VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH OCHRANY OSOBNÍCH DAT DLE OBECNÉHO NAŘÍZENÍ EU 2016/679 ZE DNE 27. DUBNA 2016

THE PROPOSAL FOR PERSONAL DATA PROTECTION ACCORDING TO THE GENERAL REGULATION (EU) 2016/679 OF 27 APRIL 2016

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Julie Bartoňová

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Julie Bartoňová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2017/18

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh ochrany osobních dat dle obecného nařízení EU 2016/679 ze dne 27. dubna 2016

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Hlavním cílem práce je na základě analytické části podat návrhy a doporučení pro uvedení vybrané společnosti do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016. Dílčím cílem je poté vyhotovení teoretického pozadí k řešené tématice, dále vytvoření nezbytných analýz, a nakonec samotný návrh vlastního řešení.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky, Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK P., V. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

ONDRÁK V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Tato diplomová práce řeší návrh ochrany osobních dat v souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016 (obecně známém pod zkratkou GDPR) ve vybrané společnosti. Práce je uvozena teoretickým pozadím, na které navazuje část řešící analýzu společnosti, jejíž výsledky jsou dále konfrontovány s vlastním řešením podávajícím návrhy a doporučení pro uvedení vybrané společnosti do souladu s GDPR.

Abstract

This diploma thesis solves the proposal for personal data protection according to the Regulation (EU) 2016/679 of 27 April 2016 (generally known under the abbreviation GDPR) in a chosen company. The thesis begins with a theoretical background followed by the part devoted to the analysis of the company. These results are further confronted with the own solution which is presenting the proposals and recommendations to bring the selected company into line with the GDPR.

Klíčové slova

GDPR, ochrana osobních dat, nařízení EU, analýza rizik

Key words

GDPR, personal data protection, EU regulation, risk analysis

Bibliografická citace

BARTOŇOVÁ, J. *Návrh ochrany osobních dat dle obecného nařízení EU 2016/679 ze dne 27. dubna 2016*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 115 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 14. května 2018

.....

podpis studenta

Poděkování

Děkuji panu Ing. Petru Sedlákovi nejen za vedení mé práce, ale také za praktické poznatky, jež vedly k lepším výsledkům.

OBSAH

ÚVOD

Vlivem rychlého vývoje informačních technologií a zvyšování zájmu o ochranu soukromí fyzických osob došlo v rámci evropských institucí k několikaletému procesu rozebírajícím tématiku ochrany osobních údajů, který vyústil ve vytvoření Obecného nařízení o ochraně osobních údajů obecně známém jako GDPR.

Jelikož toto nařízení má být uvedeno v účinnost krátce po dopsání této diplomové práce, jedná se o velmi aktuální téma. Nařízení má být účinné od 25. května 2018 a má mířit na ochranu osobních údajů všech občanů Evropské unie.

Nutnost zvýšení bezpečnosti osobních údajů potvrdily například nedávné bezpečnostní incidenty sociální sítě Facebook, ze které unikly osobní údaje několika milionů uživatelů.

Cílem této diplomové práce je podat návrhy a doporučení pro uvedení vybrané společnosti do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016.

Po uvedení základního teoretického pozadí následuje analytická a návrhová část. Kapitoly jsou vzájemně propojeny – analytická část doplňuje návrhovou, přičemž obě byly vytvořeny za úzké spolupráce s vedením řešené společnosti.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Hlavním cílem práce je na základě analytické části podat návrhy a doporučení pro uvedení vybrané společnosti do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016.

Dílčím cílem je poté vyhotovení teoretického pozadí k řešené tématice, dále vytvoření nezbytných analýz, a nakonec samotný návrh vlastního řešení.

1 TEORETICKÁ VÝCHODISKA

Kapitola s teoretickými východisky podává čtenáři shrnující rámec základních témat řešených v rámci této práce. Jedná se především o hlavní témata jako GDPR, systém řízení bezpečnosti informací, normy řady ISO/IEC 27000 včetně jejich spojitosti s GDPR, rozbor „7 S faktorů“, Lewinův model řízené změny a GAP analýzu, přičemž celá kapitola je uvozena základními pojmy dotýkajícími se téže celé řešené problematiky.

Protože není v možnostech této práce pokrýt všechna témata detailně, čtenář může využít použité literatury k bližšímu seznámení s řešenými tématy.

1.1 Základní pojmy

Prostřednictvím následujících základních pojmů bude méně zkušený čtenář uvozen do řešené problematiky pro snazší seznámení s dalším textem.

1.1.1 Informace

Informace se proplétají napříč celým světem, který jimi začíná být přesycený. Přitom tomu není dávno, kdy Claude Shannon představil své chápání informace a byla definována jednotka měření informace – bit (1).

Informace lze interpretovat jako údaje popisující reálné prostředí včetně jeho procesů a stavů (2).

Setkáme-li se s pojmem **neveřejné informace**, můžeme jej chápat jako popis takových informací, jejichž vyzrazení by mohlo ohrozit organizaci (3).

1.1.2 Data

Kódovaná data vytváří informaci. Mají formální podobu, a proto se hodí ke zpracování, jehož výsledkem jsou data sekundární. Data jsou uložena na různých nosičích a zařízeních (2, 3).

1.1.3 Osobní údaj, subjekt údajů

Osobním údajem jsou: *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě“* (4, čl. 4, odst. 1).

Výše zmíněnou fyzickou osobou se myslí **subjekt údajů**, který je možné přímo či nepřímo identifikovat. Může se tak stát identifikátorem (např. jméno) či zvláštním prvkem subjektu údajů (např. fyzický) (4).

Zvláštní kategorií osobních údajů jsou tzv. **citlivé osobní údaje**, jejichž zpracování je až na definované výjimky (které může daný stát zpřesnit) zakázáno. Takovými údaji může být sexualita, rasový původ (4).

1.1.4 Informační bezpečnost

Nebo též bezpečnost informací je součástí bezpečnosti organizace spolu s bezpečností IS/ICT. Hlavním cílem informační bezpečnosti je ochrana informací – udržení jejich dostupnosti, důvěrnosti a integrity (2).

1.1.5 ISMS

Systém řízení informační bezpečnosti využívá čtyř kroků modelu PDCA k řízení informační bezpečnost, v rámci kterých dojde k jeho ustanovení, zavedení a provozu, monitorování a přezkoumání a nakonec k údržbě a zlepšování (2).

