musí vybrat zpracovatele poskytujícího dostatečné záruky v oblasti ochrany osobních údajů, zpracovatel musí přijmout přiměřená opatření a musí existovat smlouva mezi správcem a zpracovatelem o zpracování osobních údajů. Janečková (2020, s. 734-736) se shoduje s oběma autory a dodává, pokud bude prokázáno jasné pochybení na straně zpracovatele, může být i přesto správce konfrontován za zvolení zpracovatele bez dostatečných záruk.

Melotíková (2020, s. 102-103) poukazuje na povinnost škol související s implementací GDPR, aby byla z jejich strany zajištěna kontrola zpracovatelských smluv a tyto smlouvy by měly obsahovat následující ustanovení:

- zpracovatel zpracovává osobní údaje pouze na základě pokynů správce a zároveň přijímá veškerá příslušná opatření;
- zpracovatel zajistí mlčenlivost oprávněných osob zpracovávajících osobní údaje a zapojení dalších osob může proběhnout pouze po písemném souhlasu správce;
- zpracovatel poskytuje součinnost správci v případech reagování na žádosti subjektů údajů či v ohlašování případů porušení zabezpeční osobních údajů;
- zpracovatel umožňuje realizovat správci a příslušným orgánům kontroly, audity, zpracovávaných osobních údajů;
- zpracovatel by měl ve stanovené lhůtě poskytnout správci součinnost, aby správce splnil zákonné povinnosti související se zpracováním osobních údajů, s jejich ochranou a plněním smlouvy.

K tomuto výčtu Frýbová a kol. (2019, s. 51-52) navíc zmiňuje ustanovení, že zpracovatel po ukončení zpracování osobních údajů vrátí správci všechny osobní údaje nebo provede jejich výmaz, a smlouva by měla obsahovat předmět, dobu trvání zpracování osobních údajů, povahu a účel, kategorií subjektů údajů a typ osobních údajů. Ke zpracovatelské smlouvě se vyjadřuje i Nonnemann (2018, s. 70), který poukazuje, že zpracovatelská smlouva nemusí představovat samostatný dokument, ale může mít podobu ujednání o zpracování osobních údajů, jenž je součástí hlavní smlouvy. Melotíková (2020, s. 103-104) i Nonnemann (2018, s. 72) doporučují v rámci smlouvy uvedení vhodných prostředků k zajištění závazků zpracovatele a Melotíková (2020, s. 103-104) konkrétně navrhuje finanční záruky, zástavní právo, smluvní pokuty, či právo na odstoupení od smlouvy. Delay a kol. (2019, s. 39-40) vybízí k auditování dodavatelů, resp. zpracovatelů osobních údajů za účelem ověření, že dostatečně chrání předávané osobní údaje. Dále stejný zdroj poukazuje na skutečnost, že správce by měl mít přehled o datech, které zpracovatelé zpracovávají, a to i z důvodu uplatnění některého z práv subjektů údajů, kdy bude muset být například zpracování konkrétních osobních údajů pozastaveno.

Hlášení porušení bezpečnosti osobních údajů

Jak popisuje Frýbová a kol. (2019, s. 41), správci jsou povinni ohlašovat ÚOOÚ jakékoliv porušení zabezpečení osobních údajů, které může přinášet rizika pro dotčené subjekty údajů. Zároveň by podle Frýbové a kol. (2019, s. 42) měly školy postupovat podle těchto kroků: zjištění, zda opravdu došlo k porušení zabezpečení osobních údajů, zjištění, zda z tohoto porušení vyplývají rizika pro práva a svobody subjektů údajů, ohlášení ÚOOÚ a informování subjektů údajů. Nonnemanna (2018, s. 84-87) odkazuje na skutečnost, že správci jsou mimo jiné povinni evidovat a vyhodnocovat případy porušení zabezpečení osobních údajů,

z toho vyplývá povinnost každý bezpečnostní incident posoudit a zvážit, jaká opatření je nezbytné přijmout pro vyloučení nebo alespoň omezení opakování daného případu. Nonnemann (2018, s. 84-87) zdůrazňuje uložení povinnosti všem, kteří mají přístup k osobním údajům, aby každý incident týkající se porušení zabezpečení osobních údajů byl hlášen a dále rozlišuje tři úrovně rizika od zanedbatelného až po vysoké riziko a doplňuje, že incidenty s nízkým až vysokým rizikem musí být oznámeny ÚOOÚ a toto oznámení musí proběhnout do 72 hodin od zjištění incidentu. Podobně se vyjadřuje i Nezmar (2017, s. 441-444), pokud dojde i přes nastavená bezpečnostní opatření k porušení zabezpečení dat, musí organizace příslušně reagovat a celý následný proces řídit, zároveň dodává, že jedním z možných příkladů organizačního bezpečnostního opatření je právě existence firemní zásady řešící situaci narušení bezpečnosti informací.

Pověřenec pro ochranu osobních údajů

Szalowski (2018) vnímá regulaci pozice pověřence z nařízení GDPR velmi neurčitě a nepřesně, pravomoci pověřence hodnotí jako nejednoznačně vymezené. Ačkoli Szalowski (2018) poukazuje na obecné znění ustanovení GDPR, není přesvědčen o nutnosti zavádění interních organizačních předpisů, které by upřesňovaly pravidla plnění funkce pověřence, a to z důvodu odlišné interpretace. Podle Frýbové a kol. (2019, s. 53) pověřenec usnadňuje organizacím dodržování souladu s GDPR a plní funkci zprostředkovatele mezi ÚOOÚ, subjekty údajů a správcem. Ne každá organizace má povinnost jmenovat pověřence pro ochranu osobních údajů, avšak Janečková (2020, s. 908-910), Melotíková (2020, s. 73) i Frýbová a kol. (2019, s. 53-54) shodně upozorňují, že na školy se tato povinnost vztahuje. Szalowski (2018) komentuje, že povinnost jmenovat pověřence plní zvlášť správce, zvlášť zpracovatel, nebo oba subjekty současně. Melotíková (2020, s. 75) vyzdvihuje, že pověřenec musí důkladně chápat GDPR a disponovat znalostmi v oblasti právních předpisů o ochraně osobních údajů, zároveň poukazuje, že se nemusí jednat o odborníka na bezpečnost a IT, stačí dostatečné povědomí o těchto oblastech a správce by měl v případě nutnosti pověřenci zajistit přítup k těmto odborníkům. Frýbová a kol. (2019, s. 57) poukazují, že požadavek na právní znalosti nebude splňovat mnoho zaměstnanců a v případě jmenování pověřence z jejich řad bude nutné zajistit dostatečné proškolení, zároveň ale vyzdvihují u zaměstnanců znalost procesů v jejich organizaci, jenž může představovat pro pověřence i samotnou organizaci výhodu. Ač Melotíková (2020, s. 75) uvádí, že úroveň odborných znalostí není na funkci pověřence přesně definována, upozorňuje Nonnemann (2018, s. 100-101) na odpovědnost správce i zpracovatele za splnění kvalifikačních požadavků jmenovaného pověřence, a doporučuje dokumentovat jakým způsobem byly kvalifikační předpoklady ověřeny, např. referencemi, osobním pohovorem nebo relevantním certifikátem. Přidělované certifikáty rozporuje Janečková (2020, s. 929-932) a upřesňuje, že ač mnoho subjektů nabízí kurzy pro pověřence zakončené certifikátem, GDPR nestanovuje certifikaci pověřence jako předpoklad k výkonu funkce, pověřenec tak nemusí disponovat certifikátem a jmenovaným pověřencem může být i necertifikovaná osoba, která má dostatečné právní povědomí o ochraně osobních údajů a GDPR. Frýbová a kol. (2019, s. 57) doporučují osobě na pozici pověřenec průběžně se vzdělávat v rámci seminářů, konferencí a pravidelně monitorovat webové stránky ÚOOÚ.

Melotíková (2020, s. 77-78) upozorňuje, že pověřenec musí být nezávislá osoba, jejíž pozice v rámci organizace není ve střetu zájmů a nedostává pokyny od vedení organizace. Vysoký důraz klade Melotíková (2020, s. 77) na zajištění správného postavení pověřence v organizaci, měl by být dostatečně a včas zapojen do záležitostí souvisejících s ochranou osobních údajů, být přítomen na schůzkách vedení, případné incidenty s ním musí být konzultovány, s jeho jmenováním musí být zaměstnanci obeznámeni a kompletní potřebné zdroje mu musí být poskytovány. V souvislosti s tím Frýbová a kol. (2019, s. 58) poukazují na hrozbu uložení pokuty v případě nezajištění náhledových přístupů pověřenci do školských informačních

systémů. S Melotíkovou (2020, s 77-78) je v plné shodě i Nonnemann (2018, s. 102-103). Naopak Frýbová a kol. (2019, s. 56) vidí problém v zajištění nezávilosti u pověřenců z řad zaměstnanců a upozorňuje, že ne každý zaměstnanec může tuto funkci zastávat. V případě pověřence, který je zaměstnancem Frýbová a kol. (2019, s. 56) poukazuje na nutnost podepsání doložky o zachování mlčenlivosti o všech osobních údajích a bezpečnostních opatření, o kterých se dozví v souvislosti s výkonem funkce, a podepsání, že u něj nedojde ke střetu zájmů. Melotíková (2020, s. 78) představuje úkoly pověřence, které jsou dány GDPR a mezi ně patří: poskytování informací a poradenství, monitoring souladu s GDPR a dalšími předpisy, na požádání poskytování právního poradenství, vydávání stanoviska k DPIA, spolupráce s dozorovým úřadem, působení jako kontaktní místo pro dozorový úřad a zachovávání mlčenlivosti. V souvislosti s tím Frýbová a kol. (2019, s. 60) poukazuje, že pověřenec by měl sám aktivně prověřovat soulad zpracování osobních údajů a sám by měl přicházet s doporučeními na změny. Nonnemann (2018, s 102-109) připouští, že GDPR formuluje úkoly svěřené pověřenci poměrně obecně a je na správci a zpracovatelích jaké další úkoly nebo povinnosti pověřenci uloží a pro zajištění jednotného přístupu ke zpracování osobních údajů doporučuje, aby pověřenec vykonával i další činnosti:

- evidenci všech konzultací poskytnutých vedení společnosti a všech posudků poskytnutných při posuzování vlivu nového zpracování na ochranu osobních údajů;
- evidenci stížností a uplatnění práv dotčených osob;
- evidenci komunikace s ÚOOÚ a dalšími orgány;
- evidenci historických i aktuálně používaných souhlasů se zpracováním osobních údajů a informačních memorand;
- evidenci seznamu interních předpisů, které se vztahují k pravidlům pro zpracování nebo zabezpečení osobních údajů.

Nonnemann (2018, s. 109) dále doplňuje, že pověřenec může posuzovat nahlášené případy porušení zabezpečení osobních údajů, oznamuje je ÚOOÚ a vede jejich evidenci, dále může být zapojen i do vzdělávání odpovědných zaměstnanců organizace, může připravovat školící materiály i školení sám provádět. Na rozdíl od Nonnemanna (2018, s. 108-109), který považuje školení zaměstnanců a přípravu materiálů nad rámec povinností pověřence, Frýbová a kol. (2019, s. 59-60) tuto skutečnost vidí opačně a podle nich je pověřenec povinnen aktivně informovat zaměstnance o jejich povinnostech a k předávání informací může využívat právě různá školení. Ke školení zaměstnanců se vyjadřuje i Zelena a kol. (2019), kdy v rámci školení doporučují zejména vysvětlit heslovou politiku, zabezpečování dokumentů v případě opouštění pracovního místa či jejich likvidaci. Také Lock (2018) klade důraz na školení zaměstnanců a považuje jej za klíčové, neboť nestačí mít pouze přijatelně nastavené postupy, ale tyto postupy musí být dodržovány a je potřebný odpovídající přístup k nim.

Vnitřní procesy a dokumentace

Podle Melotíkové (2020, s. 101) měly školy povinnost před nabytím účinnosti GDPR nastavit vnitřní procesy pro zacházení s osobními údaji v podobě přijetí směrnic nebo jejich revidováním o nakládání s osobními údaji. Janečková (2020, s. 851-854) přisuzuje vytvořené směrnici účel, kterým je doložení souladu s GDPR a dále jej vnímá jako podklad pro seznámení zaměstnanců s nastavenými pravidly. Součástí vnitřního předpisu podle Janečkové (2020, s. 851-854) mohou být obecná pravidla pro zpracování osobních údajů, pravidla bezpečnosti a postup při vyřizování žádostí subjektu údajů. V souvislosti s bezpečností a možnými incidenty doporučují i Denley a kol. (2019, s. 42-43) stanovit plán reakcí na incidenty, díky kterému budou zaměstnanci vědět, na koho se obrátit v případě porušení bezpečnosti osobních údajů. Stejný zdroj uvádí, pokud zaměstnanci vědí jak a komu nahlásit incident, je možné incident minimalizovat za předpokladu, že byl nahlášen rychle a efektivně.

2.1.3 Práva subjektu údajů

Jak uvádí Richter (2021) GDPR přispělo k tomu, že si i laičtí adresáti práva uvědomili, že mají právo na to, aby s jejich osobními údaji nebylo svévolně nakládáno, aby nebyly jejich osobní údaje libovolně zpracovávány a vyžadovány. Janečková (2020, s. 144-332) rozlišuje tato práva subjektů údajů: právo na informace, právo na přístup, právo na opravu a doplnění, právo na výmaz, právo na omezení zpracování, právo na přenositelnost, právo vznét námitku, právo nebýt předmětem automatizovaného zpracování a právo podat stížnost u dozorového úřadu. Nezmar (2017, s. 137-140) rozděluje práva subjektu údajů na pasivní a aktivní a toto rozlišení spočívá v tom, zda subjekt údajů musí vynaložit nějakou aktivitu pro uplatnění svého práva, mezi pasivní práva řadí právo být informován, kdy aktivitu musí vyvinout správce vůči subjektu údajů, aby mu dané informace poskytl, ostatní práva řadí mezi aktivní a tento výčet je shodný s výčtem práv podle Janečková (2020, s. 144-332) s výjimkou práva na podání stížnosti u dozorového úřadu. K výše zmíněným právům se vyjadřuje i Frýbová a kol. (2019, s. 34) a upozorňuje na právo udělit či odvolat souhlas se zpracováním osobních údajů. Toto právo však mezi samostatná práva neuvádí ani GDPR.

Právo na informace Janečková (2020, s. 143-155) představuje jako právo subjektu údajů být informován o tom, že jeho osobní údaje jsou zpracovávány a toto informování by mělo proběhnout v okamžiku shromáždění daných osobních údajů správcem a zároveň v přiměřené lhůtě v závislosti na okolnostech případu. Jak komentuje Nezmar (2017, s. 462-465), plnění této povinnosti probíhá nejčastěji prostřednictvím oznámení o ochraně osobních údajů a Janečková (2020, s. 143-155) v této souvislosti jako pomocný nástroj uvádí webové stránky, kde mohou být dané informace sděleny. Janečková (2020, s. 205-212) uvádí i výjimky, kdy není potřeba subjekt údajů informovat, a to zejména v případech, kdy zpřístupnění osobních údajů je stanoveno právními předpisy, když subjekt údajů dané informace již má nebo pokud by poskytnutí daných informací vyžadovalo neúměrné úsilí. Nonnemann (2018, s. 50-51) se také vyjadřuje k právu na informace, avšak v jeho podání se jedná o právo na poskytnutí informací, které jsou o subjektech údajů zpracovávány, a toto právo Janečková (2020, s. 255-259) a Nezmar (2017, s. 470-473) uvádějí jako právo na přístup. Přesný výčet informací, které jsou o subjektu údajů zpracovávány, a ke kterým má subjekt údajů právo získat přístup uvádí GDPR článek 15. Janečková (2020, s. 272-275) upozorňuje, že právo na opravu neznačí povinnost správce aktivně vyhledávat nepřesné údaje, avšak po obdržení žádosti by mělo okamžitě dojít k pozastavení zpracování daných osobních údajů, a to do doby ověření správnosti a případné opravy. Frýbová a kol. (2019, s. 35) doplňují, že toto právo v sobě zahrnuje také doplnění neúplných osobních údajů a dále poukazují na situaci, kdy se prokáže, že evidované osobní údaje jsou přesné, v takových případech nebude žádosti o opravu či doplnění vyhověno. Co se týče práva na výmaz, Janečková (2020, s. 287-293) vyzdvihuje, že nelze považovat za právo absolutní a GDPR článek 17 stanovuje přesné podmínky i výjimky, na základě kterých toto právo může být uplatněno nebo odmítnuto. Jak rozebírá Nezmar (2017, s. 485-488) i přesto, že je zpracování osobních údajů pozastaveno, správce smí osobní údaje ukládat, již je ale nesmí dále zpracovávat. S tím souhlasí i Nonnemann (2018, s. 58) a tento popis doplňuje o informaci, že omezení osobních údajů potrvá až do doby, než dojde k posouzení jejich přesnosti, převažujícímu zájmu nebo nemožnosti jejich další potřebě či využití ze strany subjektu údajů a dále shrnuje, že jakékoliv opravy, omezení zpracování, aktualizace i informace o výmazech osobních údajů musí být dále poskytnuty ostatním příjemcům těchto osobních údajů, kterým je správce zpřístupnil. Melotíková (2020, s. 72) toto právo uzavírá tak, že samotná problematika výmazu po technické stránce není nijak specifikována a nejčastěji dochází k anonymizaci osobních údajů u automatizovaně zpracovávaných dat. Samotné právo na omezení zpracování může subjekt údajů uplatnit podle Janečkové (2020, s. 297-301) v těchto případech: zpracování je protiprávní, byla vznesena

námitka proti zpracování, je popírána přesnost osobních údajů, správce nepotřebuje údaje pro dané účely, ale subjekt údajů je požaduje pro obhajobu právních nároků. Frýbová a kol. (2019, s. 37) představují toto právo za dočasné opatření, kdy musí následně dojít k upozornění subjektu údajů, že dochází ke zrušení omezení zpracování a osobní údaje budou vymazány nebo naopak opět zpracovávány. Nonnemann (2018, s. 60) poukazuje u práva na přenositelnost zejména na podmínky, za kterých je možné toto právo vyžadovat, a těmi je zpracování založené na souhlasu nebo na základě plnění smlouvy a prováděné automatizovaně. Nezmar (2017, s. 493-498) dodává, že správce není povinen vyhovět žádosti v případě, že doposud nevyužíval automatizovaný proces, ani není povinen jej na základě toho zavádět. V případě uplatnění práva na námitku, uvádí Janečková (2020, s. 317-322), že by mělo dojít k bezprostřednímu omezení zpracování daných osobních údajů a správce má povinnost prokázat oprávněnost důvodů pro zpracování. Za typickou situaci pro uplatnění tohoto práva považují Frýbová a kol. (2019, s. 39) když subjekt údajů nesouhlasí s pořizováním kamerového záznamu. V souvislosti s právem nebýt předmětem automatizovaného rozhodnutí Janečková (2020, s. 324-327) podotýká, pakliže konečný výsledek ovlivňuje člověk, nejedná se o automatizované rozhodnutí a dodává, že v rámci škol a školských zařízení není automatizované rozhodnutí využívano. Tuto definici potvrzují i Fialová a kol. (2020, s. 13), kteří uvádí, že rozhodnutí bývá realizováno specifickým softwarem výpočetního systému a na automatizovaném rozhodování se člověk a jeho vůle z podstatné části nepodílí. Janečková (2020, s. 328-336) se také zaobírá právem subjektu údajů na podání stížnosti u dozorového úřadu a uvádí, že podat stížnost mohou ti, kteří se domnívají, že zpracováním jejich osobních údajů je porušeno GDPR.

Je zřejmé, že i z práv subjektů údajů plynou společnostem, resp. správcům osobních údajů povinnosti, které musí zapracovat do svých procesů. A jak komentuje Janečková (2020, s. 140-146) i Nonnemann (2018, s. 48-49) správce by měl výkon práv subjektu údajů usnadňovat, měl by zajistit podmínky i pro elektronické podávání žádostí, za předpokladu dostatečných opatření k jednoznačné identifikaci osob uplatňujících práva, a pakliže má správce jmenovaného pověřence pro ochranu osobních údajů, musí sloužit jako kontaktní bod pro subjety údajů při uplatnění jejich práv, s tím souvisí i uvedení kontaktních údajů DPO (pověřenec pro ochranu osobních údajů) na webových stránkách zastupující společnosti. Stejné zdroje také uvádějí, že správce má na vyřízení žádosti 30 dnů od obdržení žádosti a v některých případech je možné tuto lhůtu prodloužit. Melotíková (2020, s. 67) vyzdvihuje, že správce musí poskytovat jasné a srozumitelné informace a ty předávat stručným způsobem. Janečková (2020, s. 144-146) pamatuje i na zaměstnance a doporučuje je všechny seznámit s těmito právy, aby bylo možné zajistit jejich správnou realizaci.

2.2 Integrace GDPR do procesního managementu

Povinnosti, které správcům osobních údajů stanovuje GDPR, musí být implementovány do procesů organizace, a k samotné implementaci je vhodné přistupovat pomocí projektu. Z tohoto důvodu jsou následující subkapitoly vyhrazeny nástrojům a technikám využívaným k implementaci GDPR a vhledu do procesního a projektového managementu, včetně nástrojů pro tvorbu projektu.

2.2.1 Nástroje implementace GDPR do procesního řízení vybrané organizace

Podle Nezmara (2020) by prvním krokem před implementací požadavků GDPR měla být vždy analýza rizik, resp. analýza procesů zpracování a vyplývajících rizik, která ukáže na nedostatky a hodnocení rizik by mělo být pravidelně opakováno. Stejný zdroj doporučuje se dívat na rizika z pohledu subjektu údajů. Ač GDPR přímo neukládá povinnost provést analýzu rizik, z článku 32 GDPR zřetelně vyplývá nutnost jejich posouzení. Melotíková (2020, s. 101) v tomto ohledu navrhuje zmapovat procesy, v kterých dochází ke zpracování osobních údajů. S tím souhlasí i MŠMT (2017), které doporučuje pravidelně prověřovat případy, kde dochází

ke zpracování osobních údajů, a to i mimo zákonem vymezenou dokumentaci a smlouvy s dodavateli. V souvislosti se zmapováním procesů zmiňuje Nezmar (2017, s. 533-554) GAP analýzu a jako následný krok vidí posouzení vlivu na ochranu osobních údajů a k těmto krokům detailněji rozvádí další postup. Níže uvedené techniky a nástroje představují ty, které jsou v souvislosti s GDPR stanoveny nebo doporučovány, jejich využití však mnohdy závisí na zpracovávaných osobních údajích a vyplývajícím riziku pro subjekty údajů.

Datový audit – GAP analýza

Jak komentuje Quinn (2021) audit shody nebo užívaný název GAP analýza dává podnikům jistotu, že dodržují nejlepší postupy, a dobře nastavená ochrana dat může zajistit úsporu času i finančních prostředků, kdy se zpracování dat stává efektivnější a správná implementace GDPR může eliminovat plýtvání zdrojů. Podle Nezmara (2017, s. 533-554) by GAP analýza měla přinést odpověď na to, co všechno a jak je potřeba změnit v organizaci a jejích procesech. Nezmar (2017, s. 533-554) také blíže popisuje jednotlivé kroky, které GAP analýze předchází, těmi jsou: identifikace uzlů sběru osobních údajů, identifikace jednotlivých zpracování pomocí dotazníku, analýza datových toků, identifikace souladu vstupních formulářů a smluvních vazeb, ověření bezpečnosti dat v listinné i digitální podobě včetně analýzy souvisejících směrnic a následně je možné přistoupit k sepsání GAP analýzy. Oproti tomu Matouš (2018) v rámci zmapování procesů prezentuje jednoduché zodpovězení základních otázek v podobě: kdo, co, proč, o kom, komu, kdy, jak a jako optimální výstup považuje přehled zpracovávaných osobních údajů, který zároveň bude podkladem pro záznamy o činnostech zpracování. Stejný zdroj dodává, že dále je nutné prověřit, zda jsou zpracovávané údaje ve shodě se stanovenými zásadami GDPR a u každého zpracování zhodnotit rizikovost a dle toho přijmout potřebná opatření. Zelena a kol. (2019) uvádějí konkrétní příklad GAP analýzy, která využívá jednoduché, avšak oproti Matouš (2018) již rozšířenější schéma otázek typu: kde jsou shromažďovány osobní údaje, kdo má přístup k osobním údajům, jaká je jejich struktura, obsah, jaké jsou závazky a smlouvy s třetími stranami, jaký je proces řízení incidentů apod. Na zhodnocení rizik odkazuje také Quinn (2021), podle které by první kroky analýzy měly směřovat k identifikaci rizik a následně k identifikaci mezer, poté by měl podnik vytvořit projektový plán. Závěrem Quinn (2021) upozorňuje, že identifikovaná rizika v GAP analýze budou vyžadovat vytvoření politik, které by měly být v rámci organizace začleněny pomocí standardů a postupů a zaměstnanci budou muset být v těchto oblastech proškoleni.

Posouzení vlivu na ochranu osobních údajů (DPIA)

Janečková (2020, s. 677-679) i Nezmar (2017, s. 549-554) popisují, že povinnost provádět posouzení vlivu na ochranu osobních údajů (dále jen „DPIA“) vzniká pouze tehdy, kdy je pravděpodobné, že zpracováním vznikne vysoké riziko pro práva a svobody fyzických osob. Podle článku 35 GDPR se DPIA bude vztahovat zejména při využívání nových technologií. Ač Janečková (2020, s. 683-687) uvádí mezi zpracování podléhající DPIA například systematické monitorování veřejně přístupných prostorů, tak Frýbová a kol. (2019, s. 72) se vyjadřuje, že zpravidla není nutné provádět DPIA v souvislosti s provozem kamerových systémů, tuto povinnost vidí pouze za předpokladu rozsáhlého a systematického monitorování veřejných prostor, avšak v prostředí škol tuto skutečnost hodnotí pouze za výjimečnou. Janečková (2020, s. 680-687) dále rozvádí, že v praxi DPIA představuje povinnost správce pravidelně vyhodnocovat rizika, která vznikají při činnostech zpracování, aby bylo možné stanovit, kdy hrozí pravděpodobnost vzniku vysokého rizika pro práva a svobody fyzických osob. V tomto případě Nonnemann (2018, s. 81-82) upozorňuje, že záleží na správci, do kolika kategorií bude rizika dělit a jak je bude hodnotit, avšak dozorový úřad si může při kontrole vyžádat zdůvodnění, proč bylo dané riziko ohodnoceno jako nízké nebo střední, a v případě zjevně nesprávné nebo zkreslené klasifikace rizika může být tato skutečnost vyhodnocena jako porušení GDPR. ÚOOÚ (2020) v rámci Metodiky obecného

posouzení vlivu na ochranu osobních údajů uvádí možný způsob provádění DPIA a tento způsob dělí na 4 etapy:

1. shromáždění informací o zpracování osobních údajů;
2. analýza, zda je nutné provést DPIA;
3. uskutečnění DPIA;
4. monitorování dodržování opatření a pravidelné revize.

Jak dále popisuje ÚOOÚ (2020), k určení, zda je nutné provést posouzení vlivu, slouží dokument seznamu druhů operací zpracování, které nepodléhají nebo naopak mohou podléhat posouzení vlivu. V souvislosti s tím Valentová (2023) doporučuje vždy provádět prvotní posouzení DPIA dle pokynů WP248, pro ověření, zda se na dané zpracování dané posouzení vztahuje. ÚOOÚ (2020) přináší detailní popis, jak postupovat při provádění DPIA, kde přímo rozvádí jednotlivé kroky. Podle Denley a kol. (2019, s. 67) by měl samotný proces DPIA popsat data, která přichází a odchází z organizace, identifikovat rizika a určit jejich řešení. Nonnemann (2018, s. 81-82) upozorňuje, že v případě identifikaci alespoň jednoho vysokého rizika, je správce povinen před zahájením plánovaného zpracování jej konzultovat s ÚOOÚ. V souvislosti s vyhodnocováním rizik Nezmar (2017, s. 721-728) upozorňuje na metodu PZH, která dané riziko vyhodnocuje s ohledem na pravděpodobnost vzniku, závažnost následku a názor hodnotitelů. Stejný zdroj dodává, že výsledné bodové rozpětí poukazuje na míru rizika a vyjadřuje naléhavost přijetí opatření k jeho snížení. Problematika GDPR je v neustálém vývoji, a tak dochází i k novým legislativním změnám, na které upozorňuje ÚOOÚ (2023), ten poukazuje na novou úpravu DPIA, která je účinná od 1.4.2023, podle té není nutné provádět posouzení, pokud již došlo k obecnému posouzení dopadů v rámci přijetí právního předpisu, tudíž tímto dochází pro správce osobních údajů k zjednodušenní provádění DPIA, zároveň je stanovena přesná struktura pro zpracování legislativního DPIA.

Balanční test

Valentová (2023) popisuje postup balančního testu, který se provádí v případech, kdy je právním titulem pro zpracování oprávněný zájem správce a je nutné jej provést před zahájením zpracování osobních údajů, v souvislosti s tím popisuje několik případů, které se řadí mezi oprávněné zájmy a jsou jimi například: zpracování osobních údajů pro účely standardního přímého marketingu, zpracování dat pro historické, statistické či vědecké účely nebo ochrana majetku, zdraví či bezpečnosti osob. Poslední bod potvrzuje a blíže rozvádí Evropský sbor pro ochranu osobních údajů v pokynech 03/2019 ke zpracování osobních údajů pomocí videotechniky v článku 3 bodech 19 a 20, kde uvádí, že účel ochrany majetku před krádeží, vloupáním nebo vandalismem, může představovat oprávněný zájem pro monitorování prostorů pomocí kamer, a upozorňuje, že doložené incidenty z minulosti mohou být přesvědčivým důkazem existence oprávněného zájmu. Frýbová a kol. (2019, s. 69-70) v tomto ohledu upozorňují na nezbytnou existenci očekávatelných či reálných rizik, pro která je nutná instalace kamerového systému, a u škol tato rizika mohou být doložena například rozhodnutím pořídit kamerový systém se záznamem jako reakce na stížnosti studentů ohledně ztrácejících se věcí ze šaten. V souvislosti s tím Hnilička (2022) odkazuje na provedení balančního testu při využití kamer ve školách a zároveň doporučuje vytvoření interních předpisů, které budou informovat o tom, po jakou dobu budou záznamy z kamer uchovávány a kdo k těmto záznamům bude mít přístup. Naopak Valentová (2023) v návaznosti na kamerové záznamy doporučuje vést evidenci každého nahlédnutí do záznamů, zároveň poukazuje na informační povinnost návštěvníků monitorovaných prostor a v souvislosti s tímto odkazuje na informační cedule, které obsahují upozornění, zda je kamerový systém se záznamem/bez záznamu, kdo je správcem, zpracovatelem, kontaktní osobou, jaký je účel, práva subjektů údajů, předávání třetím stranám, doba uchování, včetně odkázání na další zpřístupněné informace. Diskutovaným tématem je bezpochyby doba pro ukládání kamerových záznamů, například Frýbová a kol. (2019, s. 71)

doporučují uchovávat záznam po tři dny, tj. 72 hodin, kdy tato délka je obecně považována za přiměřenou. S tímto souhlasí i Valentová (2023), avšak dodává, že doba pro uchovávání záznamu může být i delší, pakliže má společnost dostatečně podložený důvod. Hnilička (2022) i Janečková (2020, s. 109-110) přibližují postup pro provedení balančního testu v případě kamerových záznamů a shodně uvádějí tyto body: stanovení účelu, posouzení záběru kamer, stanovení doby pro uchování záznamu a zabezpečení přístupu k záznamům. Hnilička (2022) navíc dodává vedení řádné dokumentace a označení monitorovaných prostorů.

Ač výše uvedené nástroje a techniky nemusí představovat pro správce povinnost, jejich dobrovolné využití může mít nejen pro společnost, ale i v případě kontroly ÚOOÚ pozitivní vliv, ostatně na jejich využití nad rámec povinností upozorňuje i Denley a kol. (2019, s. 67) a to zejména v případě provedení DPIA.

2.2.2 Přínos procesního řízení změn integrovaných s GDPR

Denley a kol. (2019, s. 43) vyzdvihují důležitost integrace GDPR do každodenních aktivit, pracovních postupů a obchodních i technologických změn v celé organizaci, pro zajištění stálého dodržování souladu s GDPR. Jurová a kol. (2016, s. 271-277) připouští, že v současné době je nutnost měnit zaváděné procesy a k tomu jsou nápomocny aktivity projektového charakteru, které slouží k zavádění změn. Procesy je možné rozdělit do tří kategorií na hlavní, řídící a podpůrné, jak rozdělují Švecová, Veber (2021, s. 1094-1103) a dodávají, pokud mají být procesy řízeny, musí být přesně zmapovány, jakmile dojde k vymezení klíčových procesů, je potřeba identifikovat jejich vnitřní strukturu, respektive činnosti, které je naplňují. Stejné základní dělení procesů rozlišují Jurová a kol. (2016, s. 282-290) a pro jejich vizualizaci odkazují na výběr z mnoha softwarových nástrojů, za nejčastěji využívaný prostředek zobrazující funkční schéma považují vývojový diagram. Podobně Švecová, Veber (2021, s. 1094-1103) doporučují pro identifikaci procesů a jejich struktury grafické znázornění na základě mapy procesů či vývojových diagramů. Dumas a kol. (2018, s. 3-4) se na proces zaměřují ve větším detailu a rozdělují ho na události a aktivity, kdy události mohou spustit sérii dalších aktivit. Stejný zdroj dodává, že proces zahrnuje také body rozhodnutí, které ovlivňují způsob provádění procesu a do procesů dále spadají aktéři, fyzické a informační objekty. S tím v souladu Jurová a kol. (2016, s. 278-290) dodávají, že procesní modely organizace se zpracovávají na několika úrovních složitosti, od hlavních procesů až po jednotlivé činnosti a závěrem upozorňují, že pracovníci jsou tak dobří, jak dobře jsou proškoleni, avšak jejich výkony závisí na dobrém nastavení procesů. Stejný zdroj využívá pro proces jednouduchou definicí a to, že proces je změna.