1.1.6 PDCA

Tento model spojovaný s Demingem prezentuje životní cyklus systému řízení (či komponenty) zasazený do fází plan, do, check and act (přeloženo jako plánuj, dělej, kontroluj a zlepšuj). Díky tomu je poskytnuta i zpětná vazba (3).

1.1.7 Nařízení

Nařízení vydaná v rámci Evropské unie jsou závazná pro všechny členské státy bez ohledu na jejich vlastí legislativu. Jejich smyslem je sjednocení práva v zemích (5).

1.2 GDPR

Kapitola předkládá obecný teoretický přehled nejdůležitějších oblastí vztahujících se k hlavní tématice této práce.

Známá zkratka „GDPR“ je užívána pro Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Toto nařízení vstoupilo v platnost zmiňovaného 27. dubna 2016, kdy bylo uveřejněno v Úředním věstníku Evropské unie (6).

GDPR bude účinné od 25. května 2018. Což znamená že k tomuto datu musí být ošetření jeho splnění nebo hrozí sankce a pokuty, a to nejen subjektům v Evropské unii, ale všem, jež chtějí zpracovávat osobní údaje občanů EU (6).

1.2.1 Od 95/46/ES k GDPR aneb stručné uvedení do problematiky

Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů začala platit již 13. prosince 1995. Členské státy Evropské unie musely tuto směrnici zanést do své vnitřní legislativy nejpozději k 24. říjnu 1998. Téměř po 11 letech vyšla „Budoucnost soukromí“ – dokument upozorňující na potřeby zlepšení a modernizaci současného právního rámce, což postupně vyústilo k diskuzím o celkové reformě tehdejších pravidel ochrany osobních údajů (6).

Jako drobný odkaz vnímání novodobých potřeb 21. století slouží jedno z rozhodnutí Evropského soudního dvoru týkající se osobních údajů a internetu. Pokud jsou na webové stránce osoby identifikovány například jménem, tak se jedná o automatizované zpracování osobních údajů (částečné či úplné) (7).

Významné podpory pro realizaci se GDPR dostalo v březnu 2014 při hlasování Evropského parlamentu, kdy pro bylo 621 hlasů, proti pouze 10 hlasů (zdrželo se 22 hlasujících). A tak si nařízení zajistilo takřka nezrušitelnou realizaci a Evropská unie dala vzniknout nejkomplexnějšímu zákonnému prostředku pro ochranu soukromí fyzických osob (6).

Z názvu samotného Obecného nařízení vyplývá zrušení 95/46/ES, které neodpovídá současným požadavkům a trendům moderního světa. Až Obecné nařízení vstoupí v účinnost bude v rámci svého rozsahu nahrazovat i český **zákon č. 101/2000 Sb.**, o ochraně osobních údajů a o změně některých zákonů. Ten se dočká novelizace, která například upraví pravidla týkající se **Úřadu pro ochranu osobních údajů** (6).

Po vstoupení GDPR v účinnost se totiž ÚOOÚ kupříkladu stane ohlašovacím místem pro hlášení porušení zabezpečení osobních údajů (6).

1.2.2 Přínosy GDPR

Současně (resp. před účinnosti GDPR) se podniky v Evropské unii musí přizpůsobit 28 různým zákonům vztahujícím se k ochraně dat, což je vysoce nákladné z pohledu administrace, především pro malé a střední podniky, kterým taková fragmentace vstup na nové trhy stěžuje nejvíce (8).

Evropská komise v květnu 2015 vydala Digitální strategii jednotného evropského trhu, která navrhovala vytvoření jednotného trhu digitálního zboží a služeb napříč EU. Strategie zdůrazňuje nejen snazší přístup na online trhy, ale také posílení digitálních sítí. Na nutnost zajištění vysoké ochrany dat jedinců upozorňovala komise ve svém návrhu již v roce 2012 (8).

Důraz na malé a střední podniky je kladen především z toho důvodu, že v EU tvoří 99 % veškerého obchodu. Zavedením nových pravidel prostřednictvím GDPR se očekávají roční přínosy ve výši 2,3 bilionů EUR (na evropské úrovni) (8).

1.2.3 Z nejdůležitějších pojmů k GDPR

Jestliže hovoříme o **zpracování** osobních údajů (či souboru osobních údajů), myslí se tím jakákoliv automatizovaná i neautomatizovaná operace, kterou je například uložení, zaznamenání, pozměnění, ale i vyhledávání, šíření, výmaz či zničení (4).

Zpracování osobních údajů může mít právní důvod (právní povinnost, splnění smlouvy, …) (6).

Jako **správce** může vystupovat nejen právnická, ale i fyzická osoba či jiný subjekt. Správce má za povinnost definovat účel a prostředky zpracování OÚ. Jestliže si tyto

činnosti rozdělí více subjektů, poté se jedná o **společné správce**. **Zpracovatel** pro správce pouze osobní údaje zpracovává. Pokud chce zapojit dalšího zpracovatele, musí k tomu získat písemný souhlas správce (4, 6).

Vztah správce a zpracovatele je třeba smluvně ošetřit (zvláštní **zpracovatelskou smlouvou** anebo připojením dodatku k jiné smlouvě) takovým způsobem, aby byly splněny požadavky definované v obecném nařízení (6).

Souhlas nese znaky svobodné, konkrétní, informované a jednoznačné vůle. Subjekt údajů jeho uložením svoluje zpracovávat své OÚ, má však také možnost svůj souhlas odvolat (4, 6).

Souhlasy udělené před GDPR mohou platit i po vstoupení účinnosti za podmínky, že plní podmínky nařízení (6).

1.2.4 Princip odpovědnosti a přístup založený na riziku

Principem odpovědnosti správce se myslí správcova odpovědnost za dodržování zásad zpracování a za schopnost toto dodržování prokázat. K **doložení souladu** mají napomoci záznamy o činnostech zpracování, ale také kodexy a osvědčení od akreditovaných subjektů. Přičemž existují výjimky, kdy společnost záznamy o činnostech zpracování vést nemusí (6).

Přístup založený na riziku nabádá správce k tomu, aby bral v úvahu zpracovávané osobní údaje, a to především z pohledu jejich povahy, rozsahu a pravděpodobných rizik. Na což by měl po vyhodnocení zareagovat adekvátním zabezpečením osobních údajů (6).

Jestliže zabezpečení osobních údajů selže, musí o tom informovat do 72 hodin ÚOOÚ (kdyby k úniku došlu u zpracovatele, ten jej hlásí správci). Pokud porušení může způsobit vysoké riziko daným subjektům údajů, je povinností správce informovat i je (6).