Dumas a kol. (2018, s. 21-22) rozlišují u implementace procesu 2 složky: automatizaci procesu a řízení organizační změny. Stejný zdroj tyto aktivity dále rozvádí a to tak, že je potřeba důkladné vysvětlení změn všem účastníkům procesu, vytvoření plánu pro řízení změn a školení nového způsobu práce včetně monitoringu změn za účelem hladkého přechodu na budoucí proces. A jak v podobné souvislosti uvádí Kotter (2015, s. 39-41), všechny prováděné transformační procesy spojuje poznatek, že realizace změny není snadná a rozlišuje proces změny o 8 krocích vztahujících se ke změně jakéhokoliv rozsahu, těmito kroky jsou: vyvolání vědomí naléhavosti, sestavení koalice schopné prosadit a realizovat změny, vytvoření vize a strategie, komunikace transformační vize, delegování v širokém měřítku, vytváření krátkodobých vítězství, využití výsledků a podpora dalších změn, zakotvení nových přístupů do firemní kultury. V návaznosti na osmikrokový proces od Kottera (2015, s. 39-41) upozorňuje Novák (2016, s. 769-772) na jeho využití spíše u změn většího rozsahu a dodává, že každá změna nese nové překážky. Stejný zdroj přináší nástroj 10 kontrolní seznam změny, viz příloha 8 Obrázek 2, který slouží jako základní vodítko pro plánování změny pomocí několika návodných otázek, ty jsou rozděleny do 3 oblastí: řízení projektu, zvládání odporu a komunikace, právě v poslední oblasti je pamatováno na přípravu důkladného komunikačního

plánu a na samotnou komunikaci s cílovými skupinami. Získané poznatky lze v zásadě shrnout tak, že pro úspěšnou transformaci či změnu je nutná vhodná a důsledná komunikace směrem k účastníkům změn a procesů.

2.2.3 Přidaná hodnota projektového řízení implementovaná do GDPR

Jak poukazují Denley a kol. (2019, s. 37) k implementaci GDPR je možné přistupovat v podobě projektu, zároveň hodnotí, že tento projekt bude potřebovat značné zdroje a vyšší prioritu, aby došlo k zajištění požadovaného souladu s GDPR. K projektovému řízení se přímo vyjadřují Švecová, Veber (2021) i Křivánek (2019, s. 15) a přisuzují mu dlouhou historii, tuto disciplínu označují za proces, při kterém dochází k využívání dovedností, znalostí, technik a zdrojů za účelem dosažení cíle projektu. Samotná definice projektu není již tak jednoznačná, avšak Doležal a kol. (2023, s. 26), Švecová, Veber (2021, s. 1128-1132) i Křivánek (2019, s. 14) se shodují na tom, že v rámci projektového managementu se projekt vyznačuje změnou současného stavu, která spěje do stavu cílového a Švecová, Veber (2021, s. 1165-1177) i Doležal, Krátký (2017, s. 53-54) rozlišují obdobně jednotlivé fáze projektu: zahájení, plánování, realizace a ukončení projektu. Pro potřeby práce budou přiblíženy první dvě fáze.

Švecová, Veber (2021, s. 1163-1170) kladou větší důraz na rozdělení iniciační fáze a fáze plánování projektu oproti Křivánek (2019, s. 522-528), který fázi přípravy a plánování slučuje. Iniciační fáze projektu podle Švecová, Veber (2021, 1167-1170) zvažuje možné varianty řešení, jejím výstupem je výsledné řešení daného problému a zakládací listina projektu včetně základního časového rámce, rozpočtu, definovaného cíle a jmenování projektového manažera. Oproti tomu cíl plánovací fáze podle Švecová, Veber (2021, s. 1167-1179) spočívá ve vytvoření plánu projektu, který je složen z několika dílčích plánů. S tím souhlasí i Doležal (2023, s. 202), jenž zároveň uvádí stejné oblasti jako Švecová, Veber (2021, s. 1171-1177), ze kterých je plán projektu tvořen: rozsah, časový plán, rozpočet, kvalita projektu, lidské zdroje, komunikační plán, řízení rizik, plán externích dodávek, řízení zainteresovaných stran a navíc Doležal (2023, s. 202) zařazuje oblast řízení projektu. Avšak Švecová, Veber (2021, s. 1171-1177) poukazují na skutečnost, že ne všechny uvedené oblasti musí být zahrnuty v každém projektu, vždy by ale měl být sestaven plán rozsahu projektu, rozpočet a časový plán. S tím souhlasí i Doležal, Krátký (2017, s. 53-54), kteří podobně za hlavní parametry zadání považují cíl, termín, rozpočet a vymezení zodpovědností a pravomocí. K tomu jak a kým by měl být projekt řízen je přistupováno různorodě a tento přístup se postupně vyvíjí v čase. Například podle Křivánka (2019, s. 36-43) je za výsledek projektu zodpovědný projektový manažer, který je zároveň vnímán plnohodnotným manažerem, jenž zastává mnoho rolí a zodpovědností, mezi všemi jeho kompetencemi je kladen důraz na systémové myšlení, které všechny kompetence integruje a dává nový pohled na problematiku řízení projektů. Švecová, Veber (2021, s. 1145-1161) rozlišují již několik variant organizačního zařazení projektu: čistá projektová struktura, maticová struktura, projektový tým s koordinátorem a řízení vlivem, kdy některé varianty pracují s projektovým manažerem, v jiných je pouze vedoucí v podobně výrazné autority nebo ustanoveného koordinátora. Naproti tomu Doležal a kol. (2023, s. 31) uznává, že musí být stanovena osoba, která bude projekt koordinovat, avšak nebude se jednat ani tak o manažera, jako spíš leadera. Co se týče ostatních hlavních parametrů pro projekt, existuje mnoho nástrojů, které lze pro jejich stanovení využít, a každý zdroj pracuje s výčtem několika z nich.

Pro potřeby této práce budou uvedeny pouze vybrané nástroje vztahující se k rozsahu projektu, časovému plánu, analýze rizik a rozpočtu. Doležal (2023, s. 211-212) doporučuje pro dostatečné stanovení rozsahu projektu vytvořit dokument, ve kterém bude rozsah definován popisným způsobem. Tento dokument by měl podle stejného zdroje zahrnovat nejen popis obsahu projektu, ale také kritéria pro akceptaci projektu, jeho omezení i předpoklady. Jak dále uvádí Doležal (2023, s. 226), následně je třeba k jednotlivým činnostem odhadnout dobu trvání, k tomu může posloužit například technika odhadu na základě osobní zkušenosti.

V souvislosti s tím Doležal, Krátký (2017, s. 415-418) doporučují při plánování trvání projektu nechat samotné zaměstnance, kteří se na projektu budou podílet, odhadnout kolik času jim jednotlivé činnosti zaberou. Po stanovení rozsahu projektu a doby trvání činností je možné přejít k znázornění časového harmonogramu. Křivánek (2019, s. 554-565) komentuje metodu kritické cesty, kdy tato metoda přináší užitečné informace o časové délce projektu, avšak stejný zdroj zároveň připouští její nedostatky. Podle Doležala a kol. (2023, s. 223-231) je nejčastěji k zobrazení časového harmonogramu využíván Ganttův graf a výhodu vidí zejména v jeho přehledném znázornění. Oproti tomu Švecová, Veber (2021, s. 234-237) a Křivánek (2019, s. 550-553) poukazují na Ganttův diagram, který také vidí jako užitečnou pomůckou vizualizace času, rozsahu a posloupnosti činností v projektu, ač Křivánek (2019, s. 550-553) připouští nevýhody tohoto zobrazení, které dle něj tkví v neposkytování informací o časových rezervách. Naproti tomu je vyzdvihován právě Doležalem a kol. (2023, s. 231) zmiňovaný Ganttův graf, který představuje kombinaci síťového grafu a Ganttova diagramu a toto sloučení zajišťuje odstranění uváděných nevýhod. Křivánek (2019, s. 550-553) za alternativu ke Ganttově diagramu vidí síťový graf projektu, oproti tomu se vyhrazuje Doležal a kol. (2023, s. 232) jenž uvádí, že v dnešní praxi se již nepracuje pouze se síťovými grafy. Dalším důležitým plánovacím krokem projektu je, jak popisuje Svozilová (2016, s. 1527-1531), identifikace rizik, kdy je třeba znát všechny předpoklady a potenciál nežádoucích jevů, některá rizika lze zmírnit nebo zcela eliminovat a výstupem této identifikace je registr rizik, který je podstatnou součástí plánu projektu. Doležal a kol. (2023, s. 271) dodávají, že nejde o sestavení vyčerpávajícího seznamu rizik, nýbrž o identifikaci významných nebezpečí, která mohou projekt výrazně ovlivnit. Nezmar (2017, s. 721-728) upozorňuje na jednu z polokvantitativních metod PZH pro hodnocení rizik, využívanou při hodnocení rizik subjektů údajů, v jejím případě dochází k posouzení rizika ve 3 jeho složkách: pravděpodobnost vzniku, závažnost následku a názor hodnotitelů. Stejný zdroj dodává, že výsledná míra rizika znázorňuje naléhavost přijetí opatření k elimninaci či snížení daného rizika. Za ideální případ pro stanovení nákladů Doležal a kol. (2023, s. 236) považují skutečnost, kdy jsou detailně popsané pracovní balíky z WBS, které mohou být dobrým vstupem pro celkový odhad nákladů na daný projekt, avšak pokud podrobný popis chybí, připouští, že lze obecně vycházet z následujících nákladů jednotlivých činností na materiál, lidskou práci, nakupované služby, dopravu, pronájem, případně další a ty patřičně nacenit. Ke stanovení rozpočtu se vyjadřuje také Svozilová (2016, s. 831-835) a vyzdvihuje zejména využívání odhadů pro některé části projektu a mezi nástroje a techniky odhadu rozpočtu řadí například odhad podle sazeb jednotlivých zdrojů či analogii. Závěrem k plánovací fázi projektu Švecová, Veber (2021, s. 1178-1182) přiřazují úspěch projektu patřičně sestavenému plánu a projektové plánování považují za klíčovou činnost, kterou není možné podcenit. Podobně se vyjadřuje i Křivánek (2019, s. 522-527), který hodnotí fázi přípravy a plánování jako zásadní z hlediska celkového úspěchu projektu a předurčuje vysoké šance na úspěšné zvládnutí řízení projektu, pokud tato fáze bude dobře připravena.

2.3 Metodika práce

V teoreticko-metodologické části diplomové práce byla využita literární rešerše na základě komparace odborných textů citovaných autorů tuzemských i zahraničních zdrojů, včetně právních předpisů, nařízení, interních zdrojů a dat, směrnic a ostatních pramenů. Empirická data a výsledky byly získány z interních zdrojů v souladu s formulací výzkumných otázek a cílů a použitých vědecko-výzkumných analýz. Vzhledem k citlivosti zpřístupněných informací těmto krokům předcházelo podepsání čestného prohlášení. Podpisem prohlášení autorka stvrzuje mlčenlivost, nezneužití osobních údajů a získaných informací, nahlížení do dokumentů s osobními a citlivými údaji za přítomnosti oprávněné osoby z řad vedení organizace a anonymizaci veškerých údajů vztahujících se k vybrané organizaci XY, které budou uváděny v diplomové práci. V analytické části byly využity tyto metody: kvalitativní

a kvantitativní výzkum, polostrukturovaný rozhovor, dotazníkové šetření, analýza interních dokumentů, komparace dat a výsledků, metoda syntézy a dedukce, datový audit, GAP analýza. Význam a přínos GAP analýzy umožnil vymezení rozsahu projektu a predikci jednotlivých projektových činností pro realizaci návrhu projektu.

Analytická část práce byla zahájena kvalitativním výzkumem v podobě polostrukturovaného rozhovoru s ředitelem organizace. Tento typ rozhovoru umožňuje pružnější reagování na získané informace během probíhajícího výzkumu a rozvíjení hlavního tématu a připravených základních otázek, zároveň je díky předepsané osnově udržována přehlednost. Rozhovor probíhal formou osobního setkání a zodpovídal otázky vztahující se k implementaci GDPR do procesů a aktuálnímu nastavení ochrany osobních údajů v organizaci. Přepis rozhovoru je uveden v příloze 1. Následně byl proveden rozbor interních dokumentů a ve spojitosti s kvalitativním výzkumem byl identifikován způsob zajišťování povinností GDPR v organizaci XY, a tím byla zodpovězena první výzkumná otázka: „Jakým způsobem jsou uplatňovány povinnosti vyplývající z GDPR v organizaci“. Spolu s výstupy z teoreticko-metodologické části došlo k vypracování kontrolního checklistu, viz Tabulka 1, a ke zhodnocení souladu dodržování požadavků vyplývajících z GDPR za pomoci komparace, jenž představuje způsob porovnávání shod a podobností. Uskutečněný rozhovor poukázal na první viditelné nedostatky a rozborem interní dokumentace bylo očekáváno jejich potvrzení a přesnější vymezení. Kontrolní checklist obsahoval pouze základní výčet povinností, vztahujících se ke školským institucím, které bylo zároveň možné v dané době posoudit, například nebyla ověřována dostatečně definovaná zákonnost zpracovávaných osobních údajů, přesné vymezení účelů zpracování nebo provedení DPIA. Jednalo se o prvotní zhodnocení, pro které byl uvedený výčet povinností plně dostačující. Již tento výzkum poukázal podle očekávání na nesoulad s povinnostmi GDPR v organizaci XY, a stal se tak podnětem k rozsáhlejšímu výzkumu. Dále bylo potvrzeno nedostatečné plnění outsourcovaných služeb k zajištění GDPR ze strany externí firmy. Získané výsledky potvrdily 1. stanovenou hypotézu: „Pokud organizace neprovádí pravidelné kontroly outsourcovaných služeb, nemůže se spoléhat na důkladné plnění povinností integrovaných s GDPR“.

Z prvotního zhodnocení vyvstala následující výzkumná otázka: „Je využití externího DPO pro danou organizaci efektivnější než tuto činnost delegovat na některého ze zaměstnanců“. Pro její zodpovězení byla zvolena komparativní metoda s využitím bodovací metody, jejichž výstupy ukáží, zda je pro organizaci efektivnější využívat externího nebo interního pověřence pro ochranu osobních údajů. Pomocí komparativní metody lze zkoumat jevy v jejich souvislostech a vztazích, naopak bodovací metoda spočívá v bodovém ohodnocení jednotlivých kritérií, kdy dochází k vypočítání váhy. Vedení organizace poskytlo své priority včetně udělení pořadí jednotlivým kritériím, viz příloha 2 Tabulka 3. V rámci bodovací metody byla každá z výhod i nevýhod ohodnocena body z intervalu $b_i \in \langle 1, 5 \rangle$, podle významnosti pro danou organizaci. Nejvyšší možné bodové ohodnocení v případě výhod je 5, naopak nejlepší ohodnocení v případě nevýhod je 1. Váha kritérií byla dosažena po součinu přiděleného bodu a součtu všech hodnot udělených v dané oblasti výhod či nevýhod. Stanovený postup těchto metod pomohl k posouzení obou variant a určení nejefektivnější z nich.

Výstup z polostrukturovaného rozhovoru se stal podnětem pro kvantitativní výzkum v podobě dotazníkového šetření mezi zaměstnanci organizace. Díky dotazníkovému šetření bylo možné sesbírat větší množství dat o aktuálně nastaveném systému ochrany a bezpečnosti osobních údajů a z nich vyvodit adekvátní závěry. Pro popis a zhodnocení výsledků dotazníkového šetření byly použity relativní hodnoty z důvodu ochrany citlivých údajů vztahujících se k organizaci XY. Respondentům bylo položeno 12 otázek, které si kladly za úkol mimo jiné zjistit, zda jsou zaměstnanci dostatečně informováni o ochraně osobních údajů v organizaci, a jak přistupují k tomuto nastavenému systému. Dotazníkové šetření probíhalo v elektronické

podobě přes docs.google.com v období od 24.04. do 05.05.2023, zapojilo se celkem 83 % z oslovených zaměstnanců a získané výsledky přinesly odpověď na 1. a 2. část výzkumné otázky: „Mají zaměstnanci potřebné informace k systému zabezpečení a ochrany osobních údajů v organizaci?“ a „Přistupují celistvě k nastavenému systému?“ Pro získání odpověďi i na 3. část výzkumné otázky: „Dbají zaměstnanci na dostatečné zabezpečení a ochranu osobních údajů před jejich neoprávněným zpřístupněním cizím osobám?“, proběhla kontrola pracovišť v rámci tzv. politiky čistého stolu dne 05.05.2023 po skončení pracovní doby za součinnosti vedení organizace. Tento nástroj se využívá pro snížení rizika narušení bezpečnosti na pracovišti a spočívá v zajištění důvěrných materiálů a jejich uzamčení v době opuštění pracovního místa. Provedená kontrola ukázala, jak zaměstnanci chrání a přistupují k zabezpečení zpracovávaných osobních údajů. Výsledná anonymizovaná zpráva z tohoto šetření je v příloze 2 Tabulka 6. Po zodpovězení obou částí byla za pomoci syntézy získána odpověď i na tuto výzkumnou otázku: „Jaký je vztah mezi současně nastaveným systémem ochrany osobních údajů v organizaci a přístupem zaměstnanců k tomuto systému“. Zároveň na základě všech doposud provedených výzkumných metod mohlo dojít k naplnění sekundárního cíle, kterým bylo provést zhodnocení současného stavu dodržování povinností stanovených GDPR v organizaci XY.

Pro přesnou identifikaci nesrovnalostí od požadovaného stavu byla zvolena GAP analýza, které předcházel rozsáhlý datový audit. GAP analýza slouží k nalezení nesrovnalostí mezi stavem reálným a plánovaným a postup byl zvolen podle popisu Nezmara (2017, s. 533-554). V první fázi proběhl rozbor dostupných dat a za součinnosti vedení organizace došlo k identifikaci uzlů sběru osobních údajů napříč organizací včetně přiřazení odpovědných osob. Následovaly další kroky datového audity, jejichž úkoly byla identifikace jednotlivých činností a v nich zpracovávaných osobních údajů, včetně vymezení přístupů, smluvních vztahů, využíváných systémů a bezpečnostních opatření. Rozbor dat se zaměřoval na zákonnost zpracovávaných údajů, účel i minimalizaci s výjimkou přesnosti údajů. Tato zásada byla ověřována pouze namátkově u vybraných činností, neboť detailní ověřování nebylo v rámci výzkumu realizovatelné. Datový audit probíhal pomocí zpřístupněných potřebných dokumentů a za součinnosti odpovědných osob hlavních procesů. Odpovědní pracovníci byli nápomocni při detailním mapování jednotlivých činností každého z procesů prostřednictvím dotazníku, jehož vzor je v příloze 4 Dotazník 2. Sběr dat se uskutečnil v období 01.03.2023 – 31.03.2023 a probíhal v tištěné podobě, viz příloha 4 Dotazník 2 – Náhled vyplnění. Tímto způsobem bylo identifikováno 51 činností, ve kterých dochází ke zpracovávání osobních údajů. Zpřístupnění a vyplnění dotazníků předcházelo seznámení odpovědných osob s jednotlivými body dokumentu a toto seznámení proběhlo osobně v organizaci XY. Výstupem datového auditu byly rozsáhlé informace o zpracovávaných osobních údajích v organizaci, na jejichž základě byla provedena komparace dat s povinnostmi vyplývajícími z GDPR. Následně bylo přejito ke shrnutí GAP analýzy, na jejímž základě byly odhaleny mezery a nesoulady od požadovaného stavu. Díky identifikaci výsledků GAP analýzy a v součinnosti s datovým auditem byla navrhnuta doporučení ke změnám včetně opatření, jak systematicky nedostatky napravit. Celkem bylo zmapováno 18 oblastí, které obsahovaly nedostatky, a za pomoci syntézy došlo k popisu kroků potřebných pro jejich odstranění. Pomocí této metody bylo možné z jednotlivých částí formulovat závěry. Tímto byla zodpovězena další výzkumná otázka: „Jaké povinnosti je nutné revidovat ve stávajícím systému ochrany osobních údajů v organizaci potřebných k naplnění souladu s GDPR?“ Zároveň byl naplněn jeden ze sekudnárních cílů, který měl za úkol identifikovat procesy napříč organizací, ve kterých dochází ke zpracovávání osobních údajů. Navrhnutá doporučení ke změnám včetně opatření, jak systematicky nedostatky napravit byly prezentovány vedení organizace XY. Ze strany vedení organizace došlo k upřesnění požadavků pro vypracování a následné akceptování návrhu projektu transformace implementovaného GDPR do procesů organizace.

Díky získaným nesouladům a stanoveným krokům k jejich odstranění bylo možné přejít k samotnému návrhu projektu. Výsledky GAP analýzy pomohly vymezit rozsah projektu, který sestává celkem z 16 činností pro odstranění identifikovaných nesouladů. Jednotlivé činnosti byly zároveň doplněny o předcházející činnosti naněž navazují a o dobu trvání jednotlivých úkolů. Délka trvání byla odvozena logickou úvahou zainteresovaných pracovníků na základě jejich zkušeností a posouzení všech proměnnýc, kdy byla vypracována škála, ze které bylo vycházeno pro logické stanovení délky trvání činností, viz příloha 2 Tabulka 8, a dále byl proveden rozbor jednotlivých činností návrhu projektu za účelem identifikace významnosti, postupu i stanovení času. Tímto vznikl podklad pro časové zobrazení projektu pomocí metody kritické cesty (dále jen „CPM“). Pro zobrazení byl využit uzlově definovaný orientovaný síťový graf. Tato metoda zobrazuje řetěz propojených úkolů, které přímo ovlivňují termín dokončení projektu, zároveň je využívána i z hlediska určení nejkratší možné doby trvání projektu. Pro reálné a detailní zobrazení časového harmonogramu projektu včetně dostupných zdrojů a časových rezerv byl zvolen Ganttův diagram, jehož znázornění proběhlo v programu Excel. Využití tohoto grafu umožňuje jednoduché odečítání rezerv i snadné zorientování se v době trvání celého projektu. Výsledná délka trvání projektu byla stanovena na 52 pracovních dnů v kalendářním roce. Pro zhodnocení projektu byla zpracována analýza rizik pomocí polokvantitativní metody PZH, díky které je zřejmá naléhavost přijetí opatření pro snížení rizika. Tato bodová metoda vyhodnocuje riziko ve třech jeho složkách zaměřujících se na pravděpodobnost vzniku, závažnost následku a názor hodnotitelů. Škály k vyhodnocení uvedených složek jsou zobrazeny v příloze 5 Obrázek 4. Zhodnocení návrhu projektu je zakončeno kalkulací nákladů, které vychází z identifikovaných činností a zpracovaného ganttova diagramu pro určení času stráveného přidělenými zaměstnanci na projektu.

Výsledné závěry jednotlivých kapitol i celé práce byly tvořeny pomocí metody dedukce. Tato metoda se využívá při vyvozování závěrů na základě odvozování obecných předpokladů, tvrzení či skutečností. Návrh projektu byl s několika možnými variantami včetně doporučené verze představen vedení organizace XY, které se jej rozhodlo přijmout a realizovat v doporučené podobě, viz příloha 5 Obrázek 5. Využití těchto metod a získaných výsledků vedlo k naplnění primárního cíle diplomové práce, kterým byla tvorba návrhu projektu transformace implementovaného GDPR do procesů organizace, zároveň byla částečně potvrzena 2. stanovená hypotéza: „Pokud organizace zjistí nedostatečné plnění povinností vyplývajících z GDPR, je schopna vlastními silami provést nápravu“, kompletní potvrzení bude možné po úspěšné realizaci projektu.

3 Analytická část práce

Na začátku analytické části práce je představena vybraná organizace, ve které je daná práce aplikována. Pro tuto práci nese zvolená organizace název „XY“ a z důvodu citlivosti údajů a výsledků, které tato diplomová práce zveřejňuje, jsou informace o organizaci anonymizovány. Tuto část práce lze pomyslně rozdělit do tří úseků, kdy první část představuje podkapitolu, která se věnuje zhodnocení reálného stavu GDPR v rámci procesů organizace. Získané výsledky jsou podkladem pro návrh projektu transformace implementovaného GDPR do procesů organizace, jemuž je věnována následující podkapitola, a třetí závěrečná část se zabývá vyhodnocením výsledků a zhodnocením přínosu práce.

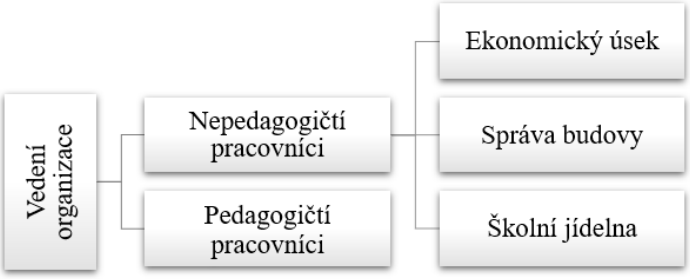
3.1 GDPR v procesech organizace

Tato podkapitola je tvořena ze tří částí a celkově je zaměřena na nastavený systém ochrany osobních údajů ve vybrané organizaci a na posouzení současného stavu ochrany dat s požadovaným stavem dle GDPR. Pro zajištění uceleného pohledu je první část věnována popisu organizace XY, následující subkapitoly se již věnují systému ochrany osobních údajů v organizaci. Potřebné informace k této části práce byly získány ze zpřístupněných interních dokumentů organizace, veřejných zdrojů a na základě zvolených výzkumných metod.

3.1.1 Představení organizace XY

Pro zajištění uceleného pohledu je účelné představit vybranou organizaci a poskytnout o ni základní informace v obecném měřítku. S ohledem na anonoymizaci údajů nebyla odhalena identita organizace XY ve prospěch tohoto požadavku. Zvolená organizace je příspěvkovou organizací a představuje vzdělávací instituci v sektoru školství, přesněji střední školu s již dlouholetou tradicí. V posledních letech došlo k restrukturalizaci organizace, a tato změna přinesla kompletní výměnu členů statutárního orgánu organizace XY (XY, 2023). Organizaci lze přiblížit malému podniku vzhledem k její velikosti do 50 zaměstnanců a v souvislosti s její činností se na ni vztahuje povinnost jmenování pověřence pro ochranu osobních údajů. Původní struktura organizace i přes uvedenou změnu zůstává bez výrazných změn a její aktuální uspořádání je zobrazeno v Diagramu 1.

Diagram 1: Organizační struktura



Zdroj: (interní dokumenty, vlastní zpracování, 2023)

Jak znázorňuje Diagram 1, organizaci XY lze obecně rozdělit do dvou skupin, a to na pedagogické a nepedagogické pracovníky, přičemž nepedagogičtí pracovníci mohou být dále členěni dle jednotlivých pracovních úseků do dalších tří skupin. Dále je nutné obezřejmit, že pracovníci správy budovy a školní jídelny přichází do kontaktu s osobními údaji v omezeném množství. Z dostupných informací (XY, 2023) je zřejmé, že vybraná organizace nezajišťuje pouze středoškolské vzdělávání, ale nabízí i jiné aktivity související s dalším rozvojem a vzděláváním. Je třeba podotknout, že tyto aktivity jsou již nad rámec hlavní činnosti (středoškolského vzdělávání), a jsou určeny komukoliv z řad veřejnosti. Jak poukazuje i výše představený Diagram 1, v organizaci je provozována školní jídelna, ve které

se mohou ke stravování přihlásit i zájemci mimo vybranou organizaci, tj. nemusí se jednat výhradně o studenty nebo zaměstnance organizace XY.

3.1.2 Současný stav dodržování práv a povinností GDPR ve vybrané organizaci

Pro objasnění aktuálního stavu a získání základních informací o zpracovávání osobních údajů v organizaci byl uskutečněn rozhovor s ředitelem organizace XY, viz Příloha 1. Z rozhovoru vyplynuly možné pochybnosti o souladu s GDPR, ty byly zaznamenány především v souvislosti s podklady vedené externí firmou, školením zaměstnanců či provozovaným kamerovým systémem. Rozhovor ukázal, že všechny náležitosti a potřebné dokumenty dle ustanovení GDPR zajišťuje organizaci na základě smluvního ujednání zmiňovaná externí firma. Přehled podkladů a dokumentů, které externí firma zpracovává a eviduje pro vybranou organizaci je uveden v příloze 2 Tabulka 2 a tyto podklady včetně smlouvy mezi oběma stranami byly poskytnutny k nahlédnutí. Ze sjednané smlouvy vyplývá, že externí firma pro organizaci XY zajišťuje:

- vedení potřebné dokumentace ve smyslu právních předpisů o ochraně osobních údajů;
- školení pro vedoucí pracovníky;
- zajištění preventivních bezpečnostních kontrol zaměřených na nakládání s osobními údaji (min. 1x ročně);
- konzultační hodiny dle požadavků organizace XY;
- výkon funkce pověřence pro ochranu osobních údajů.

Závěrem z podepsané smlouvy vyplývá, že externí firma bude činnosti vykonávat takovým způsobem, aby organizace XY plnila požadavky právních předpisů a norem na ochranu osobních údajů.

Na základě získaných informací a poskytnutých dokumentů došlo k posouzení souladu požadovaných a plněných povinností, které má správce dle uvedené legislativy zajišťovat. Pro toto posouzení byl vytvořen kontrolní checklist, který byl stanoven díky získaní teoretických znalostí z podkapitoly 2.1 GDPR a povinnosti pro organizace a k jeho vyhodnocení posloužily zpřístupněné dokumenty a získané poznatky z rozhovoru, viz Příloha 1. Soulad požadovaných a zajišťovaných povinností znázorňuje Tabulka 1 uvedená níže.

Tabulka 1: Vyhodnocení souladu stanovených a plněných povinností v organizaci XY

Bod	Stanovené povinnosti	Plněné povinnosti	Výsledek
1	Pověřenec pro ochranu osobních údajů	Zajišťuje externí firma	√/x
2	Záznamy o činnostech zpracování	Zajišťuje externí firma	x
3	Ověření zpracovatele a zpracovatelské smlouvy	Není evidován žádný záznam	x
4	Hlášení porušení bezpečnosti osobních údajů	Není evidován žádný záznam	-
5	Vnitřní procesy a dokumentace	Zajišťuje externí firma	√

Zdroj: (vlastní zpracování, 2023)

Bod 1 Pověřenec pro ochranu osobních údajů – tato povinnost je smluvně ošetřena externí firmou, která funkci pověřence zajišťuje a v dostupných zdrojích i na webových stránkách organizace XY je uveřejněn kontakt na osobu, která danou funkci za externí firmu vykonává. I přes tuto skutečnost není poskytována dostatečná požadovaná součinnost ze strany pověřence, zejména v konzultačních hodinách a prováděných bezpečnostních kontrolách, jak vyplývá z doložené dokumentace i rozhovoru s ředitelem organizace.

Bod 2 Záznamy o činnostech zpracování – záznamy jsou vedeny externí firmou a doložený soubor obsahuje oblasti: odborné vzdělávání, BOZP, účetnictví a personální agendu. Doložené záznamy byly posouzeny s údaji ze subkapitoly 3.1.1 Představení organizace XY, která uvádí,

že organizace poskytuje i další aktivity nad rámec hlavní činnosti a zajišťuje stravování ve školní jídelně. Z tohoto prvotního posouzení je zřejmé, že v záznamech chybí 2 oblasti.

Bod 3 Ověření zpracovatele a zpracovatelské smlouvy – není evidován žádný záznam, ze kterého by vyplývalo, že zpracovatelé osobních údajů prochází prověřením před podepsáním smlouvy, ani že dochází k jejich kontrolám a auditování v průběhu platnosti smluv. Dále nebyla doložena evidence zpracovatelských smluv. Vzhledem k těmto zjištěním bylo nahlédnuto do smluv mezi organizací XY a externími firmami zajišťujícími účetnictví a správu IT systémů, na tyto externí firmy bylo poukázáno v rozhovoru s ředitelem organizace XY v příloze 1. Bylo zjištěno, že žádná z těchto smluv neobsahuje ujednání o zpracování osobních údajů.

Bod 4 Hlášení porušení bezpečnostní osobních údajů – není evidován žádný záznam o zachycených incidentech, jejich vyhodnocení a následném hlášení ÚOOÚ. Tato skutečnost může potvrzovat i výstup z rozhovoru s ředitelem organizace, že k žádnému incidentu doposud nedošlo. Zároveň je nutné podotknout, že vnitřní směrnice organizace XY k ochraně osobních údajů obsahuje bod okamžitého řešení bezpečnostních incidentů týkajících se osobních údajů, sepsání záznamu o incidentu a reportování závažných incidentů ÚOOÚ. Tato směrnice ukládá povinnost všem zaměstnancům neodkladně hlásit jakékoliv zjištění porušení ochrany osobních údajů pověřenci pro ochranu osobních údajů.