1.2.5 O sankcích a pokutách

Velkým motivátorem pro dodržování GDPR jsou definované sankce a pokuty. Je však nutné si uvědomit, že ne každý nesoulad jimi bude trestán. Správce může být prvně upozorněn a bude mu zajištěn prostor pro uvedení problému do pořádku. Velmi bude záležet na konkrétním případu (6).

Finanční pokuty jsou dle závažnosti rozdělené do dvou úrovní, a to na:

- až 10 000 000 EUR (či až 2 % celkového ročního celosvětového obratu, pokud se jedná o podnik),
- až 20 000 000 EUR (či až 4 % celkového ročního celosvětového obratu, pokud se jedná o podnik) (6).

V rámci případného správního řízení budou brány v úvahu i další polehčující či přitěžující okolnosti (6).

1.2.6 Zásady GDPR

Nařízení definuje zásady, kterých musí být u osobních údajů dodrženo, jedná se o:

- transparentnost, korektnost, zákonnost,
- účelové omezení,
- minimalizaci údajů,
- přesnost,
- omezení uložení,
- integritu a důvěrnost (4).

Z minimalizace údajů vyplývá, že správce musí uchovávat pouze ty nezbytné osobní údaje, které jsou nutné – nic nad rámec. Omezení se také týká doby zpracování (viz omezení uložení), kterou je třeba jasně definovat, a to opět na co nejrelevantnější nutnou dobu (6).

Pro skrytí identity subjektu údajů je možné využít pseudonymizaci, která může být aplikována takovým způsobem, kdy jednotlivec je označen jedinečným ID, jenž je dále používán pro spojení s dalšími informacemi daného jedince. Oddělením přiřazení klíče je zajištěno skrytí totožnosti (9).

1.2.7 Práva subjektu údajů

Obecné nařízení téže rozebírá jednotlivá práva subjektu údajů ve vymezených oddílech:

- transparentnost a postupy,

- informace a přístup k OÚ,
- oprava a výmaz (4).

Konkrétně se jedná o práva:

- být informován,
- přístupu,
- na opravu,
- výmazu,
- zamezit zpracování,
- přenositelnosti dat,
- na stížnost,
- související s automatizovaným rozhodováním a profilováním (6).

1.2.8 DPIA a povinnost jeho vypracování

Posouzení vlivu na ochranu osobních údajů je vyžadováno při zpracování osobních údajů s pravděpodobným vysokým rizikem pro subjekt údajů. Při jeho realizaci se využije posudek DPO (4).

Přestože nařízení popisuje konkrétní případy, kdy je DPIA nutné, jedná se o neúplný seznam, proto je třeba počítat s tím, že existují i další operace s vysokým rizikem v nařízení nezmíněném (6).

Výjimky, kdy posouzení vlivu nebude nutné (nebo naopak nutné bude), může určit i dozorový úřad a stejně tak stát v rámci různých zpřesňujících instrukcích. Pakliže posouzení musí být vypracováno, musí obsahovat minimálně:

- popis a účely zpracování, popř. oprávněné zájmy správce,
- zohlednění přiměřenosti a nezbytnosti těchto zpracování,
- vyhodnocení rizik z pohledu subjektů údajů a jejich práv a svobod,
- opatření pro snížení těchto rizik atd. (4).

1.2.9 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů může pracovat pro více správců, resp. zpracovatelů, jestliže to nesníží hodnotu jeho odváděné práce. Jeho jmenování je určitě nezbytné, pokud hovoříme o veřejné správě (vyjma soudů), rozsáhlém monitorování subjektů údajů anebo rozsáhlém zpracování zvláštních kategorií údajů. Při výběru DPO je nutné zohlednit jeho profesní zkušenosti a znalosti z oblasti ochrany osobních údajů (4).

Jestliže je DPO jmenován, měl by se co nejdříve zapojit do všech operací spojených se zpracováním osobních údajů, dále by se mělo zajistit jeho postavení v rámci společnosti, v jejíž hierarchii by měl být podřízen přímo vrcholovému managementu a měl by mít dostatečné pravomoci a zdroje k výkonu své práce. Naopak ale také musí zachovat mlčenlivost (4).

Pro subjekty údajů působí pověřenec pro ochranu osobních údajů jako hlavní kontakt pro vyřizování záležitostí spojených se zpracováním jejich osobních údajů. Přinejmenším by měl informovat, radit při zpracování zaměstnancům, kontrolovat a zajišťovat soulad s GDPR, zvyšovat o něm povědomí, spolupracovat s dozorovým úřadem apod. (4).

1.2.10 Ochrana OÚ zaměstnanců ve světle GDPR

V případě pracovního vztahu je zaměstnavatel většinou oprávněn ke zpracování osobních údajů zaměstnance kvůli povinnostem plnění smlouvy a zákonných povinností (10).

Souhlas jako právní důvod je většinou v tomto vztahu nevhodný, spíše až nežádoucí. Pokud však chce zaměstnavatel zpracovávat fotografie/videa zaměstnance či zaměstnanci dávat přání k výročí, zde je souhlas naopak vhodný (10, 11).

Zpracování osobních údajů v rámci zaměstnaneckého vztahu lze rozdělit na zpracování během přijímacího řízení, zpracování v průběhu zaměstnání a zpracování po ukončení pracovního poměru (10).

Především v prvních dvou fázích si musí dát zaměstnavatel pozor při využívání sociálních sítí. Například využívat získané informace ze sociální sítě k výběrovému řízení nebo dokonce vyžadovat k těmto profilům přístup (10).

Jak při výběrovém řízení, tak při samotném průběhu zaměstnání musí zaměstnavatel dodržovat zásadu uchovávání pouze těch nejnutnějších osobních údajů (10).

S ohledem na konkrétní užívané technologie a zařízení je nutné nastavit adekvátní zpracování osobních údajů při monitorování informačních a komunikačních technologií, a to nejen na pracovišti, ale i mimo něj. Důležité je zavést takovou politiku, která zohlední rozsah zpracování, tj. bude prosazovat takováto zpracování pouze proporcionálně a bude pro uživatele přívětivá a plně pochopitelná (10).

Speciální přístup si vyžádá práce na dálku a BYOD, obojí totiž zvyšuje pravděpodobnost rizika, nebudou-li nastavena adekvátní bezpečnostní opatření a politiky nad rámec standardních opatření vyžadovaných na pracovišti či u zařízení sloužících čistě pro pracovní účely. I zde platí, že zaměstnanci musí být plně informováni o veškerém monitoringu a zpracování, a pokud se objeví případ vyžadující souhlas ke zpracování či sledování, musí si jej zaměstnavatel pro další činnost od zaměstnance vyžádat (10).