Bod 5 Vnitřní procesy a dokumentace – organizace XY má externí firmou vypracované informační memorandum a směrnici k ochraně osobních údajů (dále již jen „směrnice“). Memorandum je zveřejněno na webových stránkách organizace a představuje dokument, který informuje o zpracovávaných osobních údajích ze strany organizace, dále připomíná práva subjektů údajů a popisuje možnost, jak tato práva u vybrané organizace uplatnit. Směrnice zahrnuje popis přístupů k osobním údajům, postupy a organizační opatření pro nakládání s osobními údaji, včetně postupů pro zpracovatelské smlouvy a hlášení bezpečnostních incidentů. Je nutné zdůraznit, že tato směrnice není nikde v rámci organizace vyvěšena, ani není evidován záznam o jejím seznámení se zaměstnanci. Při posouzení se záznamy o činnostech zpracování je zřejmé, že ve směrnici nejsou popsány všechny činností. Dále je od externí firmy k dispozici formulář smlouvy o zpracování osobních údajů k odborné praxi studentů a dohoda o mlčenlivosti k ochraně utajovaných skutečností pro zaměstnance vybrané organizace. Oba formuláře mají potřebné náležitosti vztahující se k ochraně osobních údajů, avšak využíván je pouze formulář pro zaměstnance, využívaný formulář smlouvy k zajištění praktického vyučování studentů není nijak ošetřen z hlediska předávání osobních údajů. Připravený je i formulář pro udělení souhlasu se zpracováním osobních údajů. Tyto formuláře jsou vyplňovány každým studentem i zaměstnancem a účely, pro které mohou jednotlivci vyjádřit souhlas na daném formuláři jsou uvedeny v příloze 3. Při posouzení se subkapitolou 2.1.2 Povinnosti správců údajů je zřejmé, že ve 3 bodech dochází k nadbytečnému nebo nejasnému vyžadování souhlasů se zpracováním osobních údajů. Jedná se o vyžadování souhlasu za program Erasmus+, který v organizaci neprobíhá, dále o předávání údajů pořadateli akcí a soutěží, kterých se žáci za organizaci účastní a vystavování výtvarných prací a fotografií, v tomto případě je potřeba doplnit mimo prostory školy, aby bylo v souladu vyžadování tohoto souhlasu. Dále bylo identifikováno, že se souhlasy není následně nijak pracováno, neprobíhá jejich důkladná evidence a upozornění, pokud žák nebo zaměstnanec neudělí souhlas k některému z účelů zpracování osobních údajů.

Tabulka 1 zahrnuje hlavní povinnosti vyplývajících ze subkapitoly 2.1.2 Povinnosti správců údajů, které jsou vnímány zejména ve smyslu plnění pro školské organizace. Z této subkapitoly vyplývají i další možné povinnosti a doporučení pro správce údajů, a to: školení zaměstnanců, vyřizování žádostí subjektů údajů a vedení různých evidencí, může se jednat o evidence konzultací, stížností, bezpečnostních incidentů, uplatněných práv, komunikací s ÚOOÚ, souhlasů, interních předpisů či předávaných dat zpracovatelům. Pro základní zmapování

současného stavu plnění GDPR v organizaci bylo přihlédnuto i k uvedeným povinnostem a doporučením a proběhlo posouzení dostupných informací a podkladů s těmito zjištěními. Školení zaměstnanců – zaměstnanci organizace XY nebyli seznámeni a proškoleni v oblasti ochrany osobních údajů, tato skutečnost nejenže vyplývá z rozhovoru, viz Příloha 1, ale potvrzují ji i výsledky dotazníkového šetření mezi zaměstnanci v příloze 4 Dotazník 1 – výsledky. Smlouva stanovuje, že externí firma má zajišťovat školení vedoucích pracovníků, lze očekávat podle nejlepší praxe, že proškolení vedoucí pracovníci předají potřebné informace ostatním zaměstnancům. V důsledku těchto zjištění je pochybení i na straně vedení organizace XY, které mylně očekává, že bude docházet k proškolení všech zaměstnanců, ačkoli externí firma má na základě smlouvy zajišťovat proškolení pouze vedoucích pracovníků.

Žádosti subjektů údajů – proces podávání žádostí ze strany subjektů údajů a jejich vyřizování je popsán v informačním memorandu. Toto sdělení je umístěno na webových stránkách organizace, nikde však není doloženo, že s tímto procesem byli seznámeni i zaměstnanci. Zároveň ze subkapitoly 2.1.3 Práva subjektů údajů také vyplývá, že správci osobních údajů mají usnadňovat výkon práv subjektů údajů. V tomto ohledu je doporučováno poskytovat jednoduché formuláře, které žádajícím subjektům údajů ulehčí uplatnění jejich práv.

Vedení evidencí – nebyl doložen jediný podklad, který by zaznamenával a evidoval některé z těchto údajů: konzultace mezi pověřencem a správcem údajů, záznamy o stížnostech a požadavcích na uplatnění práv subjektů údajů, komunikace mezi pověřencem a ÚOOÚ, poskytnuté souhlasy se zpracováním osobních údajů, výčet všech interních předpisů vztahujících se k zpracovávání osobních údajů, výčet předávaných a zpracovávaných osobních údajů zpracovatelům a zjištěné bezpečnostní incidenty. Podle vyjádření ředitele organizace XY v rámci rozhovoru, viz Příloha 1 lze připustit, že doposud nebyly podány žádné stížnosti ani požadavky na uplatnění práv subjektů údajů, ani nedošlo k bezpečnostnímu incidentu. Vedení evidencí je pouze doporučováno, jejich nedoložení nepředstavuje porušení povinností.

Nyní lze přejít ke shrnutí výsledků. Organizace XY má stanoveného pověřence pro ochranu osobních údajů, vypracované a zveřejněné informační memorandum, které obsahuje proces podávání a vyřizování žádostí na uplatnění práv subjektů údajů, a směrnici, pomocí které se organizace váže k dodržování ochrany osobních údajů a k řízení bezpečnostních incidentů. Naproti tomu záznamy o činnostech zpracování nejsou řádně vedeny, neprobíhá ověření zpracovatelů a zpracovatelské smlouvy neobsahují ujednání o zpracování osobních údajů. Zaměstnanci nejsou školeni v oblasti ochrany a zpracovávání osobních údajů a nejsou vedeny podklady evidující například stížnosti, uplatnění práv subjektů údajů, vzniklé bezpečnostní incidenty nebo předané a zpracovávané osobní údaje zpracovatelům.

Pro lepší přehlednost je znázorněn pohled výhradně na agendu, která má být zajišťována na základě smlouvy s externí firmou. V tomto případě jsou výsledky následující:

- dochází k zajištění funkce pověřence pro ochranu osobních údajů;
- byla vypracována vnitřní směrnice k ochraně osobních údajů a informační memorandum, dále bylo poskytnuto několik standardizovaných formulářů (souhlasy, dohody o mlčenlivosti, viz příloha 2 Tabulka 2), jsou vedeny záznamy o činnostech zpracování osobních údajů, avšak neobsahují kompletní agendu organizace XY;
- školení vedoucích pracovníků nejsou uskutečňována;
- nejsou k dispozici žádné podklady, které by dokládaly provedení preventivních bezpečnostních kontrol ohledně nakládání s osobními údaji minimálně 1x ročně;
- konzultace v podobě osobních setkání nejsou i přes zájem organizace XY uskutečňovány, komunikace probíhá pouze omezeně v elektronické podobě;

Ač je zajištěna funkce pověřence pro ochranu osobních údajů, její výkon není dostatečně plněn a celkově je možné konstatovat, že externí firma dostatečně nezajišťuje náležitosti vyplývající

ze smlouvy. Za velmi závažné neplnění pro organizaci XY lze považovat z hlediska GDPR zejména nekompletní záznamy o činnostech zpracování. V důsledku nedostatečného plnění povinností externí firmou organizace XY nesplňuje stanovené povinnosti plynoucí z GDPR, a jak je patrné ze subkapitoly 2.1.2 Povinnosti správců údajů, odpovědnost jde zcela za správcem údajů, tedy za organizací XY.

V návaznosti na identifikované skutečnosti a pro potřeby rozhodnutí, zda zajistit nového externího nebo interního pověřence pro ochranu osobních údajů v dané organizaci, byla zvolena komparativní metoda, která porovná obě varianty k jejímu vztahu za pomoci bodovací metody. Vedení organizace stanovilo pořadí jednotlivých kritérií, viz příloha 2 Tabulka 3, ze kterých bylo pro komparaci dat a přidělení bodů vycházeno. Posouzení kladných a negativních stránek s bodovým ohodnocením obou variant znázorňuje Tabulka 4.

Tabulka 4: Výhody a nevýhody interních a externích DPO

	Externí DPO	b_i	**Interní DPO**	b_i
Výhody	Nepřetržitá služba	3 (0,14)	Kancelář přímo v organizaci	5 (0,24)
	Znalosti z více organizací	4 (0,19)	Komplexní znalost organizace	3 (0,14)
	Eliminace střetu zájmů	2 (0,10)	Potenciálně nižší náklady	4 (0,19)
Součet všech výhod za obě varianty				21
Nevýhody	Kancelář mimo organizaci	3 (0,16)	Dovolená, nemoci	3 (0,16)
	Neznalost organizace	2 (0,11)	Nutnost proškolení	4 (0,21)
	Vyšší náklady	5 (0,26)	Hrozba střetu zájmů	2 (0,11)
Součet všech nevýhod za obě varianty				19

Zdroj: (vlastní zpracování, 2023)

V souvislosti s požadovaným rozhodnutím je potřeba posoudit jednotlivá hlediska z pohledu organizace XY. Pro toto posouzení bude každá z výhod i nevýhod ohodnocena body z intervalu $b_i \in \langle 1, 5 \rangle$, podle významnosti pro danou organizaci. Nejvyšší možné bodové ohodnocení v případě výhod je 5, naopak nejlepší ohodnocení v případě nevýhod je 1. Údaje, které zobrazuje Tabulka 4 v závorce, představují váhu jednotlivých kritérií za dané oblasti výhod a nevýhod. Pokud budou vzaty v úvahu dosavadní zkušenosti s externí firmou zajišťující GDPR a současný stav nedostatečného souladu plnění povinností, je pro organizaci velmi důležitý přímý kontakt s pověřencem pro ochranu osobních údajů. Na základě této skutečnosti je kancelář přímo v organizaci ohodnocena 5 body, naproti tomu kanceláři mimo organizaci budou přiděleny 3 body. Pro organizaci jsou důležité komplexní znalosti interního zaměstnance o dané organizaci, kterými nemůže disponovat externí pracovník. Přesto lze připustit, že tato výhoda interního DPO z dlouhodobého hlediska není až tak nedosažitelná pro pracovníka mimo organizaci, z toho důvodu tato nevýhoda nepředstavuje tak vysokou váhu. Pokud by se externí DPO pohyboval v organizacích patřících do stejného odvětví, mohl by být svými zkušenostmi velmi cenný pro danou organizaci, z tohoto důvodu je tato varianta ohodnocena 4 body. Pokud bude zvážena časová dostupnost DPO, tak v případě počáteční implementace by jistě byla výhodná nepřetržitá dostupnost, avšak v tomto případě lze očekávat, že tato služba nebude představovat takový význam. U externího DPO je zaručeno, že nebude hrozit střet zájmů, ačkoli v případě interního DPO disponuje organizace minimálně 3 pracovníky, kteří se ze svých pozic této role mohou ujmout bez většího zásahu do úpravy jejich kompetencí. Jednou z výraznějších nevýhod interního DPO je nutnost jeho prvotního proškolení na danou pozici a s tím i spojené náklady, přičemž z dlouhodobého hlediska lze očekávat návratnost této investice v podobě nižších nákladů za zajištění této role interním zaměstnancem, která je organizací velmi vítána. Oproti tomu u externího DPO vyšší náklady představují významnou nevýhodu, která byla ohodnocena 5 body. V tomto ohledu byl proveden průzkum trhu,

viz příloha 2 Tabulka 5, který potvrzuje vyšší náklady u externích firem. Uvedené částky v průzkumu jsou pouze za poradenské služby, ve výsledku musí být počítáno s dalšími náklady za tvorbu dokumentace, vedení evidencí, školení zaměstnanců atd. Po přidělení bodů lze přejít k vyhodnocení, váha jednotlivých variant je získána dle vztahu bodů k celkovému součtu všech bodů dané kategorie a tyto váhy uvádí Tabulka 4 v závorce. Na první pohled je viditelné, že bodové ohodnocení u nevýhod vyšlo pro obě varianty podobně. V případě výhod je již patrný rozdíl s kladným výsledkem pro interního DPO. I vzhledem k požadavkům vedení organiazce XY, je zřejmé, že pro organizaci je efektivnější využití interní zaměstnance.

3.1.2.1 Výzkum mezi zaměstnanci organizace

Pro získání uceleného pohledu na současný stav dodržování povinností GDPR v organizaci byl uskutečněn kvantitativní výzkum v podobě dotazníkového šetření mezi zaměstnanci a proběhla kontrola jednotlivých pracovišť zaměstnanců v rámci tzv. politiky čistého stolu. Kvantitativní výzkum byl zařazen v reakci na získané podněty z polostrukturovaného rozhovoru s ředitelem organizace a jeho úkolem bylo zjistit, zda jsou zaměstnanci dostatečně informováni o ochraně osobních údajů v organizaci, a jak přistupují k tomuto nastavenému systému. Formulář dotazníku včetně výsledků je k náhledu v příloze 4 Dotazník 1 a Dotazník 1 výsledky. Struktura formuláře se skládala z 12 otázek, z nichž 1 otázka byla otevřená a ve 3 otázkách mohlo být uvedeno více odpovědí. Šetření se zúčastnilo 83 % zaměstnanců a záměrně nebylo do tohoto výzkumu zahrnuto vedení organizace XY.

Na úvod dotazníku byly zařazeny otázky dotazující se na školení zaměstnanců v souvislosti s GDPR. Celkem 76 % respondentů potvrdilo, že nebyli zaměstnavatelem proškoleni v této oblasti a zbývajících 24 % si již nevzpomíná, zda školení proběhlo či ne. Dohromady 64 % respondentů se shodlo, že by uvítali školení v tomto směru 1x za rok, ostatním 36 % by školení stačilo 1x za 2 roky, v tomto případě se jedná převážně o respondenty, kteří nepřichází v rámci pracovní činnosti do pravidelného kontaktu s osobními údaji, jak vyplynulo z identifikačních otázek jednotlivě vyplněných dotazníků. Více jak polovině respondentů (56 %) by vyhovovalo školení formou e-learningu, ostatní respondeti (44 %) se shodli na prezenční formě školení, online školení neuvedl žádný z dotazovaných. Následoval sled otázek ověřujících znalosti respondentů. Všichni respondeti zvládli zodpovědět otevřenou otázku „Co to je GDPR, čeho se týká?“, ačkoli kvalita jednotlivých odpovědí se lišila. Celkem 24 % respondentů vystihlo danou definici, u 64 % odpověď byla dostatečná, naopak 12 % neformulovalo odpověď dostatečně, avšak to podstatné z ní bylo zřejmé. Dále měli respondeti označit pojmy, které podle nich představují osobní údaje. Všichni respondeti patřičně označili jméno, příjmení, adresu, zdravotní stav, a zároveň všichni adekvátně neoznačili sídlo firmy, IČO a číslo účtu firmy. Pouze 92 % respondentů patřičně označilo fotografii a kamerový záznam a 84 % zaškrtlo emailovou adresu skládající se z jména a příjmení. Naopak 16 % respondentů nevhodně označilo služební telefonní číslo. V případě, že dojde k porušení zabezpečení osobních údajů, 76 % respondentů jej chybně nahlásí řediteli organizace, pouze 24 % patřičně bude kontaktovat pověřence pro ochranu osobních údajů. Další výčet otázek zjišťoval znalosti respondentů o aktuální situaci v jejich organizaci. Ukázalo se, že pouze 60 % respondentů si je vědomo, že organizace má pověřence pro ochranu osobních údajů, avšak jen 36 % ví, kde jsou uvedeny jeho kontaktní údaje. Ostatních 40 % neví, zda má organizace nějakého pověřence. Všichni respondeti se také shodli, že v organizaci je nastaveno bezpečnostní opatření uzamykání kanceláří/kabinetů při jejich opuštění, 84 % označilo jako další opatření přihlašování do počítačů a systémů pomocí hesel, 52 % respondentů uvedlo omezené přístupy k osobním údajům v systémech podle pracovních pozic a vypínání PC/notebooků při odchodu z pracoviště. Pouze 24 % respondentů označilo za nastavené bezpečnostní opatření v organizaci uzamčení dokumentů s osobními údaji při odchodu z pracoviště. Touto otázkou bylo zjišťováno, jaká opatření jsou v organizaci nastavena a zaměstnanci si jich jsou vědomi,

následující otázka zkoumala, jaká opatření zaměstnanci dodržují bez ohledu na to, zda jsou stanovena organizací. Všichni respondeti při odchodu z kanceláře/kabinetu zamykají místnost a při odchodu z pracoviště vypínají PC/notebook. Pouze 52 % respondentů uvedlo, že se přihlašují pomocí hesel, kdy hesla nemají předuložena. Dokumenty s osobními údaji uzamyká do příslušných skříní a polic 24 % respondentů, avšak pouhých 16 % dbá na jejich uložení/uzamčení vždy při odchodu z pracoviště. Poslední závěrečné otázky byly již obecnějšího charakteru, kdy bylo zjišťováno, jak respondenti vnímají GDPR a zbývající 2 otázky byly identifikační. S velkou převahou je GDPR vnímáno pozitivně, 72 % respondentů jej označilo za důležité, 16 % jej vnímá jako přítěž, avšak respektují ho, zbývajících 12 % GDPR považuje za zbytečné. Dále se ukázalo, že 60 % respondentů nastoupilo do vybrané organizace před vstupem platnosti GDPR, tedy před květnem 2018, zbývajících 40 % nastoupilo až po květnu 2018. Respondenti dotazníkového šetření byli tvořeni více jak z poloviny (56 %) pedagogickými pracovníky, 16 % představovali nepedagogičtí pracovníci ekonomického úseku a 28 % tvořili ostatní nepedagogičtí pracovníci, tj. může se jednat o zaměstnance správy budovy či školní jídelny.

Dotazníkové šetření poukázalo, že ač v organizaci neprobíhají školení zaměstnanců vztahující se k ochraně a zpracovávání osobních údajů, mají zaměstnanci základní povědomí týkající se problematiky GDPR. I přesto výsledky šetření poukazují na jisté mezery ve znalosti postupu ohlašování bezpečnostních incidentů či poukazují na potřebu ozřejmění zaměstnancům bezpečnostní opatření, která je potřebné dodržovat, a tím předcházet možným bezpečnostním incidentům. Výsledky poukázaly na četnost a možnou formu školení k ochraně a bezpečnosti zpracovávaných osobních údajů, která by byla pro zaměstnance vyhovující.

Jak je stanoveno v rámci směrnice, materiály ze školní matriky, osobní spisy žáků, zaměstnanců a další, jsou uloženy v k tomu příslušných uzamykatelných kancelářích v zabezpečených skříních, při práci s elektronickou evidencí matriky nesmí pracovníci opouštět počítač bez jeho odhlášení. K tomuto zacházení s osobními údaji se zaměstnanci zavazují i v rámci dohody o utajovaných skutečnostech, kterou podepisují na začátku pracovního vztahu, kde je přímo stanoveno uzamykání kanceláří, pracovních stolů a zamezování zpřístupnění informací v rámci PC a notebooků. Na základě těchto skutečností bylo zařazeno provedení kontroly pracovišť v rámci tzv. politiky čistého stolu. Tato kontrola následovala po dotazníkovém šetření a ověřovala, zda zaměstnanci dbají na dostatečné zabezpečení a ochranu osobních údajů. Kontrola proběhla po skončení pracovní doby zaměstnanců za součinnosti vedení organizace a primárně bylo ověřováno, zda na jednotlivých pracovištích nejsou volně k dispozici podklady obsahující osobní údaje a dále bylo kontrolováno vypnutí přidělené IT techniky a dle možností její uložení a zabezpečení.

Během provedené kontroly bylo náhodně nahlédnuto do 3 kanceláří, 4 kabinetů a 4 kmennových tříd. Uskutečněná kontrola ukázala v některých případech na nedostatečné zabezpečení fyzických dokumentů. V jedné z kanceláří byly volně přístupné dokumenty se jmény a doručovacími adresami osob, kterým byly zaslány dopisy, druhý případ odhalil v jednom z kabinetů volně přístupné podklady s jmennými seznami žáků jednotlivých tříd a jejich docházkou za poslední měsíc. Dále bylo ve 2 třídách zjištěno vyvěšení jmenných seznamů žáků dané třídy, a to včetně rozpisu čísel přiřazených osobních skříněk. Tato zjištění se vztahují pouze k 1 kanceláři, 1 kabinetu a 2 třídám. Ostatní pracoviště byla z hlediska zabezpečení osobních údajů vzorně zanechána zaměstnanci po jejich odchodu z práce. Také IT vybavení byly na všech kontrolovaných pracovištích povypínány, případně uloženy. Protokol se zápisem a výsledky z provedené kontroly je k nahlédu v příloze 2 Tabulka 6.

Ač kontrola ukázala na nezabezpečené dokumenty s osobními údaji na několika pracovištích, nebyly nalezeny žádné volně přístupné podklady, které by obsahovaly citlivé osobní údaje. K jmenným seznamům v rámci tříd se již při kontrole vyjádřilo vedení organizace, které

argumentuje, že žáci si nepamatují čísla osobních skříněk, nebo je nutné rozepisovat služby mezi jednotlivými studenty a tímto seznamem je o daných službách informovat a připomínat jim je. Jakkoliv se zdá být argumentace vedení organizace pochopitelná, nelze opomenout skutečnost, že kamenné třídy jsou navštěvovány i ostatními studenty, i dokonce osobami, které do školy dochází v rámci jejich dalších provozovaných činností. Dále vedení organizace při probíhající kontrole připustilo, že některá pracoviště nedisponují dostatečným vybavením pro ukládání a uzamykání dokumentů. I přes uvedená zjištění výsledky kontroly ukázaly na převážné zajišťování ochrany a zabezpečení dokumentů s osobními údaji ze strany zaměstnanců, zároveň došlo k identifikaci mezer a dalších možností pro zlepšování bezpečnostních opatření.

Na základě provedených výzkumů mezi zaměstnanci lze konstatovat, že přes identifikované mezery související zejména s bezpečnostními opatřeními a řízením bezpečnostních rizik, mají zaměstnanci základní povědomí o dané problematice, uvědomují si nastavená bezpečnostní opatření v organizaci a většina zaměstnanců dbá na jejich dodržování. Celkově je přístup zaměstnanců k nastavenému systému v této oblasti vnímám převážně jako respektující a zodpovědný, avšak s potřebou proškolení a ozřejmění všech souvisejících náležitostí.

3.1.3 Datový audit

Z předchozí subkapitoly 3.1.2 Současný stav dodržování povinností GDPR v organizaci je zřejmé, že implementace GDPR do procesů organizace nebyla provedena dostatečně a současný stav není v souladu se stanovenými povinnostmi. Aby bylo možné napravit již proběhlou implementaci, musí dojít v první řadě k identifikaci hlavních procesů vybrané organizace, získat detailní přehled o jednotlivých činnostech, které v rámci hlavních procesů probíhají, identifikovat osobní údaje, které se v nich zpracovávají, včetně získání informací o využívaných systémech, zpracovatelích a zakomponovaných bezpečnostních opatření. Na základě sběru veškerých uvedených dat bude možné provést GAP analýzu, která upozorní na potřebné nedostatky a mezery. Celý postup auditu je rozdělen a popsán v několika krocích.

1. Krok – identifikace uzlů sběru osobních údajů

Celkem bylo ve vybrané organizaci identifikováno 10 hlavních uzlů, ve kterých dochází k sběru osobních údajů. Každý uzel představuje oblast, ve které může probíhat jedna, ale i více dalších činností, ve kterých dochází ke zpracovávání osobních údajů, a každá z identifikovaných oblastí má svého odpovědného vedoucího. Z důvodu zajištění ochrany organizace a odlivu citlivých informací byly názvy 4 identifikovaných uzlů pro účely diplomové práce nahrazeny jednotným obecným názvem pouze s rozlišením dle čísel. Přehled všech uzlů znázorňuje Diagram 2.

Diagram 2: Hlavní procesy organizace XY

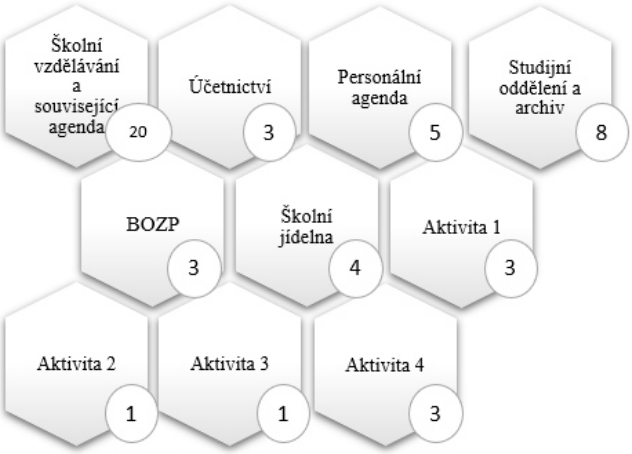
Zdroj: (vlastní zpracování, 2023)

První řada uzlů v Diagramu 2 představuje primární aktivity organizace XY, v souvislosti a návaznosti na to je druhá řada tvořena podpůrnými činnostmi, které pomáhají zajišťovat a udržovat hlavní chod organizace. Poslední třetí řada je věnována vedlejším aktivitám, které fungují po vlastní ose nad rámec primárních aktivit organizace. Tyto aktivity mohou využívat studenti i zaměstnanci organizace XY, avšak nepředstavují primární cílovou skupinu, zejména jsou tyto aktivity využívány zájemci tzv. mimo řady organizace XY.

2. Krok – označení jednotlivých zpracování

Jak bylo naznačeno již v předchozím kroku, v každém z hlavních identifikovaných uzlů může probíhat až několik dalších činností, ve kterých se zpracovávají osobní údaje. K podchycení všech těchto činností byl využit dotazník, jehož vzor je k náhledu v příloze 4 Dotazník 2. S vyplněním dotazníku a identifikací potřebných náležitostí byli nápomocni odpovědní vedoucí pracovníci za jednotlivé oblasti, kteří na základě krátkého proškolení uvedené údaje vyplňovali. Celkem bylo k 10 uzlům identifikováno 51 činností, ve kterých probíhají operace s osobními údaji. Rozřazení těchto činností k jednotlivým uzlům zobrazuje Diagram 3.

Diagram 3: Hlavní procesy organizace rozšířené o počty činností s osobními údaji



Zdroj: (vlastní zpracování, 2023)

U uvedených činností bylo na základě vyplněných dotazníklů primárně ověřováno, jestli dochází ke zpracování pouze potřebných osobních údajů, jaký je účel zpracování, zda dochází ke zpracování podle zákonných důvodů a jejich uchování trvá pouze po nezbytnou dobu, viz subkapitola 2.1.2. Povinnosti správců údajů. Tento krok přinesl mnoho důležitých zjištění.

Pouze ve 4 identifikovaných uzlech bylo shledáno vše v pořádku. Dále bylo odhaleno, že ve 3 činnostech z 51 dochází k nadbytečnému zpracovávání informací, v těchto případech se jedná o nadbytečné vyžadování zdravotní pojišťovny a rodného čísla v oblasti Školního vzdělávání a dále dochází k nadbytečnému vyžadování místa bydliště v rámci jedené z činností v Aktivita 4. Zpracovávání údajů: zdravotní pojišťovna a číslo občanského průkazu neprobíhá zákonně, toto zpracování je možné na základě souhladu subjektů údajů, který však není vyžadován. V 6 případech z 51 činností nedochází k informování subjektů údajů o tom, jaké údaje jsou o nich zpracovávány a komu jsou předávány. Celkem 10 činností z 51 není zařazeno ve spisovém a skartačním řádu organizace, ani v jiném dokumentu není stanovena lhůta pro dobu ukládání údajů. U žádné z 51 činností nebylo uvedeno, že by docházelo k řízení bezpečnostních incidentů, tj. v případě porušení bezpečnosti zpracovávaných osobních údajů u dané činnosti není nastaven systém pro řízení incidentu. Vzhledem k směrnici, která stanovuje hlášení bezpečnostních incidentů, tato skutečnost utvrzuje, že zaměstnanci s ní nejsou

seznámeni. Z vyplněných dotazníků dále vyplynulo, že Aktivita 1, Aktivita 3 a 1 z 8 činností v rámci uzlu Studijní oddělení a archiv, představují procesy zpracování, kde vybraná organizace je v roli zpracovatele.

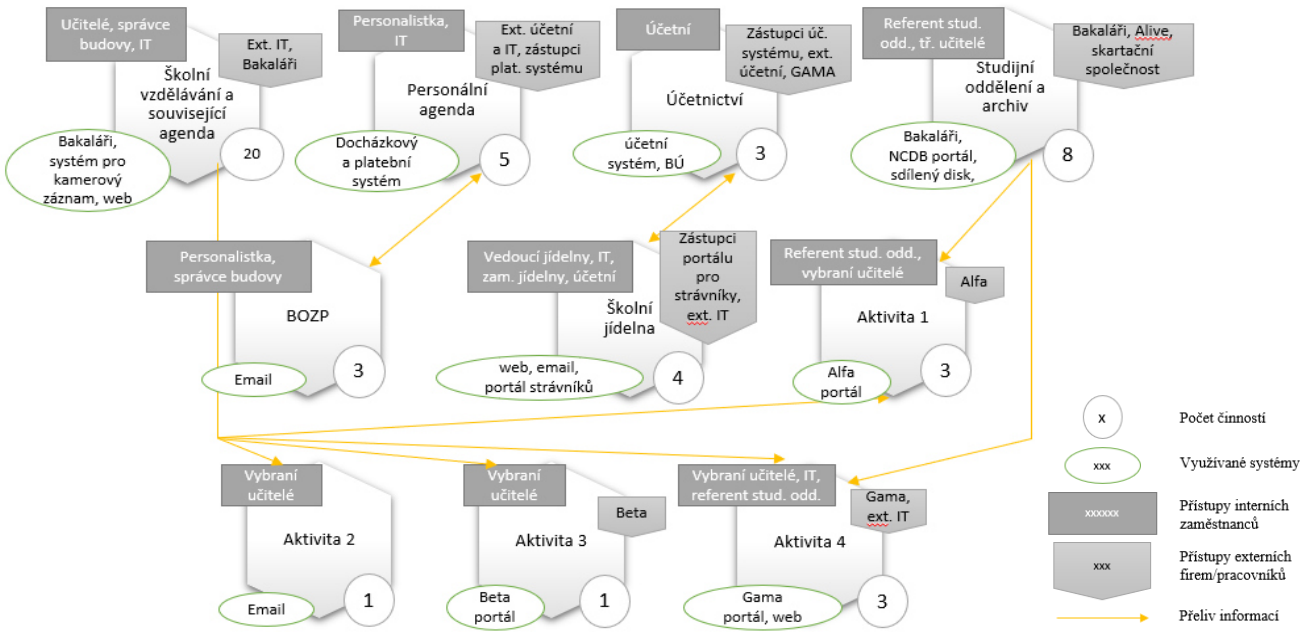
Získané údaje byly porovnávany s doloženými záznamy o činnostech zpracování osobních údajů, které vede pro vybranou organizaci externí firma. Posouzení ukázalo, že téměř 6 z 10 identifikovaných uzlů není evidováno v záznamech, v některých případech se jedná pouze o absenci konkrétních aktivit. V záznamech nejsou zahrnuty tyto oblasti: školní jídelna, aktivity 1-4 a některé z činností studijního oddělení a archivu. Jak značí subkapitola 2.1.2 Povinnosti správců údajů, nejen správci, ale i zpracovatelé jsou povinni vést záznamy o činnostech zpracování, z čehož vyplývá, že i v aktivitách, kde je organizace v roli zpracovatele, musí docházet k vedení uváděných záznamů.

Závěr dotazníku se věnoval posouzení rizik pro práva a svobody osob při jednotlivých činnostech. Ve dvou případech bylo zaznamenáno odpovědnými osobami, že pořizování kamerových záznamů a skartace dokumentů jsou činnosti, při kterých dochází ke zpracovávání osobních údajů způsobem, který představuje vysoké riziko, přičemž mezi poskytnutnými podklady od externí firmy, viz příloha 2 Tabulka 2, nebyly dohledány žádné provedené balanční testy ani uskutečněná DPIA. Dále v organizaci XY nebyl shledán nastavený proces posuzování rizik. Absenci identifikace, vyhodnocování rizik a postupů k jejich eliminaci v systému bezpečnosti a ochrany osobních údajů lze vyhodnotit jako kritickou mezeru v nastavených procesech organizace. S ohledem na získané poznatky od Valentové (2023) se doporučuje vycházet z prvotního posouzení dle pokynů WP248, jenž zodpoví nutnost provedení DPIA. Bez ohledu na dané posouzení je samozřejmostí donastavení postupu hodnocení rizik.

3. Krok – vymezení datových toků

Tento krok zmapoval napříč organizací využívané IT systémy a aplikace, ve kterých dochází ke zpracovávání osobních údajů. Zároveň identifikoval, jaké údaje jsou předávány či zpřístupněny externím pracovníkům a poukázal na interní pracovní pozice a jim zpřístupněné zpracovávané osobní údaje, ať již v tištěné či elektronické podobě. I v tomto kroku bylo navázáno na předchozí Diagramy 2 a 3, které následující Diagram 4 rozvádí o další údaje.

Diagram 4: Hlavní procesy organizace rozšířené o IT systémy a datové toky



Zdroj: (vlastní zpracování, 2023)

Každý z identifikovaných uzlů v Diagramu 4 byl doplněn o výše uvedené informace, pokud je konkrétní uzel tvořen více činnostmi, neznamená to, že přístupy mají všechny uvedené pozice nebo že uvedený systém je využíván ve všech činnostech, tj. uvedené informace byly pro každou aktivitu shrnuty za všechny činnosti. Žluté šipky naznačují provázanost interních zaměstnanců mezi jednotlivými aktivitami. Pokud dochází k předávání údajů na základě zákonné povinnosti, nedochází k uvedení těchto institucí i z důvodu zajištění přehlednosti pro následný krok datového auditu. Vedení organizace má s ohledem na výkon svých funkcí přístup ke všem zpracovávaným údajům. K osobním údajům je umožněn přístup i pověřenci pro ochranu osobních údajů, avšak pouze v případech, kdy je přístup potřebný a souvisí s výkonem dané činnosti. Jednotlivé aktivity a jejich datové toky jsou níže detailněji popsány.

Střední vzdělávání a související agenda – celkem 15 činností je zpracováváno v systému Bakaláři, z toho 13 z nich zpracovávají nebo jsou zpřístupněny učitelům, v některých případech se jedná pouze o třídní učitele. Ke zpracovávaným údajům v tomto systému mají přístup zástupci poskytující společnosti. Další 2 činnosti probíhají přes webové stránky organizace, pro 1 činnost je využíván systém pro přenos záznamů z kamerového systému. K údajům v těchto systémech má přístupy interní zástupce za IT, externí IT společnost, ta zajišťuje správu i systému Bakaláři, a k záznamům z kamer má přístupy navíc také správce budovy. Poslední 2 činnosti jsou zpracovávány pouze třídními učiteli na žádost subjektu údajů a údaje jsou zpracovávány v systému Bakaláři i mohou být uchovávány v tištěné podobě, na základě formy předložené žádosti. Personální agenda – v 1 činnosti je využíván platební systém a tyto údaje jsou předávány osobní formou externí účetní, zároveň mají do systému přístup i zástupci společnosti využívaného systému. Dále personalistka pracuje s docházkovým systémem, který spravuje externí IT společnost, přístupy k tomuto systému má i interní zástupce za IT. Ostatní údaje jsou zpracovávány pouze personalistkou v tištěné podobě a nedochází k jejich dalšímu předávání. Účetnictví – pro všechny činnosti je využíván účetní program, do kterého má přístupy pouze interní účetní a zástupci provozující společnosti. Jedna činnost probíhá za součinnosti s externí účetní, dále údaje z 1 činnosti jsou zpřístupněny organizaci GAMA. Pro všechny činnosti dochází k využívání bankovního účtu, který se váže na právní a smluvní povinnosti, nutno dodat, že přístupy k manipulaci s bankovním účtem má pouze interní účetní a vedení školy. Studijní odd. a archiv – činnosti vyřizuje referent studijního odd. a u 3 činností z 8 mají k údajům přístup i třídní učitelé. Ve 4 případech jsou využíváni zpracovatelé, kteří mají přístup k vybraným osobním údajům, z toho ve 2 případech se jedná o zástupce systému Bakaláři, v 1 případě o zástupce skartační společnosti a v 1 případě o společnost Alive, která zajišťuje ISIC karty přes portál NCDB. Co se týče skartační společnosti, té jsou podklady předávány fyzicky pomocí speciálních bezpečnostních boxů. Při poslední činnosti dochází ke zpracovávání osobních údajů přes sdílený disk, kdy jsou data předávána pouze mezi referentem studijního odd. a vedením organizace. BOZP – přístupy ke všem podkladům této oblasti obsahujícím osobní údaje má personalistka, jakožto osoba pověřená evidencí úrazů a školení, a s tím vedení souvisejících dokumentů. Správce budovy zastává zároveň pozici interní osoby zajišťující BOZP a má přístupy ke školícím podkladům. V momentě, kdy nastane úraz, dochází na základě ŠZ § 29 k nahlášení úrazu na příslušnou pojišťovnu případně další instituce zejména prostřednictvím emailové komunikace. Školní jídelna – celkem 3 činnosti jsou navázány na portál pro evidenci strávníků, přístupy do tohoto portálu má pouze z interních zaměstnanců vedoucí jídelny, 1 z těchto činností probíhá za součinnosti s interní účetní, mezi kterými je využívána pouze emailová komunikace. Poslední 4. činnost je navázána na webové stránky organizace, kde jsou zpřístupněné údaje napojeny na interního IT zástupce, na vedoucí jídelny a externí IT společnost. V 1 ze 4 činností jsou osobní údaje zpřístupněny všem pracovníkům v kuchyni, jedná se o minimální množství předávaných údajů a dochází k okamžité skartaci podkladů na konci každého dne, kdy k tomuto předání dojde. Avšak předání těchto údajů je nutné pro zajištění samotné činnosti. Aktivita 1 – všechny činnosti jsou

zpracovávány přes internetový portál Alfa a toto zpracování je zajištěno referentem studijního oddělení. K údajům z jedné z činností mají na základě tištěných podkladů přístup i vybraní učitelé, v rámci této činnosti jsou však údaje pseudonymizovány. Údaje jsou přístupné také zástupcům spravujícím portál Alfa, jakožto správci osobních údajů, organizace XY je v tomto případě v roli zpracovatele. Aktivita 2 – probíhá pod vedením vybraného učitele, v některých situacích může docházet na základě žádosti subjektu údajů ke sdílení osobních údajů přes email, není to však pravidlem. Údaje jsou evidovány pouze v tištěné podobě, uloženy v kanceláři školy a nedochází k jejich dalšímu předávání. Aktivita 3 – probíhá pod vedením vybraných učitelů, zpracování probíhá pouze v systému Beta, údaje jsou zpřístupněny zástupcům portálu, jakožto správci a organizace XY je v roli zpracovatele. Aktivita 4 – pro 2 ze 3 činností je využíván portál Gama. S tímto portálem pracuje vedení organizace, které má rozšířená oprávnění, a referent studijního odd. s již omezenými přístupy. K vybraným údajům v omezeném množství zpracovávaným v tištěné podobě mají přístup vybraní učitelé, z externích uživatelů mají přístup zástupci Gama. K zbývající 1 činnosti jsou využívány webové stránky organizace XY, přístup k těmto údajům má referent studijního odd., interní zástupce za IT a externí IT společnost.

Identifikovaná zjištění jsou nezbytným podkladem pro následující krok. Zároveň lze konstatovat, že přístupy do využívaných systémů a aplikací v rámci daných činností mají k dispozici pouze nezbytní interní i externí pracovníci. Vzhledem ke skutečnosti, že externí IT firma obstarává chod několika využívaných systémů zpracovávajících osobní údaje napříč organizací, představuje smlouva s touto firmou jeden z významnějších bodů k ověření v dalším kroku tohoto prováděného datového auditu.

4. Krok – stanovení souladu smluvních vazeb

Na základě grafického zpracování v Diagramu 4 bylo identifikováno 11 smluvních vazeb, u kterých bylo ověřováno, že aktuálně platná smlouva disponuje potřebnými náležitostmi vztahujícími se k ochraně osobních údajů. Na jednotlivé body, které by měla smlouva obsahovat odkazuje subkapitola 2.1.2 Povinnosti správců údajů, z tohoto výčtu bylo při daném posouzení vycházeno.

Smlouvy se společnostmi Gama, Bakaláři i společnost zajišťující portál pro strávníky obsahují požadované náležitosti k GDPR a lze je považovat za adekvátně nastavené. Společnost, která zaštiťuje službu skartace dokumentů, funguje na základě objednávkového systému, mezi těmito subjekty tak není smlouva. Tento nastavený proces je zajišťován pomocí vystavení protokolu o převzetí a likvidaci dokumentů, který je organizaci předán při přebírání podkladů ke skartaci. Protokol vystavený skartační společností je opatřen i GDPR certifikátem o likvidaci nosičů dat a dalšími požadovanými náležitostmi na zpracovatelské smlouvy vztahujcími se k bezpečnostním opatřením a zacházení s předanými podklady. V případě společnosti poskytující účetní program nebyly ve smlouvě identifikovány všechny potřebné náležitosti. Zároveň ustanovení ve smlouvě opravňují zpracovatele k možnosti zajistit si subdodavatele bez předchozího informování správce. V případě externích společností zajišťující účetní a IT služby bylo odhaleno, že smlouvy neobsahují žádné z požadovaných bodů k bezpečnosti a ochraně zpracovávaných údajů. Dále u společnosti poskytující platební systém, ve kterém se zpracovávají osobní údaje zaměstnanců nebyla smlouva zcela dohledána.

Již předchozí kroky datového auditu upozorňovaly na postavení organizace XY v roli zpracovatele u několika aktivit. Tuto roli organizace zastává u společností Alfa, Beta a Alive. Podepsané smlouvy s těmito společnostmi byly podrobeny ověření, resp. ověřování podléhaly nastavené smluvní podmínky vztahující se k bezpečnosti a ochraně osobních údajů. Ve všech třech případech bylo potvrzeno, že smluvní podmínky jsou v souladu s GDPR a nebyly identifikovány žádné nedostatky.

S ohledem na poskytované osobní údaje externí účetní firmě a provázanosti systémů na zpracovávané osobní údaje, které obstarává nasmluvněná IT firma, jsou zjištěné výsledky o absentujících doložkách k GDPR ve sjednaných smlouvách alarmující. Organizace se touto skutečností vystavuje závažnému riziku s ohledem na povinnosti vyplývající z GDPR, přičemž jde za ní veškerá odpovědnost. V této situaci není prostor pro jiné varianty, než sjednání nápravy nebo rozvázání smluvních vztahů.

5. Krok – popis bezpečnosti dat

Zpracovávané údaje organizací XY jsou uchovávány v tištěné nebo elektronické podobě. Údaje v tištěné podobě představují pouze omezené množství, jsou uloženy v kancelářích převážně pracovníků ekonomického úseku a tyto kanceláře jsou uzamykány, některé z nich disponují i několika uzamykatelnými skříněmi pro nejcitlivější údaje a přístup do nich je omezený pouze pro vybraný okruh pracovníků. Údaje zpracovávané v elektronické podobě a s tím související systémy i aplikace byly popisovány za součinnosti interního zástupce za IT. Jak poukázaly předchozí kroky datového auditu, organizace XY spolupracuje s externí IT společností, která zajišťuje softwarovou podporu několika používaných aplikací a webových stránek, zároveň má však organizace svého interního zástupce za oblast IT.

Využívané servery i záložní zdroje jsou umístěny v servrovně, jedná se o samostatnou uzamykatelnou místnost s omezeným přístupem z důvodu bezpečnosti, zajištění snazší správy i údržby. Popsaný stav představuje vysoké bezpečnostní riziko, neboť server a záložní zdroj mají být odděleny pro případ havárie. Správu nad serverem má již zmiňovaná externí IT společnost. Organizace má všechny přístupy pod hesly, kdy každé z hesel se skládá z několika znaků, musí obsahovat velká i malá písmena a číslice, avšak nedochází k pravidelné obměně hesel, tj. daná hesla zůstávají v nezměněné podobě po neomezenou dobu. Dále je využívána antivirová a internetová ochrana prostřednictvím antivirového programu, kde dochází k automatickým pravidelným aktualizacím. Webové stránky mají ochranný certifikát, přístup z interních zaměstnanců má pouze vedení organizace včetně zástupce za IT a v omezené míře referent studijního odd., prostor webových stránek poskytuje externí IT společnost.

Archivace a likvidace dat, v případě tištěných dokumentů se řídí vnitřním spisovým a skartačním řádem organizace, velké množství údajů se ale nachází v elektronické podobě. Podmínky pro archivaci a odmazávání emailové komunikace nejsou nijak stanoveny, nutno podotknout, že primární komunikace související s hlavní činností organizace probíhá přes systém Bakaláři. V tomto systému jsou velmi omezeny přidělená práva a přístupy, jakmile žáci přestanou být oficiálně studenty organizace, pedagogové se k jejich údajům nedostanou. Pravidelná likvidace osobních údajů není nastavena ani pro webové stránky organizace. Ostatní IT systémy využívané organizací XY mají vymezeny podmínky pro archivaci a likvidaci dat.

Organizace disponuje kamerovým systém se záznamem. Za instalaci i správu systému zodpovídá externí IT společnost. Přístup k danému systému má z interních zaměstnanců vedení organizace a správce budovy. Celkem je v prostorách organizace instalováno 33 kamer, tyto kamery zabírají pouze jednotlivé vstupy do budov, chodby a průchody v rámci budov. Kamerový záznam je bez zvuku a doba jeho uložení jsou 4 dny, tato doba je zvolena s ohledem na možné svátky a dny volna. Na kamerový systém v prostorách organizace upozorňují příslušné informační cedule umístěné u vstupů do prostor organizace, viz příloha 5 Obrázek 1. Kamerový systém je provozován na základě oprávněného zájmu z důvodu bezpečnosti a ochrany majetku, podnětem jsou případy hlášení drobných krádeží v rámci prostor s osobními skřínkami studentů a pohyb nepovolaných osob. Jak bylo naznačeno výše, není evidován záznam, který by dokládal provedení balančního testu v souvislosti s provozováním kamerového systému.

Z rozboru bezpečnosti dat jsou patrné nedostatky v jejím obstaráváním. V nastavených postupech jsou opomíjeny procesy věnující se uchovávání, archivaci a likvidaci dat, systém heslové politiky není dotažen, absentuje balanční test ke kamerovým záznamům a k nim informační cedule nejsou v porovnání s výstupy z teoretické části dostatečné. Systém bezpečnosti a ochrany osobních údajů v organizaci si vyžaduje celkově podrobit revizi, o tom vypovídají i výsledky z dotazníkového průzkumu mezi zaměstnanci, kdy byly shledány mezery ve znalostech respondentů zejména v oblasti zajišťování bezpečnostních opatření a ochrany dat.

6. Krok – shrnutí GAP analýzy

Závěrečným krokem a nejdůležitější částí GAP analýzy je její shrnutí, tedy popis nesouladů s GDPR, po kterém následuje stanovení návrhu možných opatření k odstranění identifikovaných mezer. V souvislosti s tím je potřeba ozřejmit současný a požadovaný stav a upřesnit akceptovatelnou mezeru mezi těmito stavy. Současný stav je popsán v základních bodech v subkapitole 3.1.2 Současný stav dodržování povinností GDPR v organizaci, dále se současnému stavu věnuje i subkapitola 3.1.3 Datový audit – GAP analýza v krocích 1-5. V případě požadovaného stavu je vycházeno z teoretické části ze subkapitoly 2.1.2 Povinnosti správců údajů a mezi reálným a plánovaným stavem není přijatelná ani povolena žádná mezera. Pro naplnění souladu s GDPR je potřeba napravit níže uvedené nedostatky:

Pověřenec pro ochranu osobních údajů dostatečně neplní své náležitosti – na základě provedeného výzkumu v subkapitole 3.1.2 Současný stav dodržování povinností GDPR v organizaci se doporučuje zajištění nového pověřence z řad interních zaměstnanců.
Nekompletní záznamy o činnostech zpracování osobních údajů – nutnost zapracování chybějících procesů týkajících se školní jídelny, aktivit 1-4 a některých činností studijního oddělení a archivu do záznamů o činnostech zpracování osobních údajů. Vstupním podkladem jsou vyplněné dotazníky, viz příloha 4 Dotazník 2 – Náhled vyplnění.
Neověřování zpracovatelů včetně smluvních doložek – nastavení procesu ověřování zpracovatelů před podpisem smlouvy a vytvoření typizovaného dodatku k ochraně osobních údajů, který bude podepisován v rámci zpracovatelských smluv. Zajištění dodatků ve 4 probíhajících smluvních vztazích. Dále s ohledem na GDPR ošetřit smlouvy k praktickému vyučování studentů ve firmách s využitím standardizovaných dodatků.
Zamezení nezákonného zpracovávání údajů – okamžité pozastavení zpracovávání údajů: zdravotní pojišťovna a číslo občanského průkazu. Důkladné informování dotčených pracovníků o změně zpracovávání, případné převedení osobních údajů pod zákonný důvod a dodatečné zajištění souhlasů u nadále zpracovávaných údajů.
Dochází k nadbytečnému zpracovávání osobních údajů – okamžité pozastavení zpracovávání identifikovaných nadbytečných osobních údajů ve 3 činnostech, důkladné informování dotčených pracovníků o změně zpracovávání a přijetí potřebných opatření. Doporučuje se nastavit postup, který bude ošetřovat zpracovávané osobní údaje u nově vzniklých činností tak, aby nedocházelo k jejich nadbytečnému shromažďování a zpracovávání.
Zabránění nadbytečnému vyžadování souhlasů – okamžité zamezení vyžadování 3 identifikovaných nadbytečných nebo neupřesněných souhlasů, je nutná úprava, odstranění či převedení pod jiný zákonný důvod. Dále se navrhuje nastavit postup pro zpracovávání udělených i neudělených souhlasů. Dle vyjádření Janečkové (2020, s. 391-399) se doporučuje formulář pro souhlasy žáků se zpracováním osobních údajů upravit s ohledem na vyjádření samotného studenta a zákonný zástupce informativně stvrdí svým podpisem.
Neplnění informační povinnost u 6 vykonávaných činností/procesů – zajištění informování subjektů údajů o zpracovávání jejich osobních údajů a nastavení procesu, který bude zajišťovat splnění informační povinnosti v případě vzniku nových procesů.
Absence doby uchovávání osobních údajů u 10 činností – aktualizace spisového a skartačního řádu organizace, doplnění identifikovaných chybějících položek, stanovení

procesu pro archivaci a odmazávání údajů získaných v rámci emailové komunikace a webových stránek a seznámení zaměstnanců s těmito náležitostmi.
Omezení procesu řízení bezpečnostních incidentů – zaměstnanci jsou povinni všechny bezpečnostní incidenty hlásit pověřenci pro ochranu osobních údajů, další postup pro řízení těchto situací není stanoven. V souvislosti s tím je potřeba definovat odpovědnosti a proces řízení vzniklých incidentů, proces ohlašování porušení zabezpečení osobních údajů ÚOOÚ a subjektům údajů a s celým procesem řízení bezpečnostních incidentů obeznámit všechny zaměstnance organizace. Dále se doporučuje stanovit plán reakcí na možné bezpečnostní incidenty a vymezit zvláštní dokument věnující se bezpečnosti.
Nedokonalost procesu analýzy rizik – nastavení procesu pravidelného posuzování a vyhodnocování rizik v jednotlivých činnostech, ve kterých se zpracovávájí osobní údaje.
Informační cedule o kamerovém systému nejsou dostačující – zajistit doplnění těchto informací: kamerový systém se záznamem, správce, zpracovatel, kontaktní osoba, účel, práva subjektů údajů, předávání třetím stranám, doba uchování + odkaz na další informace vztahující se k využívanému kamerovému systému. V souvislosti s tím je třeba vytvořit a zveřejnit souhrnné informační sdělení uvedené například na webových stránkách organizace.
Neexistence balančního testu – zajištění balančního testu k využívání kamerového systému.
Nepřítomnost DPIA – zajištění DPIA u zpracování s vysokým rizikem pro práva a svobody fyzických osob. V případě 2 zaznamenaných činností představujících vysoké riziko na základě dotazníků vyhodnocených odpovědnými vedoucími v rámci datového auditu se doporučuje provést prvotní DPIA posouzení dle pokynů WP248.
Neúplné znění vnitřní směrnice – vnitřní směrnice musí být doplněna o organizační opatření související s aktivitami 2-4. S ohledem na nedostatečné množství uzamykatelných skříní, musí být specifikováno, které dokumenty mají být do nich ukládány. V rámci směrnice se doporučuje zahrnout i pravidla pro výkon práv subjektů údajů, obeznámit s nimi zaměstnance a ve směrnici odkázat na všechny předpisy upravující systém ochrany osobních údajů, tak aby byla zajištěna přehlednost všech podkladů vztahujících se k dané problematice. Dále se doporučuje uvádět jmenné seznamy studentů ve třídách s využitím iniciálů.
Neproškolování zaměstnanců a jejich seznamování s vnitřními předpisy – je nezbytné zajistit proškolení zaměstnanců v oblasti ochrany osobních údajů, jejich seznámení s příslušnými směrnicemi a stanovení plánu, dle kterého budou zaměstnanci průběžně proškolování, seznamováni s potřebnými změnami a novými pracovními postupy či směrnicemi.
Neúplnost podkladů evidujících: stížnosti, souhlasy se zpracování osobních údajů, uplatnění práv subjektů údajů, vzniklé bezpečnostní incidenty, nahlédy do kamerových záznamů nebo předané a zpracovávané osobní údaje zpracovateli – ačkoli se nejedná o povinné evidence, jejich vedení je doporučeno, zejména z důvodu kontrol a přehlednosti pro danou organizaci. Agendu evidencí se navrhuje předat pověřenci pro ochranu osobních údajů, který by měl být vždy informovanou osobou, v daných případech.
Nejsou nastaveny možnosti usnadňující výkon práv subjektů údajů – doporučuje se poskytnout subjektům údajů standardizované formuláře pro snadnější uplatnění jejich práv.
Absence kontrol a kontrolních mechanismů – navrhuje se nastavení procesu pravidelných kontrol, které budou sledovat dostatečné zajišťování ochrany a bezpečnosti osobních údajů ať již ze strany zaměstnanců, tak i ze strany zpracovatelů osobních údajů.

Celkem bylo zmapováno 18 oblastí, které obsahují nedostatky. Díky identifikaci výsledků GAP analýzy a v součinnosti s datovým auditem byla navrhnuta doporučení ke změnám včetně opatření, jak systematicky nedostatky napravit. V návrzích je zohledněn ekonomický přínos, především v zajištění pověřence pro ochranu osobních údajů z řad interních zaměstnanců. Doporučená opatření představují výchozí bod nezbytné transformace k naplnění náležitostí stanovených GDPR, její vyšší přidaná hodnota spočívá v neopomíjeném nastavení procesů, které zohledňují dodržování povinností v souladu s GDPR i v budoucnosti. Získané výsledky

byly odprezentovány zástupcům vedení organizace XY. Na základě komplexního shrnutí GAP analýzy, detailního vymezení kroků pro nápravu zjištěných nedostatků a zdůraznění požadavků vedení organizace, bylo rozhodnuto přistoupit k vypracování návrhu projektu transformace implementovaného GDPR do stávajících procesů organizace.

3.2 Návrh projektu pro změnové řízení

Hlavním cílem diplomové práce je tvorba návrhu projektu transformace implementovaného GDPR do procesního řízení vybrané organizace. V návrhu projektu dojde k odstranění identifikovaných nesouladů z GAP analýzy. Projekt je navržen tak, aby došlo k požadované nápravě a zároveň aby se předešlo i dalším možným nesouladům do budoucna. Vedení organizace XY stanovilo několik parametrů, které jsou pro akceptaci návrhu projektu stěžejní. Z hlediska času bude projekt pracovat s termínem 1.9.2023, který je nejpozději přípustným datem pro dokončení projektu, tj. návrh projektu i jeho realizaci je třeba zajistit do začátku nového školního roku, důvodem je zamezení chybného zpracování osobních údajů i u nově příchozích subjektů. Celkové náklady na projekt jsou vyčleněny ve výši 50 000 Kč. Pracovníkům bude náležet odměna maximálně 140 Kč za 1 hodinu odpracovaného času a lze vyčlenit nanejvýš 4 pracovníky, kteří mohou projektu věnovat maximálně 4 hodiny denně.

Cílem samotného projektu je napravit identifikované nesoulady s GDPR v procesech organizace tak, aby všechny činnosti a procesy, ve kterých dochází ke zpracovávání osobních údajů, byly v souladu s tímto nařízením a organizace XY nebyla vystavena riziku v podobě hrozících sankcí. V první řadě je důležité stanovit jednotlivé činnosti projektu a tím vymezit jeho rozsah a vypracovat časový harmonogram. Závěrem bude provedena kalkulace nákladů a analýza rizik pro zhodnocení projektu. Konečný návrh bude představen vedení organizace.

3.2.1 Hlavní parametry návrhu projektu

Aby byl vypracovaný návrh projektu akceptován, musí časový harmonogram projektu korespondovat s realizací nejpozději do 1.9.2023 a náklady projektu nesmí přesáhnout výši 50 000 Kč, což zároveň představuje jistá omezení pro návrh i realizaci projektu. Prvním důležitým aspektem návrhu projektu je vymezení jeho rozsahu a stanovení časového harmonogramu, k tomu poslouží výsledky z GAP analýzy, viz subkapitola 3.1.3 Datový audit. Na začátek jsou vymezeny jednotlivé činnosti pro naplnění projektu, k těmto jednotlivým úkonům je přidělena doba trvání dané činnosti (ve dnech), a dále činnosti, které předchází dané aktivitě a vážou se na ni. Na základě těchto dat bude možné určit dobu trvání projektu. Přehled jednotlivých činností včetně těch předcházejících a délky trvání daných aktivit znázorňuje Tabulka č. 7.

Tabulka 7: Přehled činností projektu

Činnost	Popis činnosti	Doba trvání (dny)	Předchozí činnost
A	Zajištění nového DPO a agendy vedení evidencí	5	-
B	Revize záznamů o činnostech zpracování	3	A
C	Nastavení procesu ověřování zpracovatelů. Tvorba standardizovaných dodatků a zajištění 4 dodatků k probíhajícím smlouvám.	6	A, B
D	Zamezení zpracovávání identifikovaných nadbytečných nebo nezákonných osobních údajů včetně příslušných opatření	2	A, B

E	Revize formulářů pro udělení souhlasů se zpracováním osobních údajů včetně příslušných opatření	5	A, B
F	Zajištění informační povinnosti o zpracovávání osobních údajů u 6 identifikovaných činností	1	A, B, C, D, E
G	Revize spisového a skartačního řádu	1	A, B, F
H	Nastavení procesu řízení bezpečnostních incidentů, plán reakcí a vymezení samostatného dokumentu	3	A, B, C, D
I	Nastavení procesu analýzy rizik	4	A, B, H
J	Revize informačních cedulí o kamerovém systému	1	A
K	Provedení balančního testu ke kamerovému systému	3	A, B, J
L	Zajištění prvotního DPIA dle pokynů WP248	1	A, B, I, K
M	Vytvoření formulářů pro uplatnění práv subjektů údajů	1	A
N	Revize vnitřní směrnice	2	A, B, C, G-I, L, M
O	Proškolení všech zaměstnanců o ochraně osobních údajů a jejich seznámení s veškerými změnami a nastavení školícího plánu	2	A, C-L, N
P	Nastavení kontrolních mechanismů	2	H, I, L, N, O

Zdroj: (vlastní zpracování, 2023)

Z Tabulky č. 7 je zřejmé, že rozsah projektu tvoří 16 činností, z GAP analýzy bylo identifikováno 18 oblastí s nedostatky a některé z nich se podařilo pro rozsah projektu sjednotit. Stěžejním bodem je zajištění nového pověřence pro ochranu osobních údajů a revize záznamů o činnostech zpracování. Závěrečnými, avšak ne méně podstatnými úkoly, které na sebe i na předchozí činnosti úzce navazují jsou revize vnitřní směrnice, proškolení zaměstnanců a nastavení kontrolních mechanismů. K délce trvání jednotlivých úkolů projektu dospěli zainteresovaní pracovníci odhadem času na základě jejich detailního rozboru a zkušeností, k tomuto odhadu byla vypracována také škála pro zobrazení logického záměru, viz příloha 2 Tabulka 8. V souvislosti s realizací projektu běží na pozadí další úkoly, kterými jsou řízení projektu, průběžné kontroly plnění jednotlivých úkolů, dodržování stanoveného harmonogramu, rozpočtu a veškerá komunikace potřebných náležitostí. Sled těchto úkolů není zahrnut v Tabulce 7, nýbrž jej znázorňuje až Tabulka 9. K těmto úkolům se doporučuje přistupovat dle nástroje 10, viz příloha 5 Obrázek 2, který představil Novák (2016). Za účelem identifikace významnosti, postupu i logického odhadu času jednotlivých úkolů byl proveden popis detailního rozboru uvedených činností z Tabulky 7.