Závěrem lze konstatovat, že nedostatkem GDPR je neexistující specifická úprava týkající se zaměstnavatele a autoři nařízení předpokládají toto upřesnění ze strany státu (11).

1.2.11 Náhled na budoucí vývoj ochrany OÚ

V České republice se **adaptační zákon** pro zpřesnění GDPR nestihne před 25. květnem 2018 vydat, přestože se na něm pracuje od roku 2016. Na druhou stranu se předvídá, že pouze třetina státu bude mít k tomuto datu nastavenou adaptační legislativu. Každopádně se nečeká, že adaptační zákon přinese příliš velké úpravy oproti Obecnému nařízení. Nejvíce změn se například dotkne obcí, na které má z nařízení mířit deset paragrafů. S tím souvisí přesné vydefinování veřejného subjektu (12).

Původně s GDPR mělo vejít v účinnost i nařízení o respektování soukromého života a ochrany osobních údajů v elektronických komunikací označované jako **ePrivacy**. Přestože jeho účinnost byla odložena, jedná se o další krok pro zajištění větší ochrany soukromí, na který by mělo být bráno zřetel již nyní. ePrivacy bude směřovat jak na fyzické, tak na právnické osoby a bude řešit mimo tradiční telekomunikační operátory i OTT služby a metadata elektronické komunikace. Další oblastí ePrivacy budou cookies (13).

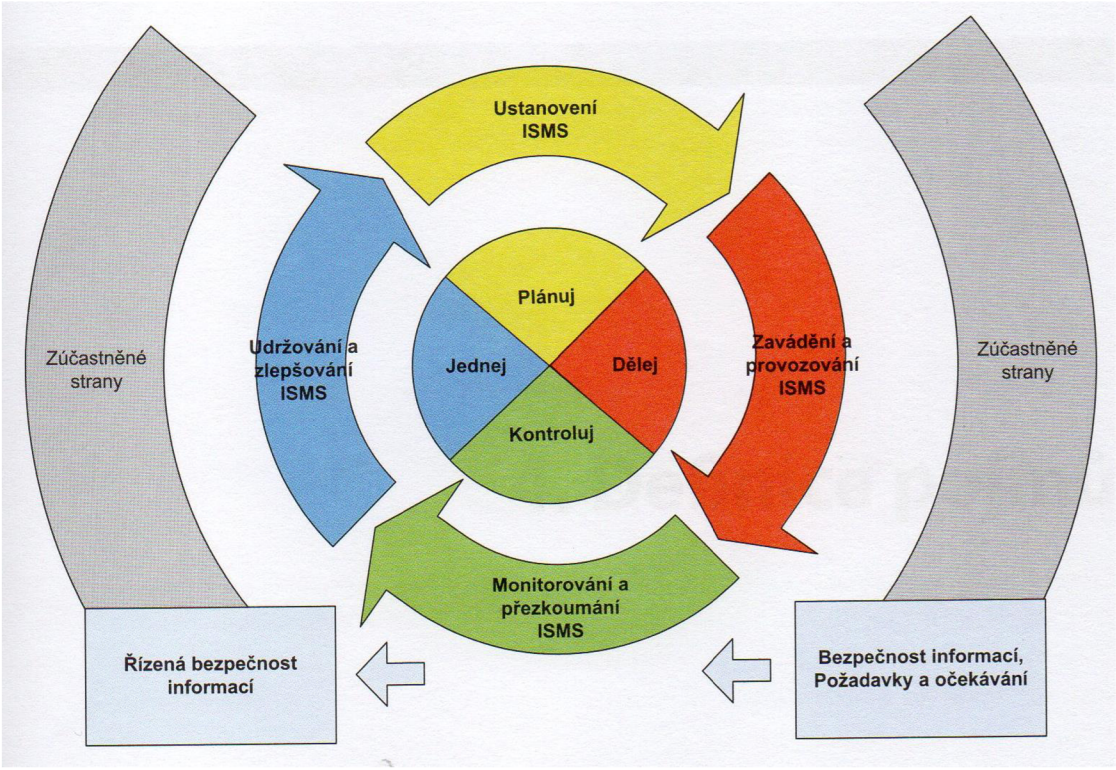
OTT služby využívají pro přenos obsahu prostředí Internetu, tudíž zákazník nemusí mít konkrétního poskytovatele, ani nepotřebuje specifické zařízení, aby mohl využívat těchto služeb. Příkladem OTT jsou WhatsApp, Messenger či Skype (13, 14).

1.3 ISMS

Systém řízení bezpečnosti informací je systém zajišťující řízení a správu informačních aktiv, a to takovým způsobem, aby bylo eliminováno jejich poškození či ztráta (2).

Životní cyklus systému řízení bezpečnosti informací lze rozdělit do čtyř hlavních fází:

- ustanovení ISMS,
- zavádění a provoz ISMS,
- monitorování, přezkoumání ISMS,
- údržba a zlepšování ISMS (3).



Obrázek č. 1: Životní cyklus ISMS

(Zdroj: 2, s. 25)

1.3.1 Ustanovení ISMS

Kvalita systému řízení bezpečnosti informací je definována již od samotného počátku, kdy dochází k jeho ustanovení (3).

Ustanovení ISMS sestává především z definice jeho rozsahu hranic, vazeb a Prohlášení o politice ISMS, které musí být navíc odsouhlaseno. Následuje řízení rizik, ze kterého jsou zbytková rizika odsouhlasena vedením společnosti. Vrcholový management musí souhlasit a podpořit i samotné zavedení ISMS. Poté může dojít k zahájení příprav Prohlášení o aplikovatelnosti (3).

Prohlášení o politice ISMS je řazeno mezi významné dokumenty. Jsou v ní mimo jiné zaneseny požadavky společnosti a určeny cíle a směr ISMS (3).

Řízení rizik je rámec objímající několik dalších činností. V prvé řadě se jedná o analýzu rizik a jejich vyhodnocení, v druhé řadě o zvládání rizik a v neposlední řadě o jejich akceptaci (3).

Prohlášení o aplikovatelnosti shrnuje vybraná bezpečnostní opatření pro minimalizaci (odstranění) zjištěných bezpečnostních rizik. Jestliže společnost usiluje o shodu s normou ISO/IEC 27001, stává se pro ni Prohlášení povinným (3).