Primárním úkolem je zajištění nového pověřence pro ochranu osobních údajů, který mimo jiné bude zajišťovat agendu vedení evidencí, tj. vedení přehledu stížností, uplatněných práv subjektů údajů, udělení souhlasů se zpracováním osobních údajů atd. Nově jmenový DPO bude také zajišťovat školení zaměstnanců. Na základě posouzení v subkapitole 3.1.2 Současný stav dodržování povinností GDPR v organizaci vychází popis úkolu z doporučené varianty, kdy je pro tuto roli stanoven interní zaměstnanec, který absolvuje potřebné školení. Dále je potřeba zajistit s tímto pracovníkem a v souvislosti s nově přidělenou agendou, podepsání dodatku ke smlouvě o nové funkci a ošetřit potřebnou mlčenlivost. V pozadí tohoto úkolu je potřeba rozvázat smlouvu s dosavadní externí firmou, vzhledem k dostatečnému neplnění smluvních

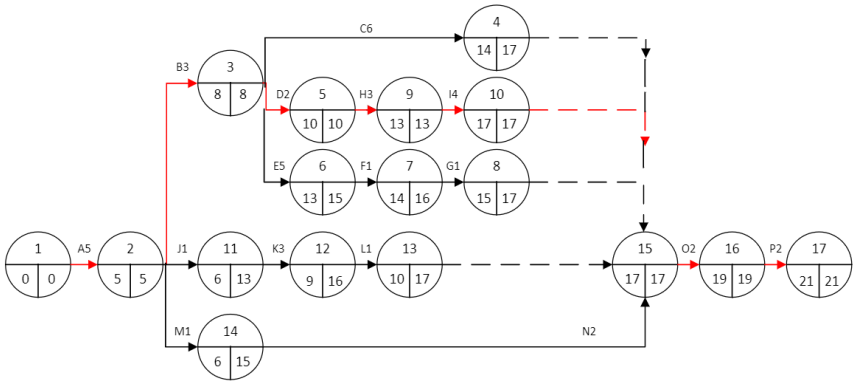
podmínek není v zájmu organizace XY čekat se zajišťením nového pověřence na ukončení stávajícího smluvního vztahu. Po zajištění nového DPO je možné přejít k revizi záznamů o činnostech zpracování. Podkladem pro tyto záznamy jsou vyplněné dotazníky z datového auditu, jejich vzor je k náhledu v příloze 4 Dotazník 2. Zároveň je nutné doplnit přesnou zákonnost zpracování osobních údajů, tj. musí být odkázáno na konkrétní nařízení a paragrafy zákonů. V revizi záznamů také nemůže být opomenuto uvedení jména a kontaktních údajů nového DPO. Zrevidované záznamy musí být předány odpovědným osobám daných úseků pro jejich přehled a kontrolu v případě opomenutí nebo potřebné změny. Zajištění tohoto úkolu je počátečním bodem, na který navazují další činnosti projektu. Proces ověřování zpracovatelů, tvorba standardizovaných dodatků a dodatečné zajištění několika dodatků je přidělen do gesce vedoucího pracovníka. Zásadním pro tento úkol je především poslední uváděný bod, a to zajištění dodatků k již běžícím smlouvám. V tomto případě je stěžejní jednotlivé zpracovatele zkontaktovat a zajistit s nimi podepsání příslušných dokumentů. Jako vzor pro vytvoření standardizovaného dodatku poslouží ukázka ve stručném návodu přímo od MŠMT (2017). Pro nastavení procesu ověřování zpracovatelů může být nápomocen výběr možných nástrojů od Nonnemanna (2018, s. 68-69). Úkol zamezení zpracovávání nadbytečných nebo nezákonných osobních údajů je přidělen pracovníkovi vedení zajišťujícího i oblast IT. Důvodem je evidence údajů souvisejících s tímto úkolem i v rámci elektronických systémů. Přičemž je nutné zamezit možnosti zpracovávání těchto údajů, případně vybrané údaje nahradit akceptovatelnějšími variantami, a zajistit podchycení této změny v rámci systémů i případných tištěných dokumentů. Celkem se jedná o zamezení 2 údajů v 1 systému, 2 textové úpravy ve fyzicky zpracovávaných dokumentech s elektronickým podkladem a 1 úprava v rámci online formuláře. Zároveň by mělo dojít k odstranění či anonymizaci údajů, které doposud byly nepřijatelně evidovány bez zákonného oprávnění, případně je třeba zajistit dodatečné oprávnění k nadálému zpracovávání těchto údajů. Revizi je třeba podrobit i formuláře souhlasů se zpracováním osobních údajů, a to jak pro žáky, tak i pro zaměstnance. Nadbytečně vyžadované souhlasy je třeba z formulářů vyřadit, případně převést pod jiný zákonný důvod. Tento úkol je propojen i s činností D, kdy pro případné pokračující zpracování vybraných osobních údajů bude nutné zajistit jejich souhlasy, tyto údaje budou naopak zahrnuty do formuláře k ostatním souhlasům. S těmito úkoly se pojí i úprava záznamů o činnostech zpracování. S ohledem na časovou realizovatelnost nápravy budou upravené formuláře předány k podpisu zaměstnancům a v případě žáků dojde k pozastavení zpracování osobních údajů na základě poskytnutých souhlasů. Následně podle již nastaveného procesu ve směrnici, dojde k předání nových formulářů pro poskytnutí souhlasů všem žákům začátkem nového školního roku bez ohledu na ukončení projektu. Tento úkol zahrnuje také nastavení procesu zpracovávání udělených i neudělených souhlasů, tj. pokud nějaký student neudělí souhlas například k zveřejňování fotografií, musí být pro tyto situace stanoven postup. V návaznosti na doposud uvedené úkoly je nutné zajistit informační povinnost o zpracovávání osobních údajů u 6 identifikovaných činností. Pro zajištění těchto informací bude nápomocno jako vzor již organizací využívané informační sdělení v rámci aktivity 1, u které je tato povinnost řádně splněna. Zároveň potřebné informace budou získány z revidovaných záznamů o činnostech zpracování. Dále je nutné nastavit proces, který v případě vzniku nových procesů bude zajišťovat splnění informační povinnosti. Úkol bude kompletně splněn, jakmile dojde k nastavení procesu a veřejnému zpřístupnění informačních sdělení dotčeným subjektům údajů. Na zajištění informační povinnosti navazuje revize spisového a skartačního řádu. Tento předpis je potřeba doplnit o 10 identifikovaných chybějících položek. Vstupními podklady pro tento úkol jsou záznamy o činnostech zpracování a informace o zpracovávaných údajích z předchozí činnosti. V souvislosti s tímto úkolem je vyžadováno stanovení procesu, který bude vymezovat postup pro archivaci a odmazávání údajů zpracovávaných v rámci emailové komunikace a webových stránek. Zajištění procesu řízení bezpečnostních incidentů je též přiděleno

pracovníkovi vedení, jenž zároveň zašťituje oblast IT. V nastaveném procesu musí být definovány kroky k řízení vzniklých incidentů a k jednotlivým krokům přiděleny odpovědnosti. Totéž je potřeba vymezit i pro ohlašování porušení zabezpečení osobních údajů ÚOOÚ a subjektům údajů. Tento úkol v sobě zahrnuje i přípravu plánu reakcí na možné bezpečnostní incidenty a zajištění samostatného dokumentu. Tento dokument je výhradně věnován oblasti bezpečnosti a ochraně osobních údajů, vychází z aktuálně platných předpisů, přičemž zajišťuje jejich sjednocení. Navazujícím úkolem je nastavení procesu analýzy rizik, kdy je v organizaci potřeba pravidelně posuzovat a vyhodnocovat rizika v rámci činností, ve kterých dochází ke zpracovávání osobních údajů. S tím se pojí určení metody, škály rizik, četnost vyhodnocování, opatření k jednotlivým vyhodnocením i stanovení odpovědností. Je důležité nastavit proces tak, aby v případě vzniku nových procesů došlo k včasnému podchycení vysokých rizik pro práva a svobody fyzických osob, s tím provedení DPIA a případné podstoupení dalších kroků. Součástí tohoto úkolu je požadováno prvotní posouzení a vyhodnocení rizik. Podklad k tomuto posouzení je obsažen v rámci vyplněných dotazníků jejichž vzor přináší příloha 4 Dotazník 2. Dalším z úkolů je zajištění revize informačních cedulí upozorňujících na kamerový systém v budovách organizace. Tyto cedule musí být doplněny o následující údaje: jedná se o kamerový systém se záznamem, kdo je správce, kdo je zpracovatel, uvedení pověřence pro ochranu osobních údajů, jaký je účel, jaká jsou práva subjektů údajů, zda jsou údaje předávány třetím stranám, jaká je doba uchování záznamů. Dále musí být odkázáno na ostatní informace vztahující se k využívanému kamerovému systému, pro tento případ je třeba informace souhrnně uvést na webových stránkách organizace. Navazujícím úkolem je provedení balančního testu ke kamerovému systému. Pro jeho zajištění je doporučeno využít ukázku náležitostí, viz příloha 5 Obrázek 3, která uvádí, co má balanční test obsahovat. V zásadě jde o důkladné posouzení oprávněnosti zpracovávání daných osobních údajů s ohledem na práva subjektů údajů. Následuje zajištění DPIA vedoucím pracovníkem dle pokynů WP248. Na tyto pokyny je odkázáno v seznamu literatury diplomové práce a jejich posouzením musí projít všechny činnosti, které byly v rámci dotazníku, viz příloha 4 Dotazník 2 vyhodnoceny s vysokým rizikem pro práva a svobody fyzických osob. Totéž platí i pro další činnosti, které představují vysoké riziko, a byly identifikovány v rámci první provedené analýzy rizik. Pakliže výstup DPIA přinese vysoké riziko, je nutné přijmout další kroky, a to v podobě ohlášení ÚOOÚ. Dalším z úkolů je vytvoření formulářů, které budou usnadňovat subjektům údajů uplatnění jejich práv. V rámci tohoto úkolu má dojít k vytvoření standardizovaných formulářů pro každé z práv subjektů údajů a jejich umístění na webových stránkách organizace, kde budou volně přístupné všem zájemcům. Formuláře by měly obsahovat minimálně identifikační údaje subjektů údajů, předmět žádosti, případně zdůvodnění žádosti a samozřejmě datum a podpis subjetu údajů, jenž žádost podává. Jedním z posledních úkolů, který navazuje hned na několik předchozích činností je revize vnitřní směrnice. Tento vnitřní předpis je třeba doplnit o organizační opatření souvisejících s aktivitami 2-4, vymezit podklady, které musí být ukládány do uzamykatelných skříních, uvést pravidla pro výkon práv subjektů údajů a dále odkázat na všechny předpisy upravující ochranu osobních údajů, tak aby byla zajištěna předhlednost a jednotnost všech podkladů vztahujících se k této oblasti. K popisu výkonu práv subjektů údajů poslouží informační memorandum, kde jsou potřebné náležitosti uvedeny, zároveň bude doplněno o informace k nově zavedeným standardizovaným formulářům. Další ze závěrečných činností je proškolení všech zaměstnanců v oblasti bezpečnosti a ochrany osobních údajů a jejich seznámení s veškerými změnami a příslušnými předpisy. Tento úkol je možné realizovat až v momentě, kdy budou všechny předpisy a potřebné procesy nastaveny, aby mohlo dojít k předání kompletních informací zaměstnancům. Součástí je i nastavení školícího plánu, který bude stanovovat periodu školení i postup pro seznamnování pracovníků s aktuálními změnami, novými postupy i předpisy. Závěrečným úkolem projektu je nastavení kontrolních mechanismů, které budou zajišťovat

kontrolu stanovených předpisů, nastavených opatření a obecně bude docházet k monitoringu dodržování souladu s GDPR. Kontrola bude zaměřena nejen na zaměstnance, nýbrž i na zpracovatele osobních údajů, bude zahrnovat osobní údaje v tištěné i elektronické podobě a její průběh bude směřován do pravidelných intervalů. To vše je potřeba specifikovat v rámci předpisu upravujícího nastavené kontrolní mechanismy včetně stanovení odpovědností a postupu v případě identifikování nedostatků a nesouladů.

Výše uvedený rozbor jednotlivých úkolů v rámci projektu byl ve spojistosti s vypracovanou škálou, viz příloha 2 Tabulka 8, nápomocen k vymezení doby trvání daných činností a k určení jejich významnosti, posloupnosti i k rozřazení jednotlivých úkolů přiděleným pracovníkům projektu. Zpracovaná a výsledná data z Tabulky 7 představují podklad pro sestavení uzlově definovaného orientovaného síťového grafu. Na základě tohoto grafu lze stanovit nejkratší dobu trvání projektu a určit jeho kritickou cestu. Vypracovaný síťový graf projektu zobrazuje Diagram 5.

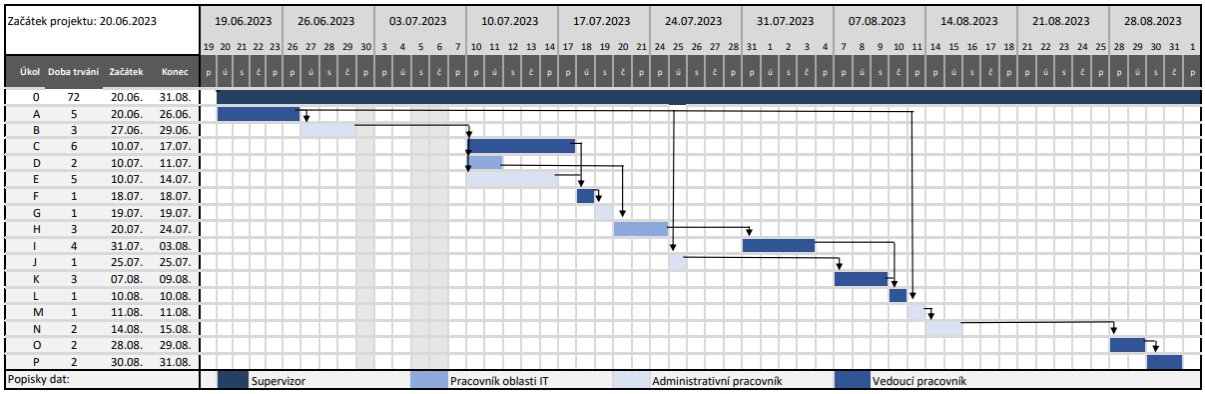
Diagram 5: Síťový graf činností projektu



Zdroj: (vlastní zpracování, 2023)

Jak zobrazuje síťový graf v Diagramu 5, nejkratší možná doba pro realizaci projektu představuje 21 dní. Červenou linkou je v rámci grafu vyobrazena kritická cesta, u těchto činností nevzniká žádná časová rezerva, jinak řečeno, zdržení počátku daného úkolu nebo prodloužení doby jeho trvání ovlivní termín ukončení projektu. Toto grafické vyobrazení slouží pouze jako možná ukázka nejkratší doby projektu, avšak nutno zdůraznit, že organizace XY nedisponuje takovým množstvím zdrojů, které by zvládly realizovat projekt v tomto čase a některé vybrané činnosti jsou ovlivněny i dalšími faktory. Pro znázornění reálného časového harmonogramu včetně dostupných zdrojů a časových rezerv byl zvolen Ganttův diagram, který vychází z dat Tabulky 7, zároveň je doplněn o potřebné informace poskytnuté organizací, zpracovaný diagram zobrazuje Tabulka 9.

Tabulka 9: Ganttův diagram činností projektu doplněný o zdroje a časové rezervy



Zdroj: (vlastní zpracování, 2023)

Z Tabulky 9 vyplývá, že průběh projektu je plánován v období 20.6. – 31.8.2023, to představuje 72 dnů, resp. 52 pracovních dnů v kalendářním roce. Vzhledem k stanovenému nejzazšímu termínu 1.9.2023, kdy nejpozději musí být projekt splněn je zřejmé, že na kritické cestě leží činnosti O a P, u kterých nemůže dojít ke zpoždění, zároveň tyto činnosti s ohledem na čerpání dovolených nelze realizovat ani v dřívějším čase. Totéž platí i pro prvotní činnosti A a B, které se nemohou opozdit. Grafické vyobrazení poukazuje na 4 přidělené lidské zdroje k jednotlivým úkolům projektu, v rámci grafu jsou tito pracovníci pro jednotlivé činnosti odlišeny barevně. Vzhledem k jejich pozicím a specializaci v rámci organizace se předpokládá jejich aktivita pouze na vyhrazených úkolech, to však nevylučuje návaznost jednotlivých činností a předávání si potřebných podkladů mezi s sebou. Souvislá činnost na projektu je vyhrazena pouze pro supervizora, který bude mít projekt na starosti z hlediska řízení a koordinace úkolů a kompletní komunikace. Vypracovaný harmonogram počítá s časovou rezervou, která bere v úvahu jiné neodkladné pracovní činnosti, dny volna i nahlášené dovolené jednotlivých pracovníků, kteří se na projektu budou podílet. Díky tomu je rozplánování projektu přesnější, zohledněný detail pomáhá supervizorovi lépe řídit a koordinovat jednotlivé aktivity projektu a celkově usnadňuje provedení potřebné transformace.

3.2.2 Zhodnocení přínosů transformace řízení

Pro zhodnocení projektu je v souvislosti s transformací implementovaného GDPR do procesního řízení organizace provedena analýza rizik a kalkulace nákladů. Na začátek bylo primární vyhodnocení rizik, která s sebou daný projekt přináší. V souvislosti s tím bylo nutné určit zdroj rizika, identifikovat nebezpečí, vyhodnotit celkové riziko a navrhnout bezpečnostní opatření, která dané riziko sníží, či zcela eliminují. Provedená analýza rizik je znázorněna v tabulce 10.

Tabulka 10: Analýza rizik návrhu projektu

	Zdroj rizika	Identifikace nebezpečí	Hodnocení závažnosti rizika				Bezpečnostní opatření
			P	Z	H	R	
Transformace implementovaného GDPR do změnového řízení	Časové zpoždění projektu	Chybné zpracování osobních údajů dalších subjetů údajů	2	3	3	18	Důkladná příprava časového harmonogramu
	Chybná vstupní data projektu	Neidentifikování všech nesouladů s GDPR	3	4	4	48	Důkladné vymezení a kontrola vstupních dat projektu, nastavení procesů a kontrolních mechanismů průběžně hodnotících soulad s GDPR.
	Neproškolení zaměstnanci	Únik osobních údajů	3	4	4	48	Naplánované školení a jeho důkladné provedení
	Chybná transformace	Nedostatečné nebo chybné pochopení povinností GDPR	3	4	4	48	Důkladné nastudování GDPR a příslušných podkladů
	Nedostatečné informování změny	Nepřijetí změnového řízení ze strany zaměstnanců	3	3	3	27	Vhodně zvolená komunikace projektu směrem k zaměstnancům

Zdroj: (vlastní zpracování, 2023)

Pro analýzu rizik v tabulce 10 byla zvolena metoda PZH, která pracuje s 3 složkami rizika, ty jsou vyhodnocovány na stupnici od 1 do 5, a škály pro vyhodnocování těchto složek jsou

znázorněny v příloze 5 Obrázek 4. V rámci analýzy rizik bylo identifikováno pro daný projekt 5 rizik, kdy nejvyšší hodnota ukazatele míry rizika je 48 a tato hodnota vyšla u 3 rizik z 5. Ačkoli tato hodnota spadá do mírného rizika, je blízko na rozhraní s nežádoucím rizikem, a proto je nutné zajistit odpovídající bezpečnostní opatření, která budou riziko snižovat případně udržovat na přijatelné úrovni. První z rizik s vyšší hodnotou ukazatele je neodhalení všech nesouladů s GDPR. Pakliže bude projekt postaven na chybných nebo nedostatečných vstupních datech, a i přes toto změnové řízení nebude dosaženo souladu, vystavuje se organizace hrozbě možných sankcí. Aby se dosáhlo snížení rizika, je důležité důkladně projít vstupní data a nastavit procesy a kontrolní mechanismy, které budou průběžně hodnotit dodržování souladu s GDPR. Únik osobních údajů v důsledku neproškolených zaměstnanců je dalším rizikem, které je potřeba snížit, k tomu poslouží důkladně provedené školení a obeznámení všech zaměstnanců. Posledním z uvedených rizik je nedostatečné nebo chybné pochopení povinností vyplývajících z GDPR, které může být jednou z příčin nesplnění povinností s dopadem možných sankcí. Pro snížení tohoto rizika je stěžejní důsledné prostudování GDPR a příslušných podkladů.

Jak bylo zmíněno v úvodu této subkapitoly, pro zhodnocení projektu je třeba dále provést kalkulaci nákladů. Projekt byl navržen s ohledem na co nejnižší náklady, avšak zároveň tak, aby nebyl ohrožen z hlediska kvality. Pro naplnění projektu jsou vyhrazeni 2 zaměstnanci, 3. zaměstnanec je zainteresován do 2 úkolů a po celou dobu projektu je k dispozici další zaměstnanec, který disponuje rolí supervizora, projekt bude řídit a dále vykonávat dohled nad plněním jednotlivých úkolů, dodržováním stanoveného harmonogramu, rozpočtu, bude zajišťovat veškerou komunikaci potřebných náležitostí a dle potřeby bude připraven pomoci zaměstnancům pracujícím na projektu. Projekt je záměrně cílen na období měsíců červenec, srpen, kdy v organizaci XY dochází k nižšímu vytížení všech pracovníků. V běžném pracovním režimu by byli pracovníci převedeni na jiné činnosti, nebo by byli nuceni čerpat dovolené, jejich pracovní náplň se v tomto období snižuje téměř o polovinu. Z tohoto důvodu je v rámci projektu počítáno s tím, že polovinu pracovní doby daného dne zainteresovaní zaměstnanci budou věnovat práci na projektu. I přes tuto skutečnost budou pro kompletní kalkulaci nákladů sledovány počty odpracovaných hodin přidělených pracovníků, kterým za strávený čas na jednotlivých úkolech projektu bude náležet odměna. V rámci projektu je třeba zajistit i nového pověřence pro ochranu osobních údajů, doporučený návrh projektu v tomto ohledu počítá se zaškolením interního pracovníka na tuto pozici a s tím souvisí i výlohy za pracovní cesty. Celkovou kalkulaci nákladů zobrazuje Tabulka č. 11.

Tabulka 11: Kalkulace nákladů návrhu projektu

Název nákladové položky	Doba trvání	Náklady celkem
Práce na projektu 1. zaměstnanec	96 hodin	13 440 Kč
Práce na projektu 2. zaměstnanec	52 hodin	7 280 Kč
Práce na projektu 3. zaměstnanec	20 hodin	2 600 Kč
Práce na projektu supervizor	57 hodin	7 980 Kč
Čas strávený na školení	16 hodin	2 240 Kč
Školení nového pověřence	-	13 310 Kč
Cestovné	-	1 000 Kč
Celkem	**-**	**47 850 Kč**

Zdroj: (vlastní zpracování, 2023)

Jak znázorňuje Tabulka 11, nejvyšší položku v nákladech představují odměny, jejichž výše byla přímo vedením organizace pro daný projekt stanovena na 140 Kč za hodinu. V návaznosti na Ganttův diagram v Tabulce 9 se předpokládá, že za každý vyznačený den přidělený pracovník odpracuje 4 hodiny na daném úkolu. Výjimku tvoří pouze zaměstnanec v roli supervizora a zaměstnanec účastnící se školení, které probíhalo po 2 celé dny. Doba trvání práce

na projektu supervizora byla získána na základě logického odhadu času. Předpokládá se, že supervizor stráví v průměru 1,5 hodiny s každým úkolem a řízením projektu stráví 3 hodiny za každý týden. Po tomto vyčíslení celková částka za odměny všech pracovníků představuje 33 540 Kč. Pro získání nákladů za školení nového pověřence pro ochranu osobních údajů ze zástupců zaměstnanců byl proveden průzkum trhu, jehož výsledky jsou uvedeny v příloze 2 Tabulka 12. Mezi jednotlivými variantami byla posuzována nejen cena, ale i průběh a výstup ze samotného školení. Jako nejvhodnější byla považována 1. nabídka od společnosti Tayllorcox, která nabízí školení prezenční formou, účastník získá nejen certifikát, ale i školící materiály, délka školení i cena odpovídají tzv. střední cestě a byly dohledány kladné reference. Při vyčíslení nákladů za cestovné se vycházelo z průměrné ceny za zpáteční jízdné od sídla organizace XY na místo školení včetně stravného, a to ve výši 500 Kč za 1 den. Celkové náklady projektu, jenž v sobě zahrnují odměny zaměstnanců, cestovné a školení 1 zaměstnance dle vyhodnocené nejvhodnější varianty jsou vyčísleny na 47 850 Kč. V rámci kalkulace nákladů nebyl záměrně uveden jeden specifický náklad, který s projektem vznikne, a tím je odměna zaměstnanci za funkci pověřence pro ochranu osobních údajů a s ní spojený výkon daných povinností. Vedení organizace předpokládá s výší odměny 1 500 Kč/měsíc v prvních měsících s možností navýšení po osvědčení daného zaměstnance a dle množství vykonávaných úkolů. Doposud organizace měsíčně hradí paušální částku externí firmě, tato částka převyšuje stanovenou odměnu zaměstnanci pověřeného nově funkcí DPO. Odměna internímu zaměstnanci za jeho novou funkci nepředstavuje pro organizaci další náklad, tato skutečnost může být dokonce vnímána jako úspornější a efektivnější varianta oproti současně vyplácené částce externí firmě.

Zhodnocení projektu lze zakončit shrnutím výše získaných výsledků. Jak vyplynulo z provedené analýzy rizik, projekt neohrožuje žádné nepřijatelné riziko, pouze 3 rizika se nachází na hraně intervalu mezi nežádoucím a mírným rizikem. Pro všechna identifikovaná rizika byla vymezena bezpečnostní opatření, pomocí kterých budou rizika postupně snižována nebo udržována na přijatelné úrovni. Celkové náklady projektu byly v rámci doporučené varianty vyčísleny na 47 850 Kč. V porovnání s rozpočtem projektu, který byl vedením organizace stanoven na 50 000 Kč, představuje uvedená částka mírnou rezervu. Do celkové kalkulace nebyla započítána výše měsíčně vyplácené odměny internímu zaměstnanci za výkon funkce pověřence pro ochranu osobních údajů, neboť nepředstavuje pro organizaci další náklad, ale úspornější variantu oproti současné paušální platbě externí firmě. Projekt je možné v důsledku uvedených zjištění označit za realizovatelný. Vypracovaný návrh projektu byl představen vedení organizace, včetně výsledků z provedených průzkumů trhu, viz příloha 2 Tabulky 5 a 12. Při prezentaci výsledků byl odprezentován doporučený návrh, který pracuje s variantou využití interního DPO z řad zaměstnanců a se školením od společnosti TAYLLORCOX, zároveň byly ozřejmeny i ostatní varianty výsledků průzkumů trhu pro ucelený pohled a možnost zvážení úpravy představeného návrhu. Ze strany organizace XY došlo k akceptaci doporučené varianty projektu transformace implementovaného GDPR do procesního řízení organizace, viz příloha 5 obrázek 5.

3.3 Vyhodnocení výsledků a přínosů

Závěrečná podkapitola je strukturována do dvou částí, v první z nich jsou blíže rozebrány a shrnuty získané výsledky z provedených výzkumů a v souvislosti s tím jsou zodpovězeny výzkumné otázky a hypotézy. Druhá část podkapitoly se věnuje zhodnocení přínosů dané práce, na které je hleděno z různých úhlů pohledu. V závěru je zdůrazněn další potenciál, který diplomová práce otevírá.

3.3.1 Diskuze výsledků

Na základě výstupů z kvalitativního výzkumu v podobě polostrukturovaného rozhovoru s ředitelem organizace a rozboru interních dokumentů byla zodpovězena 1. výzkumná otázka: *„Jakým způsobem jsou uplatňovány povinnosti vyplývající z GDPR v organizaci?“*

Vybraná organizace pro zajištění povinností plynoucích z GDPR využívá externí společnosti, která má dle smluvního ujednání zajišťovat výkon funkce pověřence pro ochranu osobních údajů, konzultační hodiny, preventivní bezpečnostní kontroly minimálně 1x ročně, školení pro vedoucí pracovníky a vedení potřebné dokumentace k ochraně osobních údajů. V případě potřeby jsou externí firmou dodávány organizaci XY standardizované formuláře, například souhlasy se zpracováním osobních údajů či dodatky ke smlouvám se zaměstnanci. Na organizaci XY zůstává již úprava obdržených formulářů do potřebné odpovídající podoby a implementace do procesů. Vybraná organizace v zajišťování povinností GDPR spoléhá na smluvní ujednání s externí firmou. Ze strany organizace nedochází ke kontrolám externí firmy, ani nedisponuje přehledem o podkladech, které za ni externí společnost vede a zpracovává. Tímto výčtem lze stručně shrnout odpověď na 1. výzkumnou otázku.

Získané výsledky z rozhovoru, rozboru interních dokumentů a ve spojistosti s výstupy z teoreticko-metodologické části pomohly ověřit hypotézu č. 1: *„Pokud organizace neprovádí pravidelné kontroly outsourcovaných služeb, nemůže se spoléhat na důkladné plnění stanovených náležitostí.“*

V souvislosti s výše zmíněnými metodami došlo k vypracovaní kontrolního checklistu, viz Tabulka 1 ke zhodnocení souladu dodržování požadavků vyplývajících z GDPR. Na začátek je třeba připomenout, že zajištění povinností plynoucích z GDPR pro organizaci vykonává externí společnost. Výsledky poukázaly, že v organizaci je stanovena funkce DPO (pověřenec pro ochranu osobních údajů), kterou zajišťuje externí firma, a jsou vypracovány vnitřní předpisy k ochraně a bezpečnosti osobních údajů. Naproti tomu vedení záznamů o činnostech zpracování není dostatečné, zpracovatelé nejsou ověřováni a smlouvy s nimi neobsahují potřebná ujednání o zpracování osobních údajů, neprobíhá školení zaměstnanců v dané problematice a nejsou vedeny evidence zaznamenávající uplatněná práva subjektů údajů, stížnosti, bezpečnostní incidenty apod. Posuzovaný kontrolní checklist obsahoval pouze základní body, které bylo v danou chvíli možné posoudit, například u zpracovávaných osobních údajů neprobíhalo ověření přesného vymezení účelů zpracování, správné definování zákonnosti zpracování nebo nutnost zajištění a provedení DPIA. I přes toto omezení byl výčet ověřovaných povinností pro prvotní zhodnocení plně dostačující. Tímto byl dle očekávání potvrzen nesoulad s GDPR v organizaci XY, a stal se tak podnětem k uskutečnění rozsáhlejšího výzkumu. Také bylo zkoumáno, které náležitosti nejsou externí firmou zcela nebo dostatečně zajišťovány na základě smluvního ujednání. V tomto ohledu byly identifikovány nekompletní záznamy o činnostech zpracování, absence školení vedoucích pracovníků, absence preventivních bezpečnostních kontrol a omezená konzultační činnost. Již v odpovědi na 1. výzkumnou otázku zaznělo, že organizace XY neprovádí kontroly externí firmy. Zjištěné skutečnosti potvrzují nedostatečné plnění outsourcovaných služeb k zajištění GDPR ze strany externí firmy a v návaznosti na tyto výsledky lze prohlásit, že stanovená hypotéza byla zcela potvrzena.

Pomocí komparativní metody ve spojitosti s bodovací metodou bylo možné stanovit odpověď na výzkumnou otázku č. 2: *„Je využití externího DPO pro danou organizaci efektivnější než tuto činnost delegovat na některého ze zaměstnanců?“*

Pro získání odpovědi bylo nutné vycházet i ze současné situace vybrané organizace, kdy aktuální stav i přes provedenou prvotní implementaci odpovídá nedostatečnému souladu s GDPR. Na základě této skutečnosti je pro organizaci velmi důležitý přímý kontakt s pověřencem pro ochranu osobních údajů, tj. kancelář přímo v organizaci je v případě interního

DPO velkou výhodou. Velmi vítané jsou i nižší náklady za výkon této funkce interním zaměstnancem a kladné hodnocení je přisuzováno také komplexním znalostem o dané organizaci a jednotlivých procesech, kterými může disponovat pouze interní pracovník. Přesto se s rolí interního DPO pojí značné nevýhody, mezi nejvýraznější patří nutnot proškolení na danou pozici, kdy daný pracovník nemusí okamžitě disponovat potřebnými znalostmi, nýbrž ty budou postupně doplňovány. Zároveň se tímto pojí pro organizaci i vzniklé náklady v podobě potřebných školení. Mezi již ne tak zásadní nevýhody patří také hrozba střetu zájmů a v případě interního DPO musí být počítáno s dny dovolené, pracovní neschopností apod. Naopak externí DPO může organizaci nabídnout mnoho zkušeností i z jiných organizací, a pokud se pohybuje v organizacích, které patří do stejného odvětví, je to značným přínosem pro danou organizaci. Zároveň u externích firem zajišťujících tyto služby nehrozí střet zájmů a nabízí nepřetržité zajištění těchto služeb. Významnou nevýhodou v případě externího DPO jsou vyšší náklady na zajištění této činnosti a působnost mimo danou organizaci. Externí pracovník také nezná detaily o dané organizaci, ačkoli z dlouhodobého pohledu může postupně dojít k odbourání této nevýhody. Všechna hlediska byla s ohledem na aktuální situaci vybrané organizace a na poskytnutá ohodnocená kritéria, viz příloha 2 Tabulka 3 vyhodnocena. Závěrem je možné konstatovat, že pro vybranou organizaci není efektivnější využití externího DPO, nýbrž je doporučeno do role DPO dosadit jedince z řad vlastních zaměstnanců.

Získaný výstup z polostrukturovaného rozhovoru se stal podnětem pro uskutečnění kvantitativního výzkumu s využitím dotazníkového šetření mezi zaměstnanci, čímž byla zodpovězena 1. a 2. část 3. výzkumné otázky a k zodpovězení poslední 3. části přispěla kontrola pracovišť v rámci tzv. politiky čistého stolu. Shrnutí všech částí přispělo za pomoci syntézy k celkovému objasnění 3. výzkumné otázky, celé její znění je následující: *„Jaký je vztah mezi současně nastaveným systémem ochrany osobních údajů v organizaci a přístupem zaměstnanců k tomuto systému?*

a) *Mají zaměstnanci potřebné informace k systému zabezpečení a ochrany osobních údajů v organizaci?*
b) *Přistupují celistvě k nastavenému systému?*
c) *Dbají zaměstnanci na dostatečné zabezpečení a ochranu osobních údajů před jejich neoprávněným zpřístupněním cizím osobám?“*

Dotazníkového průzkumu se účastnilo celkem 83 % zaměstnanců, kteří byli vystaveni souboru 12 připravených otázek, viz příloha 4 Dotazník 1. Výsledky dotazníku potvrdily absenci školení zaměstnanců v oblasti bezpečnosti a ochrany osobních údajů. V souvislosti s tím se ukázal zájem respondentů o formu školení, kdy 56 % by uvítalo e-learningové proškolení, ostatní respondenti se shodli na prezenční podobě. Dotazník byl postaven tak, aby ověřil i znalosti zaměstnanců z dané oblasti. Všichni dotazovaní dokázali vystihnout význam zkratky GDPR a také adekvátně zařadili pojmy: jméno, příjmení, adresu, zdravotní stav mezi osobní údaje. Avšak ne všichni respondenti uvedli za osobní údaj i fotografii, kamerový záznam či emailovou adresu složenou z jména a příjmení osoby, či naopak uvedli jako osobní údaj i služební telefonní číslo. V tomto případě se však jednalo o jednotky dotazovaných. Významnější neznalost byla shledána v případě reakcí na porušení zabezpečení osobních údajů, celkem 76 % respondentů by takový případ nahlásilo nesprávné osobě. Předchozímu zjištění odpovídají navazující výsledky k DPO, kdy 40 % respondentů neví, zda má organizace pověřence pro ochranu osobních údajů. Mezi respondenty bylo ověřováno, jaká bezpečnostní opatření jsou v organizaci nastavena a následně, jaká opatření jsou z jejich strany dodržována, bez ohledu na to, zda vědí o jejich stanovení. Tyto 2 otázky poukazují na skutečnost, kdy si zaměstnanci nejsou některých bezpečnostních opatření vědomi, přesto je dodržují. O tom vypovídá vypínání PC/notebooků při odchodu z pracoviště, 52 % respondentů vypovědělo, že je tato povinnost stanovena, přesto všichni dotázaní potvrdili její plnění. Dalším pozitivním výsledkem je,

že všech 100 % respondentů bere v potaz uzamykání kanceláří/kabinetů při jejich opuštění a ve stejném počtu uvádí, že na dané opatření dbají. Výsledky také ukázaly, že jen 24 % respondentů uzamyká dokumenty s osobními údaji do příslušných skříní a polic, avšak ještě méně z nich (16 %) hledí na jejich uzamčení vždy při odchodu z pracoviště. Závěrečné otázky dotazníku byly věnovány doplňujícím informacím. Většina respondentů označila GDPR za důležité, i přesto se našlo 12 % dotázaných, kteří ho považují za zbytečné. Dotazníkového šetření se zúčastnilo 56 % pedagogických pracovníků, všichni zástupci ekonomického úseku, tj. 16 % dotázaných a 28 % ostatních nepedagogických pracovníků. Na základě získaných výsledků je možné přejít k jejich shrnutí a tím zodpovězení 1. a 2. části výzkumné otázky. Přestože nedochází v organizaci k proškolování zaměstnanců v rámci bezpečnosti a ochrany osobních údajů, disponují zaměstnanci základním povědomím vztahujícím se k této problematice. Avšak výsledky poukazují na znalostní mezery v oblastech týkajících se postupu ohlašování bezpečnostních incidentů a bezpečnostních opatření, která je potřebné dodržovat v rámci organizace a tím předcházet vzniku možných bezpečnostních příhod. Kladným zjištěním je skutečnost, kdy většina respondentů považuje GDPR za důležité. Dotazníkové šetření také ukázalo, jakou formu školení a v jakých pravidelných intervalech by zaměstnanci uvítali.