1.3.2 Zavádění a provoz ISMS

V této fázi je kladen výrazný důraz na bezpečnostní opatření. Především z pohledu jejich zavedení. To souvisí i s jejich řádným popisem, k němuž je využita Příručka bezpečnosti informací (3).

Mimo sestavení Příručky jsou důležité i tyto činnosti:

- formulace Plánu zvládání rizik,
- zavedení bezpečnostních opatření,
- (pravidelné) školení v oblasti bezpečnosti,
- řízení bezpečnostních incidentů,
- řízení dokumentace o ISMS (3).

Příručka bezpečnosti informací označuje bezpečnostní politiky, směrnice apod. Taková dokumentace podporuje dodržování bezpečnostních opatření prostřednictvím stanovených odpovědností a pravidel (3).

Bezpečnostní dokumentace může být diferencována na tři úrovně. Dokumenty související s ISMS se nachází na té nejvyšší úrovni (například prohlášení o aplikovatelnosti, plán zvládání rizik). O úroveň níže jsou definovány dokumenty na podporu prosazení ISMS. Pracovní postupy se nachází na nejnižší úrovni (3).

Systematický přístup nekončícího charakteru si vyžaduje **budování bezpečnostního povědomí**, které je nezbytné pro minimalizaci chybovosti lidského faktoru (3).

1.3.3 Monitorování a přezkoumání ISMS

Ačkoli správný výběr bezpečnostních opatření a jejich implementace jsou velmi důležitými kroky, nejedná se o kroky poslední. Prostřednictvím monitorování je třeba

zajistit zpětnou vazbu podávající výstup o správnosti zavedení a funkčnosti jednotlivých bezpečnostních opatření. V případě nutnosti zajistit nápravu zjištěných nedostatků (3).

Proto by v rámci monitoringu a přezkoumávání ISMS mělo dojít k následujícím činnostem:

- monitorování bezpečnostních opatření a vyhodnocení jejich účinnosti,
- realizace interních auditů ISMS,
- závěrečné vytvoření zprávy o zjištěném stavu ISMS a jeho přehodnocení (3).

Audit zajišťuje proces, systematicky a nezávisle vedený, který je navíc dokumentován. Aby byla zajištěna jeho kvalita, tak by auditor měl mít dostatečné odborné znalosti (3).

Jedním z opěrných složek auditu jsou normy ISO/IEC 27001 a 27002 (3).

Výstupy monitorování ISMS jsou shrnuty a předloženy ve **zprávě o ISMS** sloužící k jeho přezkoumání vedením organizace. Její součástí je taktéž SWOT analýza porovnávající silné a slabé stránky systému řízení bezpečnosti informací (3).

1.3.4 Údržba a zlepšování ISMS

Nakonec je třeba ISMS udržovat alespoň v požadovaném stavu a nejlépe pracovat na jeho kontinuálním vylepšování. Jestliže je zjištěn nesoulad s požadavky, hovoříme o **neshodě**. Tu lze odstranit pomocí **nápravy**, kterou se myslí konkrétní opatření pro odstranění zjištěné neshody. V terminologii existuje i tzv. **opatření k nápravě**, jež míří přímo na příčiny dané neshody. Ovšem pragmatický přístup zajišťují obzvláště **preventivní opatření**, která se snaží odstranit potenciální neshody (3).

Ačkoli vytvoření dokonalého systému řízení bezpečnosti informací není takřka možné, je důležité pracovat na jeho neustálém zlepšování a pokusit se tohoto těžko dosažitelného stavu dosáhnout (3).

Pokud se společnost tak rozhodne, může provést certifikaci sestávající ze dvou etap – certifikace dokumentace a kontroly implementace ISMS (2).

1.4 Analýza rizik

Aby mohlo dojít ke snížení rizik, je v prvé řadě nutné je zanalyzovat, k čemuž právě slouží analýza rizika (15).

Analýza rizik může být rozdělena do následujících procesů:

- identifikace a hodnocení aktiv,
- identifikace hrozeb a jejich pravděpodobností,
- vytvoření matice zranitelnosti,
- vytvoření matice rizik (2).

Rizikem lze chápat pravděpodobnost nebezpečí, že dojde k hrozbě a vznikne škoda či jej můžeme definovat jako míru ohrožení aktiva. Riziko vzniká kvůli vzájemnému působení hrozby a rizika (15).

1.4.1 Identifikace a hodnocení aktiv

Při identifikaci aktiv je třeba definovat veškerá aktiva v rámci rozsahu řešené analýzy. Aktivem je vše, co má pro společnost hodnotu, nemusí se tedy jednat pouze o software anebo hardware (2).

Hodnocení aktiv by mělo nejlépe proběhnout jejich vlastníky, popřípadě uživateli. Toto ohodnocení nemusí být striktně prováděno pomocí finančních částek, ale může být využito jiných pohledů – například hodnocení aktiv dle dopadu rizika na společnost (2).

Součtový algoritmus patří mezi nejpoužívanější způsoby výpočtu hodnoty aktiva. Vychází z nákladů vzniklých při narušení dostupnosti (x), důvěrnosti (y) a integrity (z). Podoba součtového algoritmu je: **(x + y + z) / 3** (2).

Dle vytvořeného kvalitativního hodnocení aktiva je poté podle zjištěné váhy aktiva určena míra rizika a jeho dopad. Například dosáhne-li aktivum váhy jedna, jedná se o bezvýznamné riziko mající žádný dopad na organizaci (2).

1.4.2 Identifikace hrozeb a jejich pravděpodobností

Pokud se mluví o hrozbě, myslí se možnost, že dojde k poškození aktiva. Hrozby mohou být zapříčiněny přírodními či lidskými silami, které mohu být náhodné nebo úmyslné (2).

Pravděpodobnost hrozby určuje pravděpodobnost, že k hrozbě dojde. Stanoví se tabulka hodnocení hrozby se slovním popisem pravděpodobnosti hrozby a její číselnou hodnotou – nejčastěji (jako u hodnocení aktiv) se využívá škály od 1 do 5, kde 5 značí největší pravděpodobnost uskutečnění hrozby (2).

Na hrozby lze nahlížet mnoha způsoby. Jedním takovým způsobem je rozdělení hrozeb dle oblastí, ve kterých mohou působit:

- síťové a technické zdroje,
- procesy/procedury spojené se zpracováním osobních dat,
- osoby/strany zapojené do zpracování osobních dat,
- sektor businessu a rozsah zpracování (8).

1.4.3 Vytvoření matice zranitelnosti

Využitím předchozích dvou kroků, ze kterých byly získány výstupy s hodnocením aktiv a pravděpodobnostmi hrozeb, je sestavena matice zranitelnosti. Matice zranitelnosti je na základě posouzení doplněna o hodnoty jednotlivých zranitelností aktiv (2).

1.4.4 Vytvoření matice rizik

Nakonec se do matice rizik dopočtou jednotlivé míry rizik, a to jako násobky pravděpodobnosti vzniku hrozby (T), hodnoty aktiva (A) a zranitelnosti aktiva (V). Tedy dle vzorce **R = T*A*V**, kde R značí míru rizika (2).

Aby se určila závažnost rizik, definuje se hodnotící škála míry rizika, která dle stanovených hranic určí, zda se jedná například o bezvýznamné, mírné či nepřijatelné riziko (2).

1.5 Normy řady ISO/IEC 27000

Řada ISO/IEC 27000 se zaměřuje na řízení bezpečnosti informací a vychází z PDCA. Mezi nejvýznamnější normy patří ISO/IEC 27000 (uvádějící přehled a slovník k ISMS), ISO/IEC 27001 (řešící požadavky ISMS), ISO/IEC 27002 (s postupy pro řízení bezpečnosti informací) či ISO/IEC 27005 (o řízení rizik bezpečnosti informací) (3).

1.5.1 ISO/IEC 27000

Název: **Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník** (16).

Mimo seznámení s přehledem norem ISMS podává norma ISO/IEC 27000 úvod do definic a termínů v nich užívaných. Také seznamuje se systémy řízení bezpečnosti informací (16).

1.5.2 ISO/IEC 27001

Název: **Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky** (17).

Tato norma řeší požadavky týkající se definování, zavedení, údržby a zlepšování ISMS, který musí zachovávat zásady dostupnosti, integrity a důvěrnosti informací (17).

Pořadí požadavků v normě neznačí jejich pořadí pro implementaci ani jejich důležitost. Požadavky jsou navíc obecné a lze je využít ve všech společnostech (17).

Příloha A normy ISO/IEC 27001 předkládá jednotlivá opatření a jejich cíle (17).

1.5.3 ISO/IEC 27002

Název: **Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací** (18).

Norma ISO/IEC 27002 je vhodná pro organizace, jež mají vybraná opatření definované v ISO/IEC 27001 a plánují implementovat opatření bezpečnosti informací včetně vytvoření směrnic o informační bezpečnosti (18).

Jejím obsahem jsou kapitoly zaměřující se na jednotlivé kategorie bezpečnostních opatření. Mimo informace o opatřeních jsou poskytnuty i pokyny pro jejich zavedení (18).

1.5.4 ISO/IEC 27005

Název: **Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací** (19).

Předmětem normy jsou doporučení k řízení rizik bezpečnosti informací, nenabízí konkrétní metodiky, jejichž výběr závisí již na konkrétní společnosti (19).

I tato norma se odkazuje na normu ISO/IEC 27001, přičemž je vhodné znát k jejímu úplnému pochopení i ISO/IEC 27002 (19).

Informativní Příloha C udává seznam příkladů typických hrozeb, kterých je možno užít při jejich posuzování (19).

1.5.5 Vztah GDPR a norem řady ISO/IEC 27000

Implementací norem řady ISO/IEC 27000 může být dosaženo souladu s GDPR, jestliže bude správně pracováno s osobními údaji, respektive bude na ně brán zřetel. Především při zavedení normy ISO/IEC 27001 dochází k přijetí opatření, vytvoření dokumentace, monitoringu a neustálému zlepšování bezpečnostní situace ve společnosti, což vše vyžaduje i GDPR. Norma ISO/IEC 27001 sice nepokrývá vše nutné pro soulad s nařízením, ale výrazně jej podporuje (6).

„Implementace ISMS v souladu s normou ISO 27001 může být chápana jako jistý krok vedoucí k dosažení souladu s GDPR“ (6, s.197).

Ovšem je třeba brát v úvahu, že i při implementaci systému řízení bezpečnosti informací budou existovat oblasti, které bude třeba kvůli Obecnému nařízení vyřešit (6).

Normy ISO/IEC 27001 využívá v souvislosti s opatřeními a GDPR i ENISA – viz Guidelines for SMEs on the security of personal data processing (20).

1.6 Rozbor „7 S faktorů“

Rozbor „7 S faktorů“ řeší sedm hlavních faktorů, které zajišťují úspěch, ale také neúspěch společnosti. Pro zajištění celkového úspěchu společnosti musí být všechny faktory řešeny a měly by být vyváženy (15).

Do sedmi faktorů patří:

- strategie společnosti,
- její struktura,
- spolupracovníci,
- jejich schopnosti,
- styl řízení společnosti,
- systémy ve společnosti,
- sdílené hodnoty.

1.6.1 Strategie společnosti

Strategií se myslí dlouhodobé směřování k cílům či k jednomu cíli. To bývá podmíněno činnostmi, procesy, které musí být realizovány, aby došlo k naplnění cílů. V podnikatelském prostředí je většinou snaha o získání konkurenční výhody při zajištění spokojenosti zákazníků a stakeholderů (15).

Strategie lze dále členit na firemní, obchodní a funkční strategii (15).

1.6.2 Organizační struktura firmy

Dle rozdělení pravomocí a úkolů se časem vyvinuly následující organizační struktury: liniová, funkcionální, liniově štábní, divizionální a maticová (psáno od nejjednodušší po nejsložitější) (15).

Liniová struktura má jasně definovaný vztah nadřízenosti a podřízenosti, což umožňuje rychlé rozhodování. Na druhou stranu však musí mít vedoucí znalosti ze všech oblastí činnosti firmy (15).

1.6.3 Informační systémy

Tento faktor řeší formální i neformální informační procedury, které ve společnosti probíhají. I v dnešní době se stále setkáváme s manuálním zpracováváním informací, nikoli již jen s automatizovaným za podpory počítačů (15).

1.6.4 Styl řízení

Podle zapojení zaměstnanců do řízení společnosti dělíme styly řízení na autoritativní, demokratický a laissez-faire. V autoritativním řízení provádí rozhodování pouze vedoucí sbírající informace k rozhodování od zaměstnanců. Demokratický styl řízení umožňuje již zapojení zaměstnanců do rozhodování. A nakonec laissez-faire dává zaměstnancům úplnou volnost (15).

1.6.5 Spolupracovníci

Faktor spolupracovníků se zaměřuje na lidské zdroje, které jsou důležité pro produktivitu firmy. Zdůrazňuje významnost řízení lidských zdrojů včetně motivace zaměstnanců (15).