Provedení kontroly pracovišť na základě tzv. politiky čistého stolu bylo uskutečněno v souvislosti s vnitřními předpisy a nařízeními, které se k zaměstnancům vážou v rámci bezpečnostních opatřeních při práci s osobními údaji. Tyto předpisy zaměstnancům stanovují ukládat fyzické dokumenty s osobními údaji zaměstnanců i žáků do k tomu příslušných zabezpečených skříních v uzamykatelných kancelářích. V případě elektronických evidencí nesmí pracovníci opouštět počítač či notebook bez jeho odhlášení. Zaměstnanci se k výše uvedenému zavazují již na začátku pracovního vztahu, kdy podepisují dohodu o utajovaných skutečnostech, která přímo ukládá uzamykat pracovní stoly, kanceláře a zamezovat zpřístupnění informací dostupných v rámci PC a notebooků jiným osobám. Provedená kontrola proběhla v odpoledních hodinách po skončení pracovní doby zaměstnanců a měla za úkol ověřit, zda zaměstnanci dostatečně dbají na zabezpečení a ochranu osobních údajů. Primárně bylo na namátkově navštívených pracovištích sledováno, zda se nikde nenachází volně přístupné dokumenty obsahující osobní údaje a zda je IT technika vypnuta a dle možnosti uložena a zabezpečena. Celkem bylo nahlédnuto do 3 kanceláří, 4 kabinetů i 4 kmennových tříd. Kontrola ukázala na volně přístupné dokumenty se jmény a doručovacími adresami fyzických osob v jedné z kanceláří, dále byly v jednom z kabinetů nalezeny seznamy žáků jednotlivých tříd včetně docházky na daný předmět za aktuální měsíc, ve 2 třídách se nacházely vyvěšené jmenné seznamy žáků dané třídy s rozpisem přiřazených osobních skříněk dle čísel. Ostatní navštívená pracoviště byla v rámci stanovených hledisek v pořádku. Na všech kontrolovaných pracovištích bylo také ověřeno, že IT vybavení je vypnuto a případně uloženo v uzamčených skříních. Přestože byly v rámci kontroly identifikovány nezabezpečené dokumenty s osobními údaji, nebyly nalezeny žádné podklady, které by obsahovaly citlivé osobní údaje. Co se týče jmenných seznamů žáků uvedených v jednotlivých třídách, vyjádřilo se k nim vedení organizace přímo při probíhající kontrole. Vedení v tomto ohledu argumentovalo, že seznamy slouží k připomínání služeb mezi jednotlivými studenty či pro připomenutí čísel osobních skříněk, které si žáci nepamatují. I přes tuto argumentaci je nutné podotknout, že kmennové třídy slouží i ostatním studentům napříč školou, zároveň do školy dochází pravidelně velké množství osob v rámci jejich dalších aktivit, při kterých jsou jednotlivé třídy využívány i těmito osobami. Vedením organizace také bylo připuštěno, že některá z pracovišť nedisponují dostatečným množstvím uzamykatelných skříních pro dokumenty s osobními údaji. Ačkoli kontrola odhalila volně přístupné dokumenty s osobními údaji na některých pracovištích, je možné konstatovat, že napříč organizací

zaměstnanci dbají na zajišťování bezpečnosti a ochrany osobních údajů, přesto byly identifikovány mezery, které je potřeba dále posoudit a sjednat jejich nápravu.

Po získání výsledků ze všech částí je možné přejít k celkovému vyhodnocení 3. výzkumné otázky. Přestože v současně nastaveném systému doposud neproběhlo proškolení zaměstnanců ani jejich seznámení s předpisy vztahujícími se k GDPR, zaměstnanci mají základní povědomí dané problematiky, jsou si vědomi bezpečnostních opatření v organizaci a v převážné většině dbají na jejich dodržování. Jejich přístup lze vyhodnotit jako respektující, zodpovědný vůči nastavenému systému, avšak s identifikovanými mezerami, které souvisí zejména s potřebou proškolení v oblasti zabezpečení osobních údajů a následném dodržování stanovených pokynů.

Pomocí získaných výsledků z GAP analýzy a v součinnosti s datovým auditem bylo možné zodpovědět 4. výzkumnou otázku: *„Jaké povinnosti je nutné revidovat ve stávajícím systému ochrany osobních údajů v organizaci potřebných k naplnění souladu s GDPR?“*

Výsledky poukázaly na nedostatečné plnění povinností ze strany externího pověřence pro ochranu osobních údajů, nekompletní vedení záznamů o činnostech zpracování, absenci procesu ověřování zpracovatelů osobních údajů a využívání doložek o ochraně osobních údajů v rámci zpracovatelských smluv. Dále bylo identifikováno nezákonné zpracovávání 2 osobních údajů, nadbytečné zpracovávání osobních údajů ve 3 činnostech a nadbytečné vyžadování některých souhlasů. Poslední bod potvrzuje upozornění ÚOOÚ (2019), které poukazuje na nadbytečné vyžadování souhlasů ve školství. Nedochází k plnění informační povinnosti u 6 činností a s tím souvisí i absence doby uchovávání osobních údajů u 10 činností. Revizi vyžaduje také: proces řízení bezpečnostních incidentů, kdy nejsou stanoveny odpovědné osoby, postup v případě vzniklých incidentů včetně odpovědností a postup při ohlašování incidentů ÚOOÚ a subjektům údajů. Vybraná organizace nemá stanoven proces analýzy rizik a jak poukázaly výsledky datového auditu i přes možná vysoká rizika pro práva a svobody osob u vybraných činností neproběhlo posouzení DPIA. Nebyl proveden balanční test k využívanému kamerovému systému a umístěné informační cedule k využívaným kamerám nejsou dostačující. Vnitřní směrnice nepojednává o všech organizačních opatřeních vztahujících se k procesům s osobními údaji napříč organizací, nejsou vedeny evidence uplatněných práv subjektů údajů, stížností ani vzniklých bezpečnostních incidentů a nejsou nastaveny podmínky usnadňující výkon práv subjektů údajů. Také byla identifikována absence kontrol a kontrolních mechanismů, které by monitorovaly dostatečné zajišťění ochrany a bezpečnosti osobních údajů. Významným zjištěním je také skutečnost, že zaměstnanci nejsou pravidelně proškolováni v rámci problematiky GDPR, dokonce doposud ani jednou proškoleni nebyli, a nedochází k jejich seznamováni se souvisejícími vnitřními předpisy. Výše popsaný výčet shrnuje nejzásadnější povinnosti, které je potřeba ve stávajícím systému organizace XY revidovat.

V pořadí 2. hypotéza byla ověřena závěrečným vypracováním návrhu projektu transformace implementovaného GDPR do procesů organizace a průběhem jeho realizace. Znění dané hypotézy je následující: *„Pokud organizace zjistí nedostatečné plnění povinnosti vyplývající z GDPR, je schopna vlastními silami provést nápravu.“*

K ověření tohoto tvrzení bylo přistupováno ve 2 krocích, prvním bylo vypracování návrhu projektu a druhý krok představoval jeho samotnou realizaci. V souvislosti s návrhem projektu byl na základě identifikovaných výsledků GAP analýzy vymezen rozsah jednotlivých úkolů. V návaznosti na stanovené činnosti a jejich detailní rozbor byl proveden odhad doby jejich trvání a identifikování souvisejících předchozích činností. Díky těmto datům byl vypracován časový harmonogram projektu, pro jeho znázornění byl využit ganttův diagram, který již zahrnoval přidělené pracovníky včetně časových rezerv, které počítaly s prací mimo projekt

a braly v potaz i čerpání dovolených. Samotná tvorba návrhu projektu pracovala s několika limity, které se týkaly stanoveného rozpočtu i maximálního množství přidělených lidských zdrojů a jejich časového omezení. Délka projektu vzhledem ke všem proměnným je stanovena na 72 dnů resp. 52 pracovních dnů v kalendářním roce. Nejzazší termín pro dokončení projektu je 1.9.2023 a samotný návrh projektu s tímto termínem koresponduje. Návrh byl zakončen zhodnocením, pro který byla zpracována analýza rizik a kalkulace nákladů. Projekt není ohrožen žádným nepřijatelným rizikem, pouze 3 identifikovaná rizika jsou na pomezí intervalu nežádoucího a mírného rizika. Pro všechna nalezená rizika byla stanovena bezpečnostní opatření, pomocí kterých budou rizika udržována na přijatelné úrovni. Kalkulací nákladů byl projekt vyčíslen na 47 850 Kč, čímž je dodržen stanovený rozpočet projektu vymezený na 50 000 Kč. Do celkových nákladů nebyla započítána odměna internímu zaměstnanci nově stanovenému do funkce DPO, a to z důvodu, že doposud je externí firmě vyplácena pravidelná měsíční platba. Výplata této odměny tedy nepředstavuje pro organizaci další náklad, ale lze ji považovat za úspornější variantu oproti doposud vyplácené paušální platbě externí firmě. Projekt je na základě zhodnocení návrhu označen za realizovatelný. Vypracovaný návrh byl představen organizaci XY, včetně ostatních variant získaných z výsledků průzkumu trhu týkajících se volby mezi interním a externím DPO a výběru společnosti pro zajištění školení GDPR interního zaměstnance. Organizace XY se projekt rozhodla realizovat v navrhované, autorkou diplomové práce, doporučené formě. Kompletní realizaci projektu bude možné posoudit až po termínu 1.9.2023 finalizace projektu. Z tohoto důvodu je hypotéza potvrzena částečně.

Závěrem z provedených výzkumů vyplývá, že outsourcované služby musí být důkladně prověřovány v jejich průběhu, správci osobních údajů nemohou spoléhat na jejich požadované plnění, aniž by si ověřili skutečnost. Pokud organizace přemýšlí o výběru mezi externím a interním DPO, je důležité provést posouzení v souladu s určenými prioritami, protože volba mezi těmito dvěma možnostmi nemusí vždy znamenat větší efektivitu. Pozornost správců osobních údajů by měla být také věnována ověřování znalostí zaměstnanců v dané problematice, obecně lidé mají povědomí o GDPR, základní otázky v testování nemusí ihned ukázat na případné nedostatky, avšak při cílenějších otázkách může dojít k identifikaci potřebných mezer. Jak ukázaly výsledky výše, organizace jsou schopny vlastními silami vypracovat návrh projektu transformace implementovaného GDPR do jejich procesů. Tato skutečnost byla ověřena s předpokladem, že organizace mají k dispozici alespoň jednoho jedince, který se v dané problematice orientuje minimálně na základní úrovni.

3.3.2 Přínosy práce

Problematika GDPR je stále aktivně probíraným tématem napříč společností, čemuž přispívají nejen pravidelné kontroly správců osobních údajů ze strany dozorčího orgánu s možnou vidinou hrozby sankcí, ale i příchozí nová legislativní ustanovení, která se na oblast bezpečnosti a ochrany osobních údajů vážou nebo ji dokonce doplňují. V souvislosti s platnou legislativou musí vybrané společnosti naplňovat soulad se stanovenými povinnostmi a řídit se danými zásadami. V současné chvíli je volně k dispozici mnoho pramenů na téma implementace GDPR do procesů organizace, avšak již není příliš zdrojů, které by se věnovaly případům, kdy implementace neodpovídá stanoveným povinnostem a není tak naplněn soulad s GDPR. Problematika byla posunuta díky otevření odborného tématu chybných implementací GDPR včetně zpracování návrhu metodického postupu lze problematiku řešit komplexně, systematicky a aplikovat ji do procesního řízení vybrané organizace.

Primární přínos přináší práce především vybrané organizaci, neboť důsledkem nedostatečného zajištění bezpečnosti a ochrany osobních údajů může být vystavena organizace riziku sankcí i reputačnímu riziku. Signifikantní pro vybranou organizaci bylo odstranění chybné implementace GDPR a zajištění požadovaného souladu ochrany osobních údajů s GDPR

a eliminace hrozby sankcí. Sekundární přínos, avšak neméně důležitý, představuje provedený datový audit, díky čemuž má organizace kompletní přehled o probíhajících procesech a zpracovávaných osobních údajích. Tento podklad je přínosem v případě kontroly z ÚOOÚ, avšak získané údaje jsou cenným materiálem pro každou organizaci, společnost, která chce mít přehled o probíhajících procesech. Postup datového auditu byl zvolen na základě popisu Nezmara (2017, s. 533-554), čímž byla ověřena jeho funkčnost a logická návaznost, kdy na konkrétním příkladu této práce je daný postup prověřen a zpřístupněn i dalším organizacím a společnostem. Provedená komparativní metoda, která rozhodla o efektivnější variantě využívání interního DPO z řad zaměstnanců pro vybranou organizaci, přinesla organizaci XY úsporu nákladů díky zajištění pověřence pro ochranu osobních údajů z řad zaměstnanců.

Pedagogický přínos do výukového procesu přináší teoretická část diplomové práce, ve které je pracováno se zdroji, jenž se zaměřují na povinnosti GDPR vztahující se přímo ke školským institucím. Školská zařízení i další vzdělávací organizace v textu nachází odpovědi na často diskutované otázky související s odbornou problematikou GDPR, například k využívání kamerových záznamů nebo k získávání souhlasů se zpracováním osobních údajů. Teoretická část a její výsledky mají uplatnění i v rámci vzdělávacích programů profesně orientovaných vysokých škol a univerzit do oblasti například Podnikové ekonomiky a managementu, kde mohou problematiku transformace GDPR do procesního řízení organizací hlouběji rozvíjet.

Praktický přínos je zajištěn i dalším společnostem bez ohledu na odvětví, ve kterém působí. V první řadě se jedná o společnosti, které využívají externího pověřence pro ochranu osobních údajů. Diplomová práce zpracovávaným tématem ostatní společnosti upozorňuje na potřebu orientace v dané problematice alespoň na minimální úrovni a dle toho průběžně monitorovat outsourcovanou službu a dodržování plnění povinností v souladu s GDPR. Pokud společnosti zvažují, zda využívat externího nebo interního DPO, a která z možností je pro ně efektivnější, mohou pro své rozhodnutí postupovat dle zvolené komparativní metody s uvedením vzorového příkladu, viz Tabulka 4, kde jsou obě varianty posouzeny na základě přiděleného bodového ohodnocení. Přínos je zajištěn také institucím a organizacím, které identifikovaly ve svých procesech mezery nebo nesoulad mezi stanovenými a reálně plněnými povinnostmi vyplývajícími z GDPR, přičemž neví, jak k této situaci přistoupit. Práce obsahuje detailní popis pro sjednání nápravy, který slouží jako metodická pomůcka k provedení datového auditu a ověření souladu s GDPR s uvedením vzorového příkladu. Zároveň diplomová práce upozorňuje na nezbytnost pravidelné a důkladné kontrolní činnosti dodržování s GDPR v integraci nedostatečné implementace povinností.

Přínos z hlediska výzkumné a vědecké oblasti přináší vytvořené postupy, které slouží jako základ pro další výzkumné projekty v oblasti vzdělávání nebo mezinárodní spolupráce, přičemž jejich využití zahrnuje tvorbu odborných studií a zpráv s důrazem na současné koncepty ESG (Enviromental, Social, Governance). Diplomová práce svým rozsahem přispívá k posílení porpojení mezi oblastmi GDPR a ESG.

Přínos pro autorku kvalifikační práce je zajištěn nejen v rozvoji odborných znalostí a dovedností, ale především v naplnění osobní motivace k hlubšímu porozumění problematice transformace implementovaného GDPR do procesního řízení. Skrze intenzivní angažovanost v procesu získávání nových poznatků a jejich aplikaci do analytické části diplomové práce byl zajištěn cenný vhled do reálného fungování konceptů GDPR ve firemním kontextu. Tímto způsobem autorka diplomové práce, jako kmennový zaměstnanec vybrané organizace, rozšířila svůj profesní rozhled a aktivně přispěla k efektivnímu implementování osvojených postupů ve svém pracovním prostředí.

Nejvýznamnější dopad na diplomovou práci má bezejmenost údajů, kdy dochází ke striktní anonymizaci údajů, které by mohly odkrýt identitu vybrané organizace. Tato skutečnost má

pro organizaci XY ochranný charakter, avšak ostatní instituce využívající stejnou externí firmu k zajišťování GDPR nejsou jednoznačně upozorněny na situaci, kdy se nezajištění souladu s GDPR může vztahovat i na ně. Následná tvorba návrhu projektu transformace implementovaného GDPR do procesního řízení organizace byla limitována lidskými zdroji, jejich časovými možnostmi, stanoveným rozpočtem a termínem pro realizaci projektu. Obsah samotné práce představuje potenciál pro její další rozvoj, kdy je možné na ni dále navázat. Oblast GDPR se neustále vyvíjí, stále vstupují v platnost nové legislativní předpisy, které se ji dotýkají a nastavené procesy je potřeba průběžně monitorovat a udržovat s nimi v souladu. Nelze opomenout ani velmi rychlý vývoj digitálních technologií využívaných napříč všemi odvětvími, v souvislosti s tímto trendem se pojí například stále častěji využívaná umělá inteligence, která pro strojové učení využívá ohromné množství osobních dat. Tímto tématem se otevírá mnoho otázek, kterým může být věnován prostor právě v pokračování tématu dané práce. Nejvýznamnější a nejaktuálnější potenciál pro další práci v souvislosti s vybranou organizací představuje skutečnost, kdy při samotném návrhu projektu transformace chybně implementovaného GDPR do procesů organizace diplomové práci bylo hleděno naplnění požadovaného souladu s GDPR a splnění časového termínu s akcentem k vyšší účinnosti nastavených procesů a zdrojů pro zpracovávání osobních údajů. Navazující kvalifikační práce se může zaměřit na účelnost a hospodárnost vynaložených prostředků navrhovaného projektu.

4 Závěr

Problematika bezpečnosti a ochrany osobních údajů je diskutovaným tématem, které vešlo do povědomí především díky účinnosti GDPR a s tím související další zavádějící se legislativy. Tímto nařízením vznikly nové povinnosti mnoha organizacím, které musely své procesy uzpůsobit povinnostem dané legislativy a tím eliminovat hrozbu sankcí. Implementace GDPR do procesů jednotlivých společností musela proběhnout do předem stanoveného termínu, a i přes mnoho zdrojů, které se této problematice a samotné implementaci GDPR napříč odvětvími věnují, nejsou příliš známy ty, které by se zabývaly jejím chybným provedením.

Primárním cílem diplomové práce bylo navrhnout projekt transformace implementovaného GDPR do procesního řízení vybrané organizace. Sekundárními cíli bylo zhodnocení současného stavu dodržování povinností integrovaných s GDPR ve prospěch vybrané organizace s identifikací jednotlivých proceseů, ve kterých dochází ke zpracovávání osobních údajů napříč organizací.

Na úvod teoreticko-metodologické části práce byl zařazen stručný vhled do oblasti GDPR, významný prostor byl věnován povinnostem, kterým čelí správci osobních údajů se zaměřením na školské instituce, a završení proběhlo rozebráním práv subjektů údajů. Tímto je uzavřena první část. Druhá část se teoreticky více zabývá realizací potřebných kroků k zaopatření souladu s GDPR. V souvislosti s tím jsou popsány nástroje využívané k provedení impelementace a dále je přiblížen vhled do procesního a projektového řízení včetně vybraných nástrojů pro tvorbu projektu. Aby organizace měly jistotu, že zpracovávají v souladu s GDPR všechny osobní údaje, se kterými pracují, musí mít důkladný přehled o jednotlivých procesech probíhajících v jejich organizaci. Nesmí se však opomenout, že nastavení procesů není jedinou vyžadovanou aktivitou¨, nýbrž souborem činností, ke kterým je signifikantní přistupovat racionálně a zodpovědně napříč celou organizací. Proto nelze podcenit seznámení zaměstnanců s procesy ochrany osobních údajů, neboť její vyžadování je striktní. Teoretickou část diplomové práce zakončuje kapitola Metodika práce.

V analytické části je stručně představena organizace, která byla pro diplomovou práci zvolena a nese název XY. Jedná se o střední školu a z důvodu citlivosti a ochrany údajů jsou bližší informace o organizaci anonymizovány. Na úvdo této části byl proveden rozbor současného stavu dodržování povinností vyplývajících z GDPR v dané organizaci. Na výsledná zjištění navázal rozsáhlý datový audit, kterým byly detailně identifikovány jednotlivé procesy napříč organizací, ve kterých dochází ke zpracovávání osobních údajů. Realizovaný audit byl završen GAP analýzou, jejímž výstupem byly identifikovány mezery od požadovaného stavu. Na základě identifikace výsledků GAP analýzy a v součinnosti s datovým auditem byla navrhnuta doporučení ke změnám včetně opatření, jak systematicky nedostatky napravit. Získané výsledky byly představeny vedení organizace, které zároveň shrnulo požadavky pro akceptaci následného návrhu projektu. V návaznosti na získané podklady a výsledky GAP analýzy byl zpracován návrh projektu transformace implementovaného GDPR do procesů organizace. Hlavní parametry návrhu projektu se zabývaly rozsahem práce a časovým harmonogramem, pro zhodnocení projektu byla provedena analýza rizik a kalkulace nákladů. Vypracovaný návrh projektu byl představen vedení organizace XY. Analytická část práce je finalizována kapitolou Diskuse výsledků a Přínosy práce.

Zhodnocení současného stavu dodržování povinností ukázalo, že organizace XY outsourcuje služby spojené s GDPR, avšak ze strany organizace nedochází k provádění kontrol daného zpracovatele. Výsledky zhodnocení aktuální situace potvrdily nedostatečné plnění povinností vyplývajících z GDPR a nesoulad byl identifikován i u činností zpracovávaných externí firmou. Nejsou plněny povinnosti vztahující se zejména k vedení záznamů o činnostech zpracování osobních údajů, ke smlouvám se zpracovateli osobních údajů a neprobíhá školení zaměstnanců

k problematice GDPR. Externí firma dle smluvních podmínek dostatečně nezajišťuje zmiňované záznamy o činnostech zpracování a proškolování vedoucích zaměstnanců, dále neprovádí bezpečnostní kontroly a poskytuje pouze omezené konzultační služby. Pokud organizace využívá outsourcing daných služeb, nesmí opomíjet důkladné prověření dané společnosti, dostatečné smluvní ošetření a pravidelný dohled nad plněním předaných náležitostí. Zástupci organizace musí disponovat minimálně základními znalostmi o potřebných náležitostech, které jsou pro zajištění souladu s GDPR stěžejní. Na základě toho by mělo docházet k pravidelnému vyhodnocování plnění stanovených smluvních podmínek s externí firmou. Každý správce osobních údajů si musí uvědomit, že jakékoliv nedodržení povinností vyplývajících z GDPR jde primárně za ním. S ohledem na zjištění výše byla provedena komparativní metoda, která posuzovala, zda je pro organizaci XY efektivnější využívat interního nebo externího pověřence pro ochranu osobních údajů. Na základě získaných výsledků bylo organizaci doporučeno pověřit do funkce DPO interního zaměstnance. Kvantitativní výzkum ukázal, že zaměstnanci mají i přes absenci školení základní znalosti v oblasti GDPR a k nastaveným povinnostem systému ochrany osobních údajů v organizaci přistupují převážně s respektem a zodpovědně. Přesto je proškolení zaměstnanců nevyhnutelné, i z důvodu patrných mezer ve znalosti a dodržování bezpečnostních opatření. Provedený datový audit, který proběhl v návaznosti na výsledky výše, identifikoval celkem 51 činností, ve kterých dochází napříč organizací ke zpracovávání osobních údajů, v souvislosti s tím byly zmapovány odpovědné osoby, zpracovávané osobní údaje, přidělené interní i externí přístupy, využívané systémy i zavedená bezpečnostní opatření. Tímto postupem podle Nezmara (2017, s. 533-554) byly identifikovány další nesoulady s GDPR, zároveň byla ověřena jeho logická návaznost a funkčnost. Odhalenými nesoulady jsou: nadbytečné či nezákonné zpracovávání několika osobních údajů, neplnění informační povinnosti o zpracovávaných údajích, nadbytečné vyžadování souhlasů se zpracováním osobních údajů, absence balančního testu a provedení DPIA. K identifikaci mezer mezi plánovaným a reálným stavem souladu dodržování GDPR v organizaci pomohla GAP analýza, ve které byly odhaleny mezery a na jejich základě v součinnosti s výsledky datového auditu byla navrhnuta doporučení ke změnám včetně opatření, jak dokonaleji nedostatky napravit. Zároveň tento výstup posloužil jako primární podklad pro zpracování návrhu projektu včetně stanovení jeho rozsahu. Samotný rozsah se skládal z 16 činností a na základě časového harmonogramu byla určena délka celého projektu na 52 pracovních dnů v kalendářním roce. Délka trvání byla stanovena s ohledem na přidělené lidské zdroje i časové rezervy. Analýza rizik projektu poukázala na 5 rizik z toho 3 se nacházejí v intervalu mezi mírným a nežádoucím rizikem a pro všechna identifikovaná rizika byla stanovena bezpečnostní opatření, viz Tabulka 10. Celkové náklady projektu představují 47 850 Kč a projekt je na základě zpracovaného návrhu a stanovených požadavků označen za realizovatelný. Návrh projektu i s možnými variantami byl předán vedení organizace XY, která jej přijala v doporučené variantě a zahájila jeho realizaci dle vypracovaného časového harmonogramu. Závěrem je třeba podotknout, že zvládnutí nápravy chybného stavu a úspěšné ukončení projektu neznamená konec. Problematika GDPR vyžaduje pravidelné sledování a monitoring. Organizace tak ani nadále nemine průběžné vyhodnocování dodržování souladu s GDPR, uskutečňování pravidelných kontrol a školení zaměstnanců. Tyto uvedené body byly zahrnuty do jednotlivých činností návrhu projektu, tak aby došlo k jejich začlenění do procesů organizace XY. Získané výsledky z uskutečněných výzkumů potvrdily hypotézu č. 1: „Pokud organizace neprovádí pravidelné kontroly outsourcovaných služeb, nemůže se spoléhat na důkladné plnění povinností integrovaných s GDPR“. Tímto bylo zároveň potvrzeno nedostatečně zajištěné plnění povinností GDPR a vidina hrozby vystavení organizace XY sankcím. Zpracovaný návrh projektu transformace implementovaného GDPR do procesů organizace a jeho přijetí organizací částečně potvrdilo 2. stanovenou hypotézu: „Pokud organizace zjistí nedostatečné plnění povinnosti vyplývající z GDPR, je schopna

vlastními silami provést nápravu“. Aby mohlo dojít k úplnému potvrzení hypotézy, musí být projekt úspěšně realizován, ověření bude možné po termínu 1.9.2023, kdy dojde k postupnému zhodnocení úspěšnosti projektu.

Na základě zákonnosti, korektnosti, transparentnosti a dalších zásad integrovaných s GDPR, viz subkapitola 2.1.2 Povinnosti správců údajů, došlo k posouzení účinnosti doporučení s náměty z kapitoly 3.3 Vyhodnocení výsledků a přínosů. Výsledky, jenž poukazují na nezákonné a nadbytečné zpracovávání osobních údajů, nadbytečné vyžadování souhlasů se zpracováním osobních údajů, na neplnění informační povinnosti a na absenci stanovené doby pro uchovávání osobních údajů u 10 činností potvrzují, že v organizaci XY nejsou naplněny tyto zásady: zákonnosti, transparentnosti, účelového omezení, minimalizace a omezení uložení údajů. Tyto výsledky jsou podnětem pro organizaci XY ke zdokonalení procesů systému ochrany osobních údajů.

Dopady a omezení přináší diplomové práci bezejmenost údajů. Tato skutečnost byla zvolena z důvodu citlivosti a bezpečnosti údajů, které jsou v diplomové práci v souvislosti s organizací XY uváděny. Pokud by dané údaje v práci nepodléhaly anonoymizaci, organizace využívající stejnou externí firmu pro zajišťování služeb spojených s GDPR, by byly upozorněny, že se nedostatečné plnění souladu s GDPR může vztahovat i na ně. Samotný návrh projetu byl limitován ve využití kapacit, kdy byly omezeny lidské zdroje pouze na dostupný počet a s ohledem na jejich časové možnosti, návrh projektu musel korespondovat s vyhrazeným termínem a s přiděleným rozpočtem za účelem jeho akceptace a následné možné realizace.

Kvalifikační práce má přínos nejen pro samotnou organizaci, v níž byla aplikována, ale i pro ostatní veřejné organizace působící ve stejném nebo příbuzném odvětví. Signifikantní pro vybranou organizaci bylo odstranění chybné implementace GDPR a zajištění požadovaného souladu s GDPR. V obecné rovině návrh transformace GDPR do procesního řízení organizace slouží ostatním veřejným institucím i neziskovým organizacím jako metodická pomůcka k provedení datového auditu a ověření souladu s GDPR s uvedením názorného postupu, viz kapitola 3.1.3 Datový audit. Podobný přínos představuje provedená komparativní metoda, jejíž ukázka, viz kapitola 3.1.2 Tabulka 4 je nápomocna při rozhodnutí, zda využívat externího nebo interního pověřence pro ochranu osobních údajů. Není mnoho zdrojů, které by admitovaly eventualitu nesprávné implementace, a v důsledku toho nedodržení povinností v souladu s GDPR. Odborná tématika GDPR byla diplomovou prací posunuta díky otevření odborného tématu chybných implementací GDPR včetně zpracování návrhu metodického postupu lze problematiku řešit komplexně, systematicky a aplikovat ji do procesního řízení vybrané organizace. V neposlední řadě i teoretická část přináší odpovědi na často diskutované otázky týkající se využívání kamerových systémů a souhlasů se zpracováním osobních údajů v sektoru školství a vzdělávání, které jsou určeny ostatním vzdělávacím institucím.

Závěrem lze konstatovat, že primární cíl práce byl naplněn, návrh projektu v jeho doporučeném znění byl akceptován vedením organizace XY na operativní poradě dne 12. 06. 2023 a implementován do vnitřních předpisů organizace, viz příloha 5 Obrázek 5. V diplomové práci byly průběžně zodpovězeny jednotlivé výzkumné otázky. Druhá hypotéza byla potvrzena částečně z důvodu dobíhající realizace projektu. Díky navrácení vložených nákladů do školení získává projekt nejen ekonomickou přidanou hodnotu, ale i zásadní společenský přínos prostřednictvím rozvoje pracovníků a udržitelného přístupu. Tyto faktory ve vzájemném působení vytvářejí solidní základ pro budoucí inovace a udržitelný růst, což otevírá perspektivní cestu směrem ke zkvalitňování nastavených procesů ve střednědobém a dlouhodobém horizontu. Potenciál navazující kvalifikační práce tkví v orientaci na účelnost vynaložených nákladů do projektu a efektivnost nastavených procesů z hlediska využitelnosti a hospodárnosti zdrojů a vložených prostředků pro účely zpracovávání osobních údajů.

Literatura

Primární zdroje

Evropský sbor pro ochranu osobních údajů pokyny 03/2019, ze dne 29. ledna 2020, verze 2.0

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

ÚOOÚ: Metodika obecného posození vlivu na ochranu osobních údajů, ze dne 11. listopadu 2020, verze 1.0.

WP248 rev. 1 Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679

Zákon č. 110/2019 Sb. ze dne 24. dubna 2019, zákon o zpracování osobních údajů.

Zákon č. 89/2012 Sb. ze dne 3. února 2012, zákon občanský zákoník.

Monografie

DENLEY, A., FOULSHAM, M., HITCHEN, B., *GDPR: how to achieve and maintain compliance*. New York: Routledge, Taylor & Francis Group, 2019. 211 s. ISBN 978-0-429-44997-0.

DOLEŽAL, J. a kol. *Projektový management*. 2. vydání. Praha: Grada Publishing, 2023. 432 s. ISBN 978-80-271-3619-3.

DOLEŽAL, J., KRÁTKÝ, J. *Projektový management v praxi: naučte se řídit projekty!* Praha: Grada, 2017. 176 s. ISBN 978-80-247-5693-6.

DUMAS, M. et al. *Fundamentals of Business Process Management*. 2. vydání. Germany: Springer Berlin Heidelberg, 2018. 527 s. ISBN 978-3-662-56509-4.

FIALOVÁ, E., MATEJKA, J., GÜTTLER, V. *Profilování a automatizované rozhodování (nejen) ve světle lidských práv a základních svobod.* Praha: Ústav státu a práva AV ČR, 2020. 78 s. ISBN 978-80-87439-42-5.

FRÝBOVÁ, A. a kol. *První zkušenosti s GDPR ve školství*. Praha: Wolters Kluwer, 2019. 208 s. ISBN 978-80-7598-601-6.

JANEČKOVÁ, E. *GDPR: řešení problémů v praxi škol*. 1. vyd. Praha: Grada Publishing, 2020. 352 s. ISBN 978-80-271-1354-5.