1.6.6 Sdílené hodnoty

Sdílené hodnoty jsou chápány jako kultura společnosti. Ta udává především hodnoty a přístupy společnosti z dlouhodobého hlediska (15).

1.6.7 Schopnosti

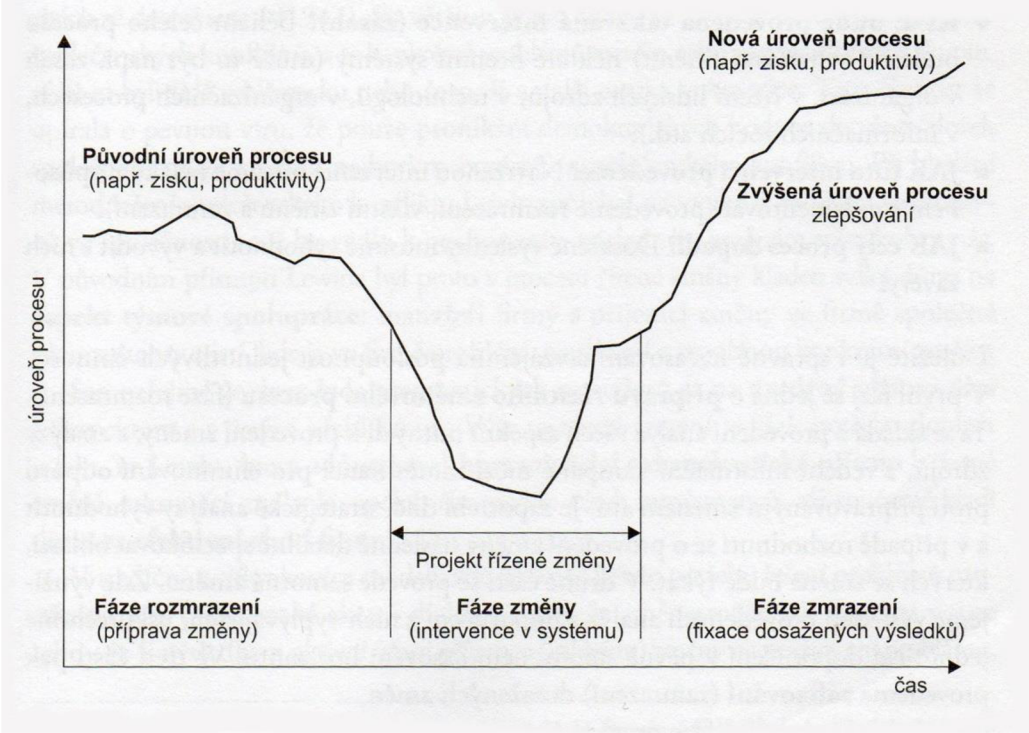
Faktor schopností vyzdvihuje důležitost rychlé adaptace manažerů, přestože je třeba klást důraz i na jiné kvalifikace, a to nejen u manažerů, ale také ostatních pracovníků (technické, výrobní schopnosti) (15).

1.7 Lewinův model řízené změny

Lewinův model řízené změny umožňuje řídit změnu pomocí jejího rozložení na více částí a činností, kterými mohou být:

- definování sil inicializujících proces změny,
- určení nositele (agenta) a sponzora změny,
- stanovení intervenční strategie,
- provedení samotné realizace za určených operačních metod,
- zhodnocení (21).

Proces řízení změny lze taktéž rozdělit na tři fáze: rozmrazení, změnu a zamrazení. Ve fázi rozmrazení dochází především k přípravám změnového procesu. Změna značí samotné provedení změny, a nakonec zamrazení zajišťuje zakotvení proběhlé změny ve společnosti a její udržování (21).



Obrázek č. 2: Fáze procesu změny

(Zdroj: 21, s. 51)

Pro řízení změny je třeba identifikovat síly působící pro a proti změně. Především je třeba se pokusit zeslabit negativní změny, nejlépe je úplně odstranit (21).

1.8 GAP analýza

Též srovnávací či rozdílová analýza určuje a srovnává současný a plánovaný stav dle stanového cíle, jehož dosažení zajišťuje naplnění stanovených ukazatelů (22).

GAP (v překladu mezeru) značí právě prostor mezi současným a požadovaným stavem, který je třeba překonat. Nalezne využití ve spojitosti se strategickými cíli společnostmi, ale také jejími aktivitami nebo při zkoumání trhu či výpočet úrokového rizika (22).

1.8.1 GAP analýza při implementaci GDPR

Požadovaný stav při implementaci GDPR určují samotné požadavky definované v nařízení. Po zjištění současné situace, definování nedostatků, lze jejich odstraněním přejít do plánovaného stavu (6).

Mezi nejdůležitější kroky GAP analýzy upravené pro GDPR patří:

- zajištění angažovanosti vedení,
- definování uzlů zpracování osobních údajů,
- identifikace zpracování OÚ,
- popis datových toků (nejlépe za pomocí programu, např. Visio),
- bezpečnosti dat,
- vytvoření souhrnné zprávy o nálezech a doporučeních (6).

Pro popis datových toků lze využít **diagram toku dat**, anglicky Data Flow Diagram (DFD). DFD diagramy patří do metod funkčního modelování. Zobrazují především datové vstupy a výstupy, činnosti a jejich činitele (23).

DFD diagramy mohou mít různou úroveň – nultou (sloužící pro kontext), první, druhou atd. Z nejpoužívanějších notací symbolů je notace Yourdon and Coad, Gane and Sarson a SSDAM (23).

2 ANALÝZA SOUČASNÉHO STAVU

Předmětem této kapitoly je analýza řešeného problému a současné situace vybrané společnosti za asistovaného zhodnocení ze strany jejího vedení, s tím, že snahou bylo pokrýt co největší oblast, a to co nejpřesněji, navzdory obchodnímu tajemství a anonymizaci této práce.

V úvodní části je proveden rozbor „7 S faktorů“, následuje stěžejní GAP analýza, na kterou navazuje neméně důležité DPIA využívající jejich výstupů. Součástí analýz jsou doporučení do návrhové části, a to takové, aby byl zajištěn soulad s GDPR. Celá analytická kapitola je uzavřena závěrečným zhodnocením.