JUROVÁ, M. a kol. *Výrobní a logistické procesy v podnikání*. Praha: Grada Publishing, 2016. 264 s. ISBN 978-80-247-5717-9.

KOTTER, P. J. *Vedení procesu změny: Osm kroků úspěšné transformace podniku v turbulentní ekonomice.* 2. vydání. Praha: Management Press, 2015. 224 s. ISBN 978-80-7261-314-4.

KŘIVÁNEK, M. *Dynamické vedení a řízení projektů: systémovým myšlením k úspěšným projektům*. Praha: Grada, 2019. 208 s. ISBN 978-80-271-2645-3.

MELOTÍKOVÁ, P. *Osobní údaje v kontextu GDPR*. Praha: Leges, 2020. 140 s. ISBN 978-80-7502-507-4.

NEZMAR, L. *GDPR: praktický průvodce implementací*. 1. vyd. Praha: Grada Publishing, 2017. 304 s. ISBN 978-80-271-0921-0.

NONNEMANN, F. *Příručka pověřence pro ochranu osobních údajů*. 1. vyd. Praha: Klika, 2018. 144 s. ISBN 978-80-88298-10-6.

NOVÁK, A. *Inovace je rozhodnutí: kompletní návod, jak dělat inovace nejen v byznysu.* Praha: Grada, 2017. 208 s. ISBN 978-80-271-0333-1.

QUINN, B. *Data Protection Implementation Guide: A Legal, Risk and Technology Framework for the GDPR.* The Netherlands: Kluwer Law International B.V., 2021. 384 s. ISBN: 978-94-035-2902-8.

SVOZILOVÁ, A. *Projektový management: systémový přístup k řízení projektů*. 3. vydání. Praha: Grada Publishing, 2016. 424 s. ISBN 978-80-271-9473-5.

ŠVECOVÁ, L., VEBER, J., *Produkční a provozní management*. Praha: Grada Publishing, 2021. 344 s. ISBN 978-80-271-4621-5.

VOIGT, P., BUSSCHE A. *The EU general data protection regulation (GDPR): a practical guide*. Cham: Springer, 2017. 382 s. ISBN 978-3-319-57958-0.

Odborné knihy a časopisy

SZALOWSKI, R., *Data protection officer in the light of the provisions of the General Data Protection Regulation (GDPR).* Ius Novum, 2018, ročník 12, č. 4, 115-130 s. DOI:10.26399/iusnovum.v12.4.2018.38/r.szalowski.

RICHTER, Š. *Právník: Ochrana osobních údajů v kontextu poskytování digitálních dat spotřebitelům.* Praha: Právnická jednota, 2021, č. 9. 745-758 s. ISSN 0231-6625.

ZELENA, M. a kol., *The Use of GAP Analysis Method for Implementing the GDPR in a Healhcare Facility.* Tomas Bata University in Zlín, 2018, č. 14. 643-652 s. ISSN 2224-3496.

Internetové zdroje

GEMBALOVÁ, K., *Nadbytečné vyžadování souhlasů – věčný problém GDPR ve školství. Gdpr-pověřenec.com [online]*. 2019 [cit. 2023-03-07]. Dostupné z WWW: https://gdpr-poverenec.com/nadbytecne-vyzadovani-souhlasu-vecny-problem-gdpr-ve-skolstvi/.

HNILIČKA, L., *Kamery na úřadech a ve školách: na co si dát pozor. Gdpr-pověřenec.com [online]*. 2022 [cit. 2023-03-08]. Dostupné z WWW: https://gdpr-poverenec.com/kamery-na-uradech-a-ve-skolach-na-co-si-dat-pozor/.

LOCK, S., *GDPR for schools: how will the new data regulations affect my school? Tes.com [fonline]*. 2018 [cit. 2023-03-19]. Dostupné z WWW:

https://www.tes.com/magazine/archive/gdpr-schools-how-will-new-data-regulations-affect-my-school.

MATOUŠ, R., *GDPR: jak efektivně implementovat za „pět minut dvanáct“? Epravo.cz [online]*. 2018 [cit. 2023-02-19]. Dostupné z WWW: https://www.epravo.cz/top/clanky/gdpr-jak-efektivne-implementovat-za-pet-minut-dvanact-107384.html.

MŠMT: *Metodická pomůcka k aplikaci GDPR ve školství [online]*. 2017 [cit. 2023-04-07]. Dostupné z WWW: https://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane.

NEZMAR, L., *Jak na analýzu rizik – prakticky a jednoduše. Gdpr-pověřenec.com [online]*. 2020 [cit. 2023-04-04]. Dostupné z WWW: https://gdpr-poverenec.com/jak-na-analyzu-rizik-prakticky-a-jednoduse/.

ÚOOÚ: *Nová úprava DPIA [online]*. 2023 [cit. 2023-03-12]. Dostupné z WWW: https://www.uoou.cz/nova-uprava-dpia/d-56808.

ÚOOÚ: *Od ledna řešil ÚOOÚ přes sto porušení zabezpečení osobních údajů [online]*. 2020 [cit. 2023-03-07]. Dostupné z WWW:

https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=42768&n=od-ledna-resil-uoou-pres-sto-poruseni-zabezpeceni-osobnich-udaju.

ÚOOÚ: *Praxe s nadbytečným vyžadováním souhlasů ve školství přetrvává [online]*. 2019 [cit. 2023-03-07]. Dostupné z WWW:

https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=35989&n=praxe%2Ds%2Dnadbytecnym%2Dvyzadovanim%2Dsouhlasu%2Dve%2Dskolstvi%2Dpretrvava.

VALENTOVÁ, K., *Balanční test – kdy a jak ho provést? Gdpr-pověřenec.com [online*]. 2023 [cit. 2023-03-07]. Dostupné z WWW: https://gdpr-poverenec.com/balancni-test-kdy-a-jak-ho-provest/.

XY: *Pro uchazeče [online]*. 2023 [cit. 2023-01-19]. Dostupné z WWW: https://www.xy.cz/pro-uchazece/.

Konference

Valentová, K., *P*růšvihy s kamerami a monitoringem. GDPR na pranýři: zákony 2023 a bující kontroly. Nakladatelství FORUM s.r.o., Praha, 2023 [cit. 2023-05-18].

Interní materiály

XY. Informační memorandum (2018)

XY. Podklady k GDPR organizace XY (2018-2023)

XY. Směrnice k GDPR (2018)

XY. Smlouvy (2018-2023)

XY. Souhlasy se zpracováním osobních údajů (2018-2023)

XY. Spisový a skartační řád (2022)

SENSIO. Interní dokumenty (2023)

PORADCE-GDPR. Interní dokumenty (2023)

BELL CONSULTING. Interní dokumenty (2023)

TAYLLORCOX. Interní dokumenty (2023)

GDPR SUPPORT. Interní dokumenty (2023)

KRUCEK. Interní dokumenty (2023)

CEMS CO. Interní dokumenty (2023)

GDPR CERTIFIKACE&COMPLIANCE. Interní dokumenty (2023)

Seznam příloh

Příloha 1 Přepis rozhovoru s ředitelem organizace XY II
Příloha 2 Tabulky V
Příloha 3 Výčet účelů z formuláře Souhlas se zpracováním osobních údajů VII
Přílohy 4 Dotazníky VIII
Příloha 5 Obrázky XIX

Přílohy

Příloha 1 Přepis rozhovoru s ředitelem organizace XY

Rozhovor probíhal v polostrukturované podobě a nesl se v neformálním duchu. Rozhovor vedla autorka diplomové práce. Některé údaje byly anonoymizovány z důvodu zajištění ochrany.

Datum realizace rozhovoru: 23.01.2023 v 14:00
Místo realizace: organizace XY
Délka rozhovoru: 38 minut

Autorka: *„Můžete popsat, jaké činnosti, aktivity jako střední škola vykonáváte, a při kterých zpracováváte osobní údaje?“*

Ředitel: V první řadě poskytujeme středoškolské vzdělání, zároveň našim studentům i dalším zájemcům poskytujeme stravování ve školní jídelně. Také nabízíme určité typy vzdělávání pro zájemce z řad veřejnosti. Pro veřejnost připravujeme i několikrát do roka různé aktivity, akce a někdy jsou tyto akce omezené počtem, takže v těchto případech sbíráme také osobní údaje.

Autorka: *„Jak jste si poradili s Nařízením GDPR a implementací stanovených povinností, které vešlo v platnost v roce 2018, znamenalo toto nařízení pro vás mnoho změn?“*

Ředitel: V roce, kdy vešlo nařízení v platnost jsem ještě nebyl na této pozici, ředitelem školy jsem
se stal až [redacted], to bych rád, aby zaznělo hned na začátek. Postupně se probírám smlouvami, předpisy a vším, co škola musí splňovat a dodržovat. Ne všechny tyto dokumenty byly v pořádku za předchozího vedení, a tak se to snažíme postupně napravit. Co se týče GDPR, tak škola má od roku 2018 smlouvu s externí firmou, která má zajišťovat vše potřebné včetně pověřence. Podle smlouvy by škola měla mít vše v tomto ohledu zajištěno. Od doby mého nástupu do funkce
se marně snažíme, aby firma plnila své náležitosti dle smlouvy, jak to fungovalo dříve nevím. Každopádně máme pochyby, zda je u nás opravdu vše v souladu s požadovaným stavem.

Autorka: *„Jaké konkrétní náležitosti podle vás externí firma neplní?“*

Ředitel: Za celou dobu, co „řediteluju“ se nám nepodařilo přidělenou pověřenkyni k nám do školy dostat. Ať už aby s námi probrala potřebné věci, nebo aby proškolila zaměstnance. Pokud potřebujeme nějaké souhlasy s GDPR například pro studenty, kteří k nám nově nastupují, tak většinou obdržíme nějaký standardizovaný formulář s tím, ať si jej upravíme podle potřeby. Za sebe mohu říct, že s tímto přístupem nejsem vůbec spokojen a chceme to nějak řešit, ale toho, co řešíme denně je spousta a zatím jsme se k tomuto ještě nedostali.

Autorka: *„Říkáte, že minimálně od 06/2021 nebyl nikdo z vaší organizace pověřencem proškolen ohledně zpracovávání osobních údajů a obecně v problematice GDPR. Jak jste tuto skutečnost řesili? Snažili jste se například zaměstnance seznámit s problematikou GDPR jiným způsobem?“*

Ředitel: Bohužel je to tak, opakovaně žádáme externí firmu o schůzku s pověřencem a o možnost proškolení nás i zaměstnanců, ale stále se nám to nepodařilo. Za tu dobu k nám dokonce nastoupilo minimálně 8 nových zaměstnanců, a to jak pedagogičtí i nepedagogičtí pracovníci. A zcela upřímně, zaměstnanci nejsou nijak proškoleni, nezajišťovali jsme to jiným způsobem, stále se snažíme přimět externí firmu, aby toto školení zajistila přímo ona.

Autorka: *„Jsou nějaká nařízení, například v nějaké směrnici, která stanovují, jak zaměstnanci mají nakládat s osobními údaji?*

Ředitel: V rámci smluv podepisují zaměstnanci mlčenlivost a zmiňovaná směrnice zavazuje zaměstnance k bezpečnému nakládání s osobními údaji, se kterými přijdou v rámci pracovní činnosti
do styku. Zaměstnanci mají také vyhrazené uzamykatelné skříně pro ukládání fyzických dokumentů s osobními údaji dle jejich pracovní náplně, kam mají uzamykat podklady po skončení pracovní doby, stejně tak musí dbát na bezpečnost i přidělených IT zařízení proti odcizení, zpřístupnění apod.

Autorka: ***„V jakých dalších oblastech máte pochybnosti, zda jsou z hlediska GDPR dodržovány, respektive nedodržovány?“***

Ředitel: Smlouva, kterou máme se zmiňovanou externí firmou podepsanou, obsahuje, že všechny náležitosti, které musí naše organizace z důvodu GDPR dodržovat, budou zajištěny externí firmou. Předpokládám, že bývalé vedení školy spoléhalo na tuto smlouvu. Mé pochybnosti už zazněly a týkají se právě neplnění uvedených povinností. Možná ještě mě napadá kamerový systém, ale to je právě
o tom, aby sem pověřenkyně přijela a vše jsme to s ní mohli projít a posoudit.

Autorka: ***„Jaké podklady máte od externí firmy z hlediska GDPR k dispozici a jaké podklady za vás tato organizace zpracovává?“***

Ředitel: Máme od externí firmy vypracované Informační memorandum, které je umístěno na našem webu a někde určitě máme i směrnici. Pokud jsme někdy potřebovali nějaký formulář, tak jsme si o něj napsali a byl nám zaslán standardizovaný vzor. O jiných podkladech nevím, možná bych ještě něco dohledal v emailech. Zároveň musím přiznat, že nemám k dispozici přehled podkladů, které za nás eviduje externí firma, ale věřím, že v případě vyžádání nebude problém nám tyto údaje zpřístupnit.

Autorka: ***„Zmiňoval jste formuláře a standardizované vzory. Jaké náležitosti, které souvisí s GDPR, si zajišťujete sami nebo například ve spolupráci s externí firmou?“***

Ředitel: Vždy na začátku roku dáváme podepsat novým studentům souhlasy s GDPR, formuláře k těmto souhlasům máme právě od externí firmy. Všechny souhlasy si kompletně evidujeme a zajišťujeme my sami. Nic dalšího mě asi v tuto chvíli už nenapadá.

Autorka: ***„Jak jsou na tom vaše počítačové systémy a využívané online nástroje z hlediska zabezpečení proti úniku informací?“***

Ředitel: Využíváme online systém Bakalář pro základní administrativu. V tomto systému jsou nahrané potřebné informace o studentech, ale přístupy pedagogů jsou omezené, každý vidí pouze ty údaje, které jsou pro něj potřebné. Například pokud nejste třídním učitelem, můžete pouze zapisovat známky
a docházku k jednotlivým žákům, nemáte přístupy k dalšímu osobním údajům. Všechny přístupy
do Bakalářů, pracovních emailů, počítačů nebo přidělených notebooků probíhají pod hesly. U zaměstnanců se elektronicky zpracovávají pouze platby, a k nim má opět přístup jen úzký okruh lidí.

Autorka: ***„Jaké agendy pro vás zpracovávají externí firmy, a zároveň tyto agendy pracují i s osobními údaji studentů, zaměstnanců atp.?“***

Ředitel: Například na mzdy máme externí účetní, servery i kamerový systém nám zajišťuje i obstarává externí IT firma. Možná by se ještě našlo pár dalších věcí, ale teď si nevzpomenu.

Autorka: ***„Jak často přichází požadavky na uplatnění práv subjektů údajů, stížnosti na zpracování osobních údajů a kolik incidentů na zabezpečení osobních údajů evidujete?“***

Ředitel: Předpokládám, že se lidé budou v těchto případech primárně obracet na pověřence a následně se ke mně tyto informace dostanou. Za dobu, po kterou jsem ředitelem, ale o žádném požadavku, stížnosti, incidentu ani ničem podobném nevím.

Autorka: *„Do jakých projektů jste jako škola zapojeni? Dochází například k předávání osobních údajů i do zemí EU nebo dokonce zemí mimo EU.“*

Ředitel: Jestli se ptáte například na projekt Erasmus+, tak musím přiznat, že v tomto ohledu naše škola pokulhává a zatím se nám nepodařilo realizovat žádné zahraniční pobyty, stáže ani exkurze.
Do budoucna to určitě máme v plánu, ale momentálně toto u nás neprobíhá.

Autorka: *„Jak byste zhodnotil ochranu osobních údajů ve vaší organizaci, může podle Vás takto nastavený systém fungovat dál?*

Ředitel: I přes uvedené obavy věřím, že ano. Informace o studentech i zaměstnancích máme uložené v příslušných kartotékách a přístup ke složkám má pouze omezené množství lidí. Podklady jsou v kancelářích, které zamykáme a jsou zakódovány alarmem, zároveň jsou veřejné, prostory a jednotlivé vstupy podchyceny velmi dobře kamerovým systémem.

Autorka: *„Pane řediteli, děkuji za zodpovězení dotazů, v tuto chvíli je to za mě zatím vše.“*

Zdroj: (vlastní zpracování, 2023)

Příloha 2 Tabulky

Tabulka 2: Seznam evidovaných dokumentů a podkladů externí firmou pro organizaci XY

1	Informační memorandum se zpracováním osobních údajů a informovaný souhlas
2	Vnitřní směrnice k ochraně osobních údajů
3	Záznam o činnostech organizace XY
4	Dohoda o mlčenlivosti k ochraně utajovaných skutečností ve škole pro zaměstnance
5	Souhlas se zpracováním osobních údajů pro studenty i zaměstnance
6	Smlouva o zpracování osobních údajů pro studentské praxe
7	Smlouva o poskytování poradenských služeb v oblasti agendy ochrany osobních údajů

Zdroj: (vlastní zpracování, 2023)

Tabulka 3: Pořadí kritérií DPO dle vedení organizace

Pořadí	**Výhody**	Pořadí	**Nevýhody**
1	Kancelář v organizaci	1	Vyšší náklady
2	Nižší náklady	2	Nutnost proškolení
3	Znalosti z více organizací	3	Kancelář mimo organizaci
4-5	Znalost organizace	4	Dovolená, nemoci
4-5	Nepřetržitá služba	5	Neznalost organizace
6	Eliminace střetu zájmů	6	Hrozba střetu zájmů

Zdroj: (interní dokumenty, 2023)

Tabulka 5 Průzkum trhu 1 – cena za služby externího DPO

	Sensio.cz	**Mgr. Martin Chval**	**Bell Consulting s.r.o.**
Činnost	DPO – poradenská činnost	DPO – poradenská činnost	DPO – poradenská činnost
Omezení	Pouze telefon, email	-	-
*Cena	2 178 Kč – 3 hodiny měsíčně	Od 5.000 Kč / měsíc	Od 3.000 Kč /měsíc

*Uvedené částky jsou pouze za poradenské služby. V souhrnu musí být počítáno s dalšími náklady, a to například za tvorbu dokumentace, vedení evidencí, školení zaměstnanců atd.

Zdroj: (vlastní zpracování, 2023), stav k 6.6.2023

Tabulka 6 Záznam z kontroly čistého stolu

Kontrolu provedl/a:	[redacted]	Bc. Simona Kyjovská
Termín kontroly:	5.5.2023	
Stručný popis kontroly:	Kontrola proběhla v pozdních odpoledních hodinách po skončení pracovní doby zaměstnanců. Kontrola byla provedena v několika kancelářích, učebnách a kabinetech, které byly vybírány namátkově.	
Závěr kontroly:	Celkem byly zkontrolovány 3 kanceláře, 4 kabinety a 4 třídy, z toho 1 kancelář, 1 kabinet a 2 třídy obsahovaly volně přístupné nezajištěné nebo chybně vyvěšené materiály	

Zdroj: (vlastní zpracování, 2023)

Tabulka 8 Škála pro stanovení délky trvání projektu na základě logického odhadu času

Činnost	Odhad času dle zkušeností (ve dnech)
Revize formulářů, předpisů s jednoznačně definovanými úpravami. Tvorba formulářů, předpisů podle vzoru a jednoznačně vymezené kontroly dokumentů.	1
Jednoznačně definované úkoly provázané na IT systémy, revize a procesy s rozsáhlejším nebo nejednoznačným zpracováním bez návaznosti na IT oblast.	2
Rozsáhlejší revize a procesy související s IT oblastí, úkoly vyžadující si specifickou činnost v podobě orientace v zákonech a předpisech.	3-4
Úkoly, při kterých je potřeba zajištění a součinnost i dalších osob (zaměstnanci, externí firmy), s výjimkou proškolení vlastních zaměstnanců.	5-6

Zdroj: (interní dokumenty, 2023)

Tabulka 12 Průzkum trhu 2 – školení GDPR

	TAYLLORCOX	**GDPR Support s.r.o.**	**KRUCEK s.r.o.**	**CeMS-CO s.r.o.**	**GDPR Certifikace & Compliance s.r.o.**
Typ školení	Pro pověřence	Pro pověřence	Pro pověřence	Soulad GDPR a zákona č. 101/2000 Sb.	Pro pověřence
Přidaná hodnota	Certifikát, školící materiály	Certifikát, hodina online konzultace	Certifikát, školící materiály	-	Certifikát
Místo školení	Praha/online	Přednatočená videa	Online	Online	Praha
Čas školení	2 dny	-	5 dnů	1 den	3 dny
Cena vč. DPH	13.310 Kč	4.999 Kč	33.990 Kč	4.719 Kč	18.150 Kč

Zdroj: (vlastní zpracování, 2023) stav k 8.6.2023

Příloha 3 Výčet účelů z formuláře Souhlas se zpracováním osobních údajů

- Pořízení fotografií, videozáznamů a audiozáznamů při vyučování a na akcích, kterých se škola účastní za účelem zveřejnění a propagace školy
  - ANO/NE
- Zveřejnění fotografií, videozáznamů, audiozáznamů na webových stránkách školy
  - ANO/NE
- Předání ke zveřejnění za účelem propagace školy: Městu Kolín, Středočeskému kraji, zahraničním partnerům školy
  - ANO/NE
- Zveřejnění ve školní kronice, fotoalbu, výroční zprávě, na nástěnce vně i v okolí školy
  - ANO/NE
- Zveřejnění v místním tisku např. Kolínský týdeník Pres a v dalších médiích
  - ANO/NE
- Zveřejnění v rámci propagace školy na veřejných akcích a propagačních materiálech, na kanálu školy YOUTUBE
  - ANO/NE
- Předání pořadateli akcí a soutěží, kterých se škola účastní
  - ANO/NE
- Předání společnostem a agenturám zajišťujícím dopravu, ubytování, stravování, program, pojištění na akcích školy (exkurze, zájezd, program Erasmus atd.)
  - ANO/NE
- Předání informací v rámci programu Erasmus +
  - ANO/NE
- Vystavení výtvarných prací a fotografií za účelem propagace školy
  - ANO/NE

Zdroj: (interní dokumenty, 2023)

Příloha 4 Dotazníky

Dotazník 1

Dotazníkový formulář pro zaměstnance organizace XY

Dobrý den,

tímto Vás chci požádat o vyplnění dotazníku, který se vztahuje k problematice GDPR ve vaší organizaci. Vyplnění dotazníku je zcela anonoymní a jeho vyplnění nezabere víc než pár minut Vašeho času.

Výsledky dotazníku budou využity pro diplomovou práci, která se zaměřuje na implementaci GDPR.

1. Proškolil Vás zaměstnavatel v oblasti GDPR?
   - Ano, pravidelně
   - Ano, jednou
   - Ne
   - Nepamatuji si

2. Jak často byste uvítal/a školení ohledně GDPR?
   - 1x ročně
   - 2x ročně
   - Jiné:

3. Jakou formou by školení mělo probíhat?
   - Prezenčně
   - Online – například přes MS Teams
   - E-learning

4. Popište stručně svými slovy, co to je GDPR, čeho se týká:
   ……

5. Označte pojmy, o kterých si myslíte, že představují osobní údaje:
   - Jméno, příjmení, adresa
   - Fotografie
   - Kamerový záznam
   - Služební telefonní číslo
   - Zdravotní stav
   - Sídlo firmy, IČO
   - Emailová adresa: vaclav.novak@gmail.com
   - Číslo účtu firmy

6. Jak budete postupovat v případě zjištění porušení zabezpečení osobních údajů?
   - Nahlásím incident řediteli organizace
   - Budu dělat, že se nic nestalo
   - Poradím se s kolegou
   - Nahlásím incident pověřenci pro ochranu osobních údajů
   - Předám incident Dozorčímu úřadu

7. Má organizace pověřence pro ochranu osobních údajů a jsou někde uvedeny jeho kontaktní údaje?
   - Má a jeho údaje jsou uvedeny na webu školy
   - Má, ale kde jsou jeho údaje uvedeny nevím
   - Má, ale jeho údaje nejsou nikde uvedeny
   - Ne, organizace nemá pověřence
   - Nevím, zda má organizace nějakého pověřence

8. Máte v organizaci nastavena některá z těchto opatření?
   - Přihlašování do počítače a systémů pomocí hesel
   - Omezené přístupy k osobním údajům v systémech, podle pracovních pozic
   - Uzamykatelné skříně pro dokumenty s osobními údaji
   - Vypínání PC/notebooku při odchodu z pracoviště
   - Uzamčení dokumentů s osobními údaji při odchodu z pracoviště
   - Uzamčení kanceláře/kabinetu při odchodu
   - Další:

9. Jaká opatření dodržujete bez ohledu na jejich stanovení organizací?
   - Přihlašování pomocí hesel – hesla nemám předuložena
   - Dokumenty s osobními údaji uzamykám do příslušných skříní/polic
   - Při odchodu z kanceláře/kabinetu vždy uzamykám místnost
   - Při odchodu z pracoviště vypínám PC/notebook
   - Při odchodu z pracoviště dbám vždy na uložení/uzamčení všech dokumentů s osobními údaji
   - Další:

10. Jak vnímáte GDPR?
    - Je důležité a musí být dodržováno
    - Je zbytečné
    - Otravuje mě, ale respektuji ho

11. Kdy jste nastoupil/a do organizace?
    - Před květnem 2018
    - Po květnu 2018

12. Jaké je Vaše pracovní zařazení v organizaci?
    - Pedagogický pracovník
    - Nepedagogický pracovník – ekonomický úsek
    - Nepedagogický pracovník – ostatní

Děkuji za Vaše odpovědi,

Bc. Simona Kyjovská

Zdroj: (vlastní zpracování, 2023)

Dotazník 1 – Výsledky

Jednotlivé otázky s možnou variantou odpovědi:	**Absolutní četnost:**	**Relativní četnost v %:**
1. Proškolil vás zaměstnavatel v oblasti GDPR?		
- Ano, pravidelně		0,0
- Ano, jednou		0,0
- Ne		76
- Nepamatuji si		24
2. Jak často byste uvítal/a školení ohledně GDPR?		
- 1x ročně		64,0
- 2x ročně		0,0
- 1x za 2 roky		36,0
3. Jakou formou by školení mělo probíhat?		
- Prezenčně		44,0
- Online – například přes MS Teams		0,0
- E-learning		56,0
4. Popište stručně svými slovy, co to je GDPR, čeho se týká:		
- Osobních údajů		64,0
- Ochranou osobních údajů fyzických osob		24,0
- Informací o nás		12,0
5. Označte pojmy, o kterých si myslíte, že představují osobní údaje:		
- Jméno, příjmení, adresa		100,0
- Fotografie		92,0
- Kamerový záznam		92,0
- Služební telefonní číslo		16,0
- Zdravotní stav		100,0
- Sídlo firmy, IČO		0,0
- Emailová adresa: vaclav.novak@gmail.com		84,0
- Číslo účtu firmy		0,0
6. Jak budete postupovat v případě zjištění porušení zabezpečení osobních údajů?		
- Nahlásím incident řediteli organizace		76,0
- Budu dělat, že se nic nestalo		0,0
- Poradím se s kolegou		0,0

- Nahlásím incident pověřenci pro ochranu osobních údajů		24,0
- Předám incident Dozorčímu úřadu		0,0
7. Má organizace pověřence pro ochranu osobních údajů a jsou někde uvedeny jeho kontaktní údaje?		
- Má a jeho údaje jsou uvedeny na webu školy		36,0
- Má, ale kde jsou jeho údaje uvedeny nevím		24,0
- Má, ale jeho údaje nejsou nikde uvedeny		0,0
- Ne, organizace nemá pověřence		0,0
- Nevím, zda má organizace nějakého pověřence		40,0
8. Máte v organizaci nastavena některá z těchto opatření?		
- Přihlašování do počítače a systémů pomocí hesel		84,0
- Omezené přístupy k osobním údajům v systémech podle pracovních pozic		52,0
- Uzamykatelné skříně pro dokumenty s osobními údaji		24,0
- Vypínání PC/notebooku při odchodu z pracoviště		52,0
- Uzamčení dokumentů s osobními údaji při odchodu z pracoviště		24,0
- Uzamčení kanceláře/kabinetu při odchodu		100,0
- Další:		0,0
9. Jaká opatření dodržujete bez ohledu na jejich stanovení organizací?		
- Přihlašování pomocí hesel – hesla nemám předuložena		52,0
- Dokumenty s osobními údaji uzamykám do příslušných skříní/polic		24,0
- Při odchodu z kanceláře/kabinetu vždy zamykám místnost		100,0
- Při odchodu z pracoviště vypínám PC/notebook		100,0
- Při odchodu z pracoviště dbám vždy na uložení/ uzamčení všech dokumentů s osobními údaji		16,0
- Další:		0,0
10. Jak vnímáte GDPR?		
- Je důležité a musí být dodržováno		72,0
- Je zbytečné		12,0
- Otravuje mě, ale respektuji ho		16,0

11. Kdy jste nastoupil/a do organizace?		
- Před květnem 2018		60,0
- Po květnu 2018		40,0
12. Jaké je Vaše pracovní zařazení v organizaci?		
- Pedagogický pracovník		56,0
- Nepedagogický pracovník – ekonomický úsek		16,0
- Nepedagogický pracovník – ostatní		28,0

Zdroj: (vlastní zpracování, 2023)

Dotazník 2

Dotazník identifikace procesů a zpracovávaných osobních údajů v organizaci XY

Název zpracování:	Počet zaměstnanců organizace, kteří zpracovávají dané údaje:

Upřesnění vztahu organizace k danému zpracování:		
1. Správce	ano/ne	Je využíván zpracovatel: ano/ne (Pokud ano, uvést zpracovatele):
2. Zpracovatel	ano/ne	Pokud ano, uvést, kdo je správce
- jsou využíváni další subzpracovatelé?	ano/ne	Pokud ano, uvést kdo je subzpracovatel

Subjekty údajů:	
· Zaměstnanci	
· Studenti SŠ	
· Zákonní zástupci	
· Osoby do 15 let	

Právní základ zpracování:			
Osobní údaje:	ano/ne	Zvláštní kategorie osobních údajů:	ano/ne
· Souhlas		· Výslovný souhlas	
· Smlouva		· Plnění povinnosti a zvláštních práv v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a ochrany	
· Právní povinnost		· Zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas	
· Ochrana životně důležitých zájmů		· Zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace,	

		sdružení nebo jiný neziskový subjekt u svých členů …	
· Veřejný zájem		· Zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů	
· Oprávněný zájem		· Zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků	
		· Zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva Unie nebo členského státu	
		· Zpracování je nezbytné pro účely preventivního nebo pracovního lékařství	
		· Zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví	
		· Zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely	

Rozsah zpracování:	
Kolik subjektů údajů zpracování zahrnuje?	
Systematické zpracování:	
Je zpracování systematické?	

Které identifikátory jsou shromažďovány?	
jméno, příjemní	
titul	
datum narození	
rodné číslo	
pohlaví	
rodinný stav	
vzdělání	
adresa	
email	
telefon	

fotografie (podobizna)		
podpis		
Zvláštní kategorie osobních údajů:		
rasový/etnický původ		
politické názory		
náboženské vyznání		
filozofické přesvědčení		
členství v odborech		
genetické údaje		
biometrické údaje		
zdravotní stav		
sexuální život/orientace		
Informování subjektu údajů:		
Uveďte, zda je pro zpracování povinné informovat subjekty údajů, a pokud ano, zda bylo provedeno.	Informace je povinná	Informace byla podána
	ano/ne	ano/ne
Řízení incidentů:		
Uveďte, zda je zpracování zahrnuto v současném systému řízení incidentů.	Incident je řízen	Incident by měl být řízen
	ano/ne	ano/ne

Je v rámci zpracování prováděno:	
profilování	ano/ne
generalizace	ano/ne
odvozování	ano/ne
Použitá technická a organizační opatření:	
pseudonymizace	ano/ne
anonymizace	ano/ne
šifrování	ano/ne

Uveďte případně další technická a organizační opatření k zabezpečení osobních údajů (hesla, uzamčená skříň…).	
Uložení osobních údajů:	
Manuální	ano/ne
IS – pokud ano, uveďte přesné názvy programů a úložišť	ano/ne
Doba zpracování:	
Uveďte, po jakou dobu je potřebné osobní údaje shromažďovat.	
Interní odpovědnost:	
Uveďte, kdo má interní odpovědnost za toto zpracování.	
Přístupy k tomuto zpracování:	
Uveďte, kdo z interních zaměstnanců má přístup k osobním údajům v rámci tohoto zpracování.	