2.1 Obecné představení společnosti

Hlavním předmětem podnikání řešené společnosti je tvorba a správa webových stránek a internetových obchodů (v obchodním rejstříku zapsáno jako „Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona“). Z pohledu právní formy se jedná o společnost s ručením omezeným. Délka trvání její působnosti je relativně krátká, jelikož na zmíněném trhu působí pouze přes dva roky, a to od 1. 10. 2015, kdy se současný majitel po několikaletém podnikání jako osoba samostatně výdělečně činná rozhodl rozšířit své podnikání a založit si vlastní společnost. Sídelním městem společnosti je Ostrava.

Vzhledem k tématu, kterým se zabývá tato diplomová práce, zaměřenému na ochranu osobních dat, a které se dotýká neveřejných informací společnosti, si vybraná společnost nepřeje, aby byla jakkoliv identifikována, ať už přímě či nepřímě, a proto takové údaje, jež by tak mohly činit a řešenou společnost odhalit, jsou v práci záměrně vynechány, popřípadě po konzultacích upraveny, avšak takovým způsobem, aby nebyla zkreslena podstata řešená v rámci této práce. Pro účely dalšího textu bude společnost nadále označována jako společnost XYZ.

2.2 Rozbor „7 S faktorů“

Pro další popis společnosti XYZ je využit rámec „7 S faktorů“ firmy Mc Kinsey, který rozebírá a nahlíží na sedm faktorů (ne)úspěchů firmy (struktura, strategie, systémy, sdílené hodnoty, schopnosti, spolupracovníci a styl).

2.2.1 Strategie firmy

Z dlouhodobého hlediska firma zcela logicky usiluje o neustálé navyšování kvality nabízených služeb. Od konkurence se chce diferencovat vytvářením vlastních produktů, namísto užívání open source řešení či řešení třetích stran. Konkrétně lze zmínit například vytvoření vlastního CMS či e-shopu. Cílem je nabízet kvalitní produkty mající vysokou úroveň adaptace zákazníkovi a efektivní podporu, a to takovým způsobem, aby se společnost zařadila mezi špičkové odborníky ve svém oboru. Pro dosažení a udržení takového stavu jsou vytyčeny podpůrné cíle, jako jsou například kvalitní zaměstnanci a jejich vysoká odborná úroveň, kterou je nadále třeba udržovat (školení apod.).

2.2.2 Organizační struktura firmy

Jelikož se jedná o společnost velmi malého rozsahu, neb má pouze tři zaměstnance na HPP, její organizační struktura je jednoduchá. Vedle tohoto čísla počtu zaměstnanců na HPP ještě společnost zaměstnává studenty na zkrácené úvazky (v průměru tři až čtyři), smluvně ošetřené dohodami o provedení práce, a také spolupracuje s OSVČ (v průměru dva až tři).

Hovoříme-li o zaměstnancích, jedná se primárně o programátory, kteří jsou dle svého zaměření (definovaného užívanými programovacími jazyky) rozdělení do dvou skupin, podle toho, zda se při tvorbě zaměřují na backend či frontend, avšak umístění zaměstnance vzhledem k jeho širším znalostem nemusí být vždy tak striktní. Obě skupiny mají své seniorní programátory, kteří zodpovídají za kontrolu kvality kódu, případně řídí koordinaci při práci na rozsáhlejších projektech. Avšak primární řízení projektů má na starosti projektový manažer spolu s majitelem společnosti XYZ, přičemž je běžné, že jeden programátor může pracovat na více projektech. Projektový manažer a majitel

zodpovídají i za personální řízení (ve firmě není žádný personalista, respektive osoba zabývající se výhradně HR, proto jsou v této oblasti využívány externí služby, a to jak v oblasti účetnictví, tak příležitostně v oblasti právní (viz pracovní smlouvy atd.). O obchodní záležitosti a získávání zakázek se též starají majitel a projektový manažer.

Vzhledem k širokému rozsahu služeb, které mohou být k webovým stránkám a internetovým obchodům nabízeny, spolupracuje společnost XYZ s externími firmami. Jedná se především o zajišťování marketingových služeb a vytváření grafických podkladů a návrhů. Sekundárně se pak může jednat o doplnění programátorských služeb, ať už kvůli nedostatečným kapacitám či specifickému požadavku zákazníka.

2.2.3 Informační systémy

Pro potřebu interního fungování používá společnost XYZ pro práci s informacemi softwarová řešení třetích stran, a to jak placená, tak volně dostupná, která mají především online charakter. Tyto informace jsou spojené se zpracovávanými projekty. Vzhledem k velikosti společnosti XYZ neexistuje žádný automatizovaný systém pro řízení dat o zaměstnancích, spolupracujících osobách či společnostech, dodavatelích anebo odběratelích. Tyto údaje jsou uchovávány a zpracovávány majitelem, projektovým manažerem, popřípadě externí mzdovou účtárnou.

Zaměstnanci využívají na svých počítačích program *Paymo*, který slouží pro monitoring odpracovaného času, přiřazuje explicitně zaměstnance k projektům a umožňuje v reálném čase odhadovat některé významné parametry, jako je odhadovaný čas k dokončení projektu či zbývající finanční prostředky u daného projektu, jestliže byl předem nastaven nějaký finanční strop. Dalším významným prostředkem pro řízení kooperace na projektech je webová aplikace *Asana*, pomocí níž jsou zaměstnancům zadávány již detailní jednotlivé úkoly k projektům. Aplikace tak umožňuje jednoduše sledovat proces postupu vyhotovení úkolů a nabízí dostatečný prostor pro diskuzi v případě potřeby ujasnění či řešení problémů. Samozřejmostí je přikládání různých příloh, nastavování termínů dokončení úkolů a podobně. A nakonec pro nejrychlejší komunikaci mezi zaměstnanci slouží webová a mobilní aplikace *Slack*. Zde existují různé komunikační kanály (general, frontend, news, intern,…) anebo lze kontaktovat některého z uživatelů přímo.

2.2.4 Styl řízení

Jelikož se zaměstnanci podílejí na rozhodnutí, můžeme styl řízení ve společnosti XYZ označit za demokratický. Zaměstnanci poskytují nadřízenému (majiteli či projektovému manažerovi) své odborné názory a postřehy, čímž podávají nadřízenému potřebné informace pro rozhodování, na kterém se i podílí, což vede ke stmelenější atmosféře. Za konečné rozhodnutí zodpovídá nadřízený, i v takové situaci, ve které podpoří myšlenku jednoho z programátorů, ačkoli důsledky za případné špatné rozhodnutí by mohl nést spíše daný programátor.

2.2.5 Spolupracovníci

I když ve společnosti XYZ neexistuje osoba zabývající se pouze lidskými zdroji, je ze strany majitele vyvíjená aktivita tento fakt vykompenzovat