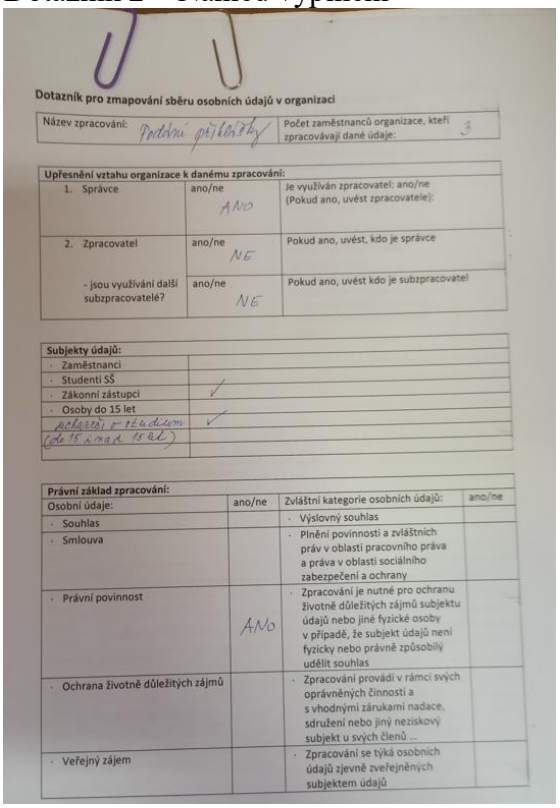
Posouzení rizik pro práva a svobody osob:	
Uveďte, zda je u tohoto zpracování přítomen některý z níže uvedených rizikových faktorů.	
Automatizované, systematické vyhodnocování osobních aspektů týkající se fyzických osob včetně profilování s následným rozhodováním s právním nebo obdobně významným účinkem.	
Rozsáhlé systematické monitorování veřejně přístupných prostorů.	
Zpracování OÚ zvláštní kategorie.	
Zpracování je rozsáhlé.	
Soubory dat, které byly porovnány nebo zkombinovány.	
Zahrnutí údajů týkajících se zranitelných subjektů údajů.	
Inovativní používání nebo uplatňování technologických nebo organizačních řešení (např. biometrika).	
Přesun dat přes hranice mimo EU.	
Pokud samotné zpracování zabraňuje subjektům údajů vykonávat právo nebo využívat službu nebo smlouvu.	

Jedná se o zpracování s vysokým rizikem pro práva a svobody osob:	ano/ne

Uveďte, jaká další rizika mohou být spojena s daným zpracováním a mohou mít dopad na ochranu a bezpečnost zpracovávaných osobních údajů:

Zdroj: (modifikace, 2023), Nezmar (2017)

Dotazník 2 – Náhled vyplnění



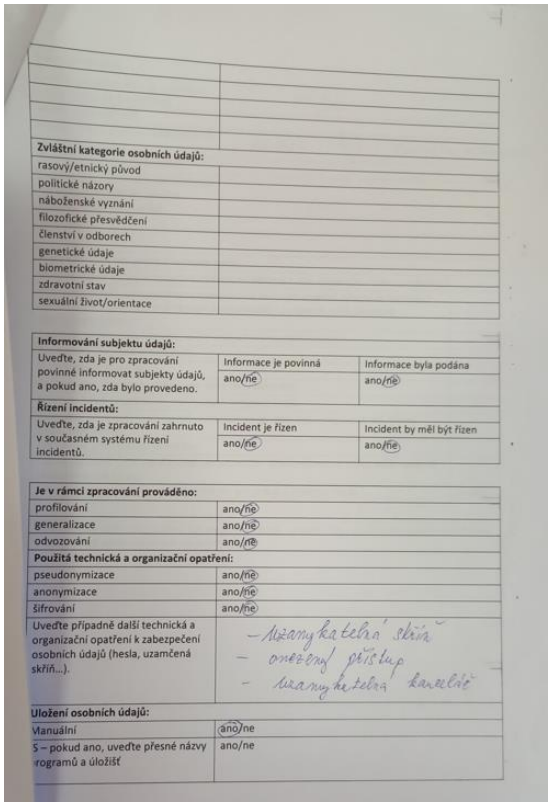
Dotazník pro zmapování sběru osobních údajů v organizaci

Název zpracování:	Počet zaměstnanců organizace, kteří zpracovávají dané údaje:
Dotační příležitosti	3

Upřesnění vztahu organizace k danému zpracování:		
1. Správce	ano/ne ANO	Je využíván zpracovatel: ano/ne (Pokud ano, uvést zpracovatele):
2. Zpracovatel	ano/ne NE	Pokud ano, uvést, kdo je správce
- jsou využívání další subzpracovatelé?	ano/ne NE	Pokud ano, uvést kdo je subzpracovatel

Subjekty údajů:	
· Zaměstnanci	
· Studenti SŠ	
· Zákonní zástupci	✓
· Osoby do 15 let	
pečovatelé o studium (do 15 i nad 15 let)	✓

Právní základ zpracování:			
Osobní údaje:	ano/ne	Zvláštní kategorie osobních údajů:	ano/ne
· Souhlas		· Výslovný souhlas	
· Smlouva		· Plnění povinností a zvláštních práv v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a ochrany	
· Právní povinnost	ANO	· Zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas	
· Ochrana životně důležitých zájmů		· Zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt u svých členů ...	
· Veřejný zájem		· Zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů	



Zvláštní kategorie osobních údajů:	
rasový/etnický původ	
politické názory	
náboženské vyznání	
filozofické přesvědčení	
členství v odborech	
genetické údaje	
biometrické údaje	
zdravotní stav	
sexuální život/orientace	

Informování subjektu údajů:		
Uveďte, zda je pro zpracování povinné informovat subjekty údajů, a pokud ano, zda bylo provedeno.	Informace je povinná ano/ne	Informace byla podána ano/ne
Řízení incidentů:		
Uveďte, zda je zpracování zahrnuto v současném systému řízení incidentů.	Incident je řízen ano/ne	Incident by měl být řízen ano/ne

Je v rámci zpracování prováděno:	
profilování	ano/ne
generalizace	ano/ne
odvozování	ano/ne
Použitá technická a organizační opatření:	
pseudonymizace	ano/ne
anonymizace	ano/ne
šifrování	ano/ne
Uveďte případně další technická a organizační opatření k zabezpečení osobních údajů (hesla, uzamčená skříň...).	– uzamykatelná skříň – omezený přístup – uzamykatelná kancelář
Uložení osobních údajů:	
Manuální	ano/ne
S – pokud ano, uveďte přesné názvy rogramů a úložišť	ano/ne

Zdroj: (interní dokumenty, 2023), stav k 31.3.2023

Příloha 5 Obrázky

Obrázek 1 Upozornění na kamerový systém

Zdroj: (vlastní zpracování, 2023), stav k 5.5.2023

Obrázek 2 Nástroj 10 Kontrolní seznam změny

Kdy:

Kontrolní seznam změny je použitelný pokaždé, když se účastníme projektu změny, kde se dá očekávat odpor zaměstnanců.

Pro koho:

Nástroj je určený pro manažery změn, projektové manažery a členy změnových týmů obecně.

Postup:

Plánování a realizace změny je proces, v němž bychom měli provést všechny důležité oblasti. Základem změny je samotný obsah změny, musí tedy vzniknout konkrétní výstup, který povede k očekávaným přínosům. Navrhnout výstup však nestačí. Změna je projekt jako každý jiný, a proto do jejího provádění vstupuje

řízení projektů z pohledu času, nákladů a kvality. Mluvili jsme o zvládání odporu. Právě to je další vrstvou řízení projektu. Vytipujte si všechny potenciální překážky a hrozby pro změnový projekt a pracujte s nimi. Další a často nejdůležitější oblast řízení změny se vztahuje ke komunikaci. Následující výčet bodů představuje to, na co bychom v rámci všech uvedených oblastí neměli zapomenout:

Řízení projektu

- Mám změnový projekt naplánovaný z pohledu času, nákladů i kvality?
- Mám sestavený projektový tým a jasně stanovené odpovědnosti jeho členů?
- Mám dostatečně přesně nadefinováno, co bude výstupem dané změny?
- Vím, která část výstupu bude realizována první jako malé vítězství?
- Promyslel jsem, co všechno jsou hlavní benefity a přínosy, které změna přinese?
- Prozkoumal jsem, do jaké míry jsou výstupy změny slučitelné se stávajícími procesy a systémy organizace?
- Vyjednal jsem pro změnu dostatek finančních i jiných zdrojů?

Zvládání odporu

- Sestavil jsem dostatečně silnou koalici, která se mnou bude prosazovat změnu, a získal jsem od jejích členů závazek ke spolupráci?
- Získal jsem na svou stranu všechny relevantní klíčové manažery a autority organizace?
- Identifikoval jsem a zmapoval všechny oponenty změny a jejich zájmy?
- Vím, jakým způsobem budu komunikovat a získávat oponenty na svou stranu?
- Identifikoval jsem všechny další překážky a rizika vyplývající z charakteru změny?
- Připravil jsem plán, jakým způsobem ošetřím všechna případná rizika a překážky?
- Promyslel jsem, do jaké míry je změna slučitelná se stávající organizační kulturou?

Komunikace

- Určil jsem si důležité cílové skupiny komunikaci a stanovil plán jak s nimi komunikovat?
- Vytvořil jsem dostatečně kvalitní vizi změny a vím, jakým způsobem ji budu komunikovat?
- Deklaroval jsem v rámci komunikace změny podporu vrcholového managementu?
- Mám připravený komunikační plán pro jednotlivé fáze změny?
- Identifikoval jsem všechny skupiny zaměstnanců, které bude potřeba zaškolit?
- Sestavil jsem plán pro školení zaměstnanců a připravil školicí materiály?

Zdroj: (Novák, 2016)

Obrázek 3 Body pro balanční test

1. Posouzení váhy oprávněného zájmu
Každý oprávněný zájem má jinou váhu a význam. Oprávněné zájmy můžeme rozdělit do několika skupin (v pořadí od nejvýznamnějších): a) výkon základních práv a svobod (například ochrana vlastnictví) b) veřejné zájmy nebo zájmy širší komunity (například předcházení podvodům) c) subjektivní zájmy správce (například přímý marketing)
2. Posouzení důsledků zpracování pro subjekty údajů (negativních i pozitivních)
Jedná se o identifikaci jakýchkoliv důsledků zpracování, které mohou vyplynout ze zpracování samotným správcem, ale také z jednání jiné osoby například po předání nebo zveřejnění osobních údajů. Je nutné posoudit pravděpodobnost, že určitá újma vznikne, její závažnost a přiměřenost či nepřiměřenost. K tomu poslouží následující vodítka: a) povaha zpracovávaných osobních údajů (standardní, nebo citlivé údaje) b) způsob zamýšleného zpracování a jeho rizikovost c) postavení a vztah mezi správcem a subjektem údajů d) oprávněná očekávání subjektu údajů ohledně zpracování
3. Vyvážení oprávněného zájmu a jeho důsledků pro subjekt údajů
Správce provede poměření oprávněného zájmu se zájmy a právy subjektů, do nichž bude zpracováním osobních údajů zasaženo, s ohledem na rizikovost důsledků zpracování a pravděpodobnosti jejich vzniku. Aby správce mohl využít oprávněný zájem jako právní titul ke zpracování osobních údajů, musí výše uvedené poměření skončit závěrem, že zájmy a práva subjektu údajů nepřevažují nad zájmem správce.
4. Přijetí dodatečných záruk pro ochranu práv a svobod subjektu údajů
Pokud je výsledek balančního testu nejednoznačný nebo velmi těsný ať už pro subjekt údajů, nebo správce, je možné přijmout dodatečná opatření, aby nakonec došlo k jasnému převážení oprávněného zájmu. Může se jednat o zvýšenou transparentnost a odpovědnost správce za dané zpracování nebo je možné poskytnout subjektu údajů větší kontrolu nad zpracováním či neomezené právo na námitku proti zpracování.

Zdroj: (Valentová, 2023)

Obrázek 4 Metoda PZH – škály

P – pravděpodobnost vzniku a existence nebezpečí

Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Z – závažnost možných následků ohrožení

Poškození údajů bez následků pro subjekty údajů	1
Poškození s minimálními následky pro subjekty údajů	2
Poškození dat bez trvalých následků pro subjekty údajů	3
Poškození dat se závažnými následky pro subjekty údajů	4
Poškození dat s fatálními následky ohrožujícími život subjektů údajů	5

H – názor hodnotitelů

Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

Stupeň rizika	**Celkové riziko R**	**Míra rizika**
I.	> 100	Nepřijatelné riziko
II.	51 ÷ 100	Nežádoucí riziko
III.	11 ÷ 50	Mírné riziko
IV.	3 ÷ 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Vzorec celkového rizika: R = P x Z x H

Zdroj: (Nezmar, 2017)

Obrázek 5 Zakládací listina projektu

Název projektu:	**Transformace implementovaného GDPR do procesního řízení** [redacted]
Číslo projektu:	[redacted]
Přínosy:	Soulad s GDPR, zlepšení systému bezpečnosti a ochrany osobních údajů
Cíl projektu:	Naplnění povinností vyplývajících z GDPR
Plánované náklady:	**50 000 Kč**
Plánovaný termín zahájení:	**20.06.2023**
Plánovaný termín dokončení:	**31.08.2023**
Kritéria úspěšnosti:	Dodržení termínu Dodržení rozpočtu Naplnění úkolů viz příloha 1 Úspěšná kontrola viz příloha 2
Schválené výjimky:	Nejsou
Zadavatel projektu:	[redacted]
Supervizor projektu:	[redacted]
Členové projektu:	[redacted]
Odměny projektového týmu:	Každému členovi náleží 140 Kč za 1 odpracovanou hodinu na projektu.

Datum schválení:	12.06.2023
Schváleno:	[redacted]

Zdroj: (interní dokumenty, 2023)

VŠEM VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU

Návrh transformace implementovaného GDPR do procesního řízení vybrané organizace

Bc. Simona Beneš Kyjovská, KEMMA05

Řešená problematika

úvod

Systém bezpečnosti a ochrany osobních údajů v organizaci a shoda s platnou legislativou.

problém

Zajištění souladu a implementace GDPR do procesů organizace.

přístup

Tvorba návrhu projektu transformace implementovaného GDPR do změnového řízení organizace.

Postup řešení

zdroj

Tuzemské a zahraniční, právní předpisy, směrnice, nařízení, interní zdroje a data, ostatní prameny.

získávání

Literární rešerše
Kvalitativní a kvantitativní výzkum, analýza interních dokumentů, komparace výsledků a dat, datový audit, GAP analýza

zpracování

Ganttův diagram, analýza rizik, kalkulace nákladů

Výsledky práce

Tabulka 1: Výhody a nevýhody externích a interních DPO (pověřenec pro ochranu osobních údajů)

	Externí DPO	b_i	Interní DPO	b_i
Výhody	Nepřetržitá služba	3 (0,14)	Kancelář přímo v organizaci	5 (0,24)
	Znalosti z více organizací	4 (0,19)	Komplexní znalost organizace	3 (0,14)
	Eliminace střetu zájmů	2 (0,10)	Potenciálně nižší náklady	4 (0,19)
Součet všech výhod za obě varianty				21
Nevýhody	Kancelář mimo organizaci	3 (0,16)	Dovolená, nemoci	3 (0,16)
	Neznalost organizace	2 (0,11)	Nutnost proškolení	4 (0,21)
	Vyšší náklady	5 (0,26)	Hrozba střetu zájmů	2 (0,11)
Součet všech nevýhod za obě varianty				19

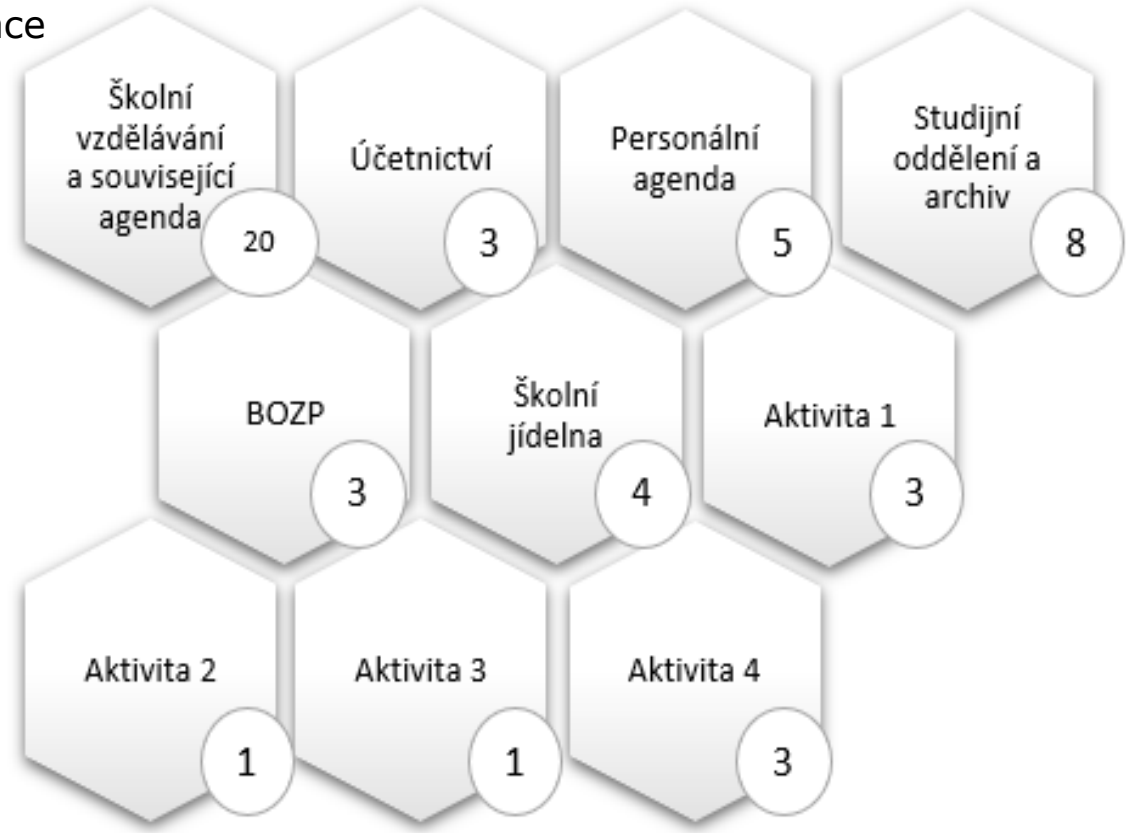
	min	max
Výhody	<1,5>	
Nevýhody	<5,1>	

Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Datový audit

Diagram 1: Hlavní procesy organizace

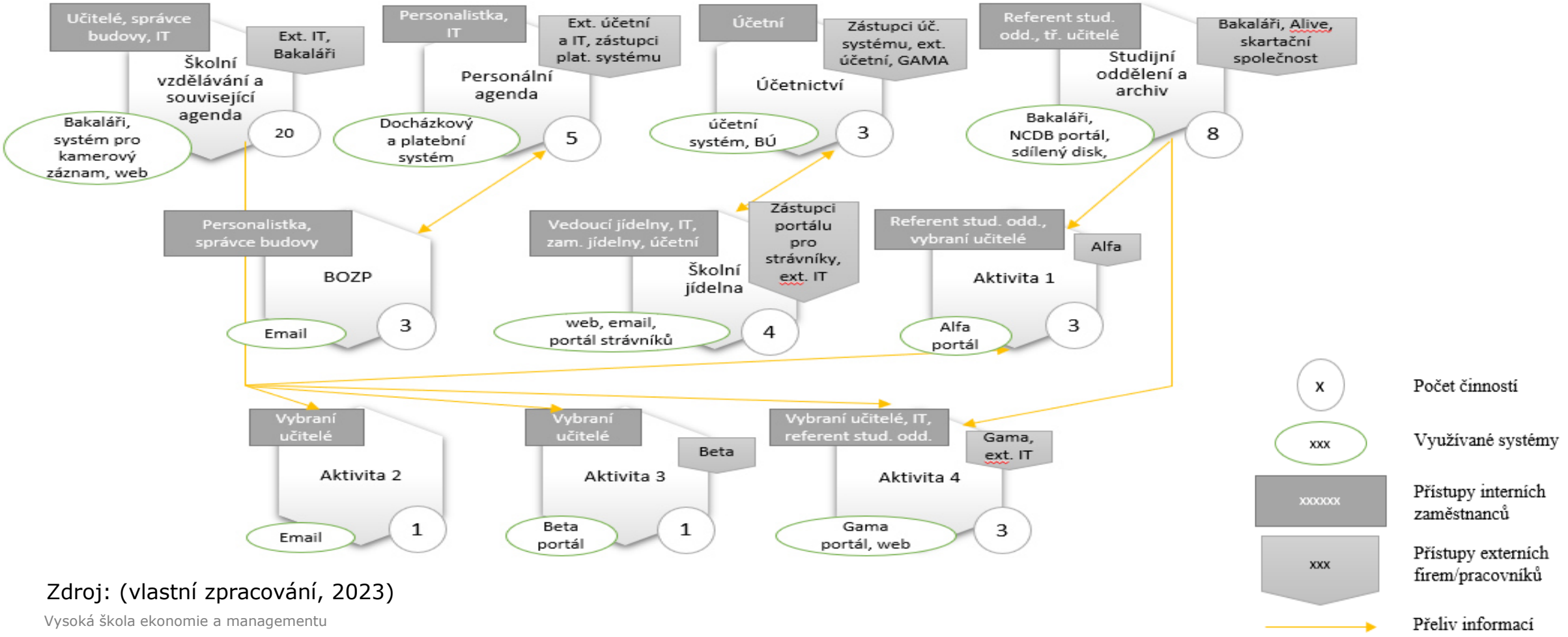


Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Datový audit

Diagram 2: Hlavní procesy organizace – rozšířené o detail

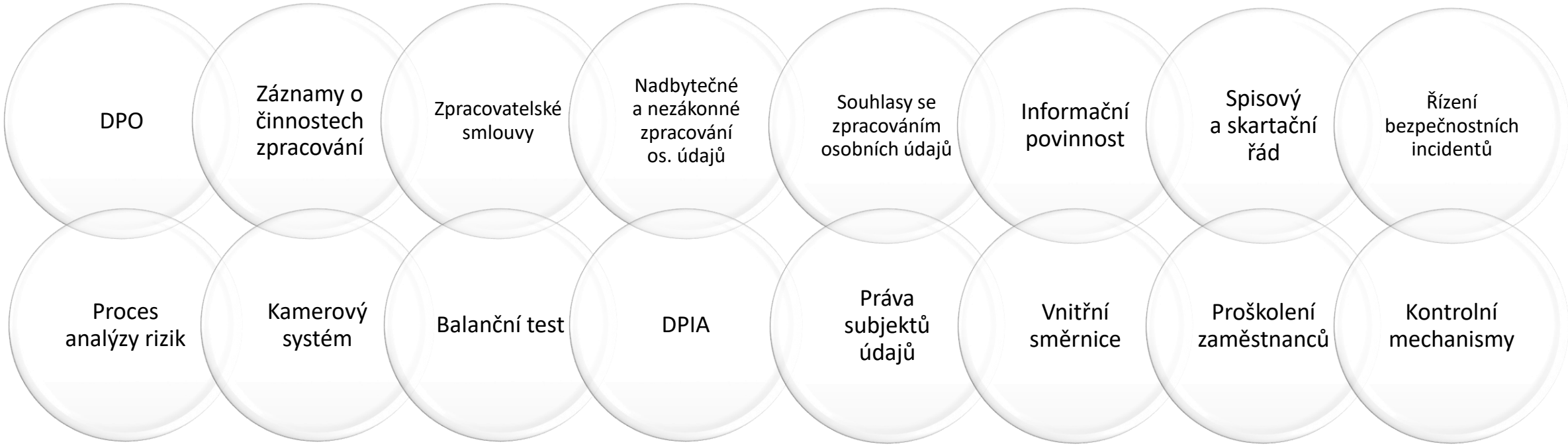


Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Datový audit – GAP analýza

Obrázek 1: Identifikované mezery



Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Rozsah projektu

Tabulka 2: Přehled činností projektu

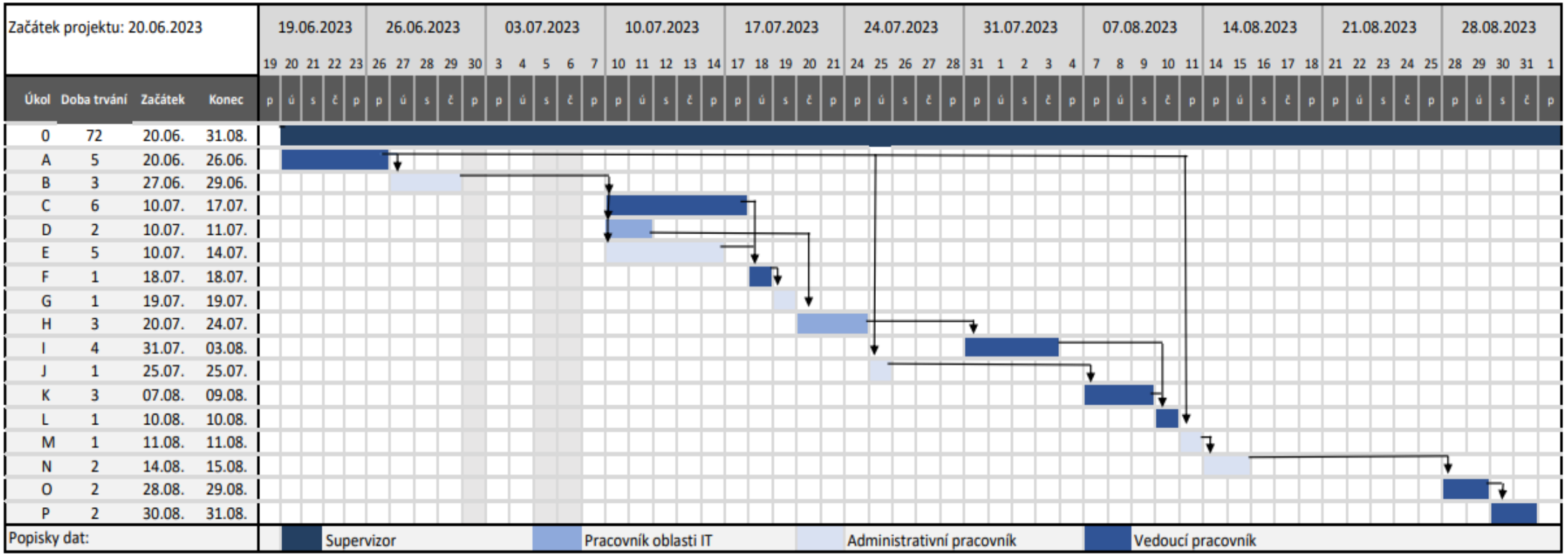
Činnost	Popis činnosti	Doba trvání ve dnech	Předchozí činnost
A	Zajištění nového DPO a zajištění agendy vedení evidencí	5	-
B	Revize záznamů o činnostech zpracování	3	A
C	Nastavení procesu ověřování zpracovatelů před podepsáním smlouvy. Vytvoření standardizovaných dodatků a zajištění 4 dodatků k probíhajícím smlouvám.	6	A, B
D	Zamezení zpracovávání identifikovaných nadbytečných nebo nezákonných osobních údajů včetně příslušných opatření	2	A, B
E	Revize formulářů pro udělení souhlasů se zpracováním osobních údajů včetně příslušných opatření	5	A, B
F	Zajištění informační povinnosti o zpracovávání osobních údajů u 6 identifikovaných činností	1	A, B, C, D, E
G	Revize spisového a skartačního řádu	1	A, B, F
H	Nastavení procesu řízení bezpečnostních incidentů, stanovení plánu reakcí a vymezení samostatného dokumentu	3	A, B, C, D
I	Nastavení procesu analýzy rizik	4	A, B, H
J	Revize informačních cedulí kamerového systému	1	A
K	Provedení balančního testu ke kamerovému systému	3	A, B, J
L	Zajištění prvotního DPIA dle pokynů WP248	1	A, B, I, K
M	Vytvoření formulářů pro uplatnění práv subjektů údajů	1	A
N	Revize vnitřní směrnice	2	A, B, C, H, G, I, L, M
O	Proškolení všech zaměstnanců o ochraně osobních údajů a jejich seznámení s veškerými změnami a nastavení školícího plánu	2	A, C, D, E, F, G, H, I, J, K, L, N
P	Nastavení kontrolních mechanismů	2	H, I, L, N, O

Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Časové znázornění projektu

Tabulka 3: Ganttův diagram



Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Zhodnocení významu a přínosu projektu

Tabulka 4: Analýza rizik návrhu projektu

Činnost	Zdroj rizika	Identifikace nebezpečí	Hodnocení závažnosti rizika				Bezpečnostní opatření
			P	Z	H	R	
Transformace implementovaného GDPR do změnového řízení	Časové zpoždění projektu	Chybné zpracování osobních údajů dalších subjetů údajů	2	3	3	18	Důkladná příprava časového harmonogramu
	Chybná vstupní data projektu	Neidentifikování všech nesouladů s GDPR	3	4	4	48	Důkladné vymezení a kontrola vstupních dat projektu, nastavení procesů a kontrolních mechanismů průběžně hodnotících soulad s GDPR.
	Neproškolení zaměstnanci	Únik osobních údajů	3	4	4	48	Naplánované školení a jeho důkladné provedení
	Chybná transformace	Nedostatečné nebo chybné pochopení povinností GDPR	3	4	4	48	Důkladné nastudování GDPR a příslušných podkladů
	Nedostatečné informování změny	Nepřijetí změnového řízení ze strany zaměstnanců	3	3	3	27	Vhodně zvolená komunikace projektu směrem k zaměstnancům

Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Zhodnocení významu a přínosu projektu

Tabulka 5: Kalkulace nákladů návrhu projektu v doporučené variantě

Název nákladové položky	Částka za odpracovanou hodinu	Doba trvání	Náklady celkem
Práce na projektu 1. zaměstnanec	140 Kč	96 hodin	13 440 Kč
Práce na projektu 2. zaměstnanec	140 Kč	52 hodin	7 280 Kč
Práce na projektu 3. zaměstnanec	140 Kč	20 hodin	2 600 Kč
Práce na projektu supervizor	140 Kč	57 hodin	7 980 Kč
Čas strávený na školení	140 Kč	16 hodin	2 240 Kč
Školení nového pověřence	-	-	13 310 Kč
Cestovné	-	-	1 000 Kč
Celkem	**-**	**-**	**47 850 Kč**

	Interní/ext.	cena školení
Real. - doporučená	Interní DPO	13 310,00 Kč
Optimistická	Interní DPO	do 5 000,00 Kč
Pesimistická	Interní DPO	od 18 000,00 Kč

Zdroj: (vlastní zpracování, 2023)

Výsledky práce

Shrnutí projektu

Tabulka 6: Závěrečné posouzení návrhu projektu

	Požadavky vedení organizace XY	Návrh projektu v doporučené variantě
Náklady	50.000 Kč	47.850 Kč
Termín	Do 1.9.2023	Do 1.9.2023
Lidské zdroje	4	4

Zdroj: (vlastní zpracování, 2023)

Přínos

1. **Naplnění souladu systému ochrany osobních údajů s GDPR, eliminace hrozby sankcí, úspora nákladů díky zajištění nového pověřence pro ochranu osobních údajů z řad interních zaměstnanců**

2. **Metodická pomůcka k provedení datového auditu a ověření souladu s GDPR s uvedením vzorového příkladu**

3. **Nezbytnost pravidelné a důkladné kontrolní činnosti dodržování s GDPR v integraci nedostatečné implementace povinností**

Závěr

- Práce přinesla identifikaci mezer mezi plánovaným a reálným stavem systému ochrany osobních údajů v souladu s GDPR procesně řízené organizace.
- Novým řešením je realizace navrženého projektu na základě metodického pokynu s uvedením názorného příkladu.
- Problematika byla posunuta díky otevření odborného tématu chybných implementací GDPR včetně zpracování návrhu metodického postupu lze problematiku řešit komplexně, systematicky a aplikovat ji do procesního řízení vybrané organizace.
- Přidaná hodnota kvalifikační práce spočívá v ekonomickém, sociálním a udržitelném paradigma procesně řízené organizace.


VŠEM
VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU
DĚKUJI ZA POZORNOST

Průzkumy trhu k doporučené variantě

Tabulka 7: Průzkum trhu 2 – cena za služby externího DPO

Firma	Sensio.cz	Mgr. Martin Chval	Bell Consulting s.r.o.
Činnost	DPO – poradenská činnost	DPO – poradenská činnost	DPO – poradenská činnost
Omezení	Pouze telefon, email	-	-
***Cena**	2 178 Kč – 3 hodiny měsíčně	Od 5.000 Kč / měsíc	Od 3.000 Kč /měsíc

Zdroj: (vlastní zpracování, 2023)

Tabulka 8: Průzkum trhu 2 – školení GDPR

Firma	TAYLLORCOX	GDPR Support s.r.o.	KRUCEK s.r.o.	CeMS-CO s.r.o.	GDPR Certifikace & Compliance
Typ školení	Pro pověřence	Pro pověřence	Pro pověřence	GDPR a zákona č. 101/2000 Sb.	Pro pověřence
Přidaná hodnota	Certifikát, školící materiály	Certifikát, hodina online konzultace	Certifikát, školící materiály	-	Certifikát
Místo školení	Praha/online	Přednatočená videa	Online	Online	Praha
Čas školení	2 dny	-	5 dnů	1 den	3 dny
Cena vč. DPH	13.310 Kč	4.999 Kč	33.990 Kč	4.719 Kč	18.150 Kč

Zdroj: (vlastní zpracování, 2023)

Kritéria výběru DPO

Tabulka 9: Pořadí kritérií DPO dle vedení organizace XY

Pořadí	Výhody	Pořadí	Nevýhody
1	Kancelář v organizaci	1	Vyšší náklady
2	Nižší náklady	2	Nutnost proškolení
3	Znalosti z více organizací	3	Kancelář mimo organizaci
4-5	Znalost organizace	4	Dovolená, nemoci
4-5	Nepřetržitá služba	5	Neznalost organizace
6	Eliminace střetu zájmů	6	Hrozba střetu zájmů

Zdroj: (interní dokumenty, 2023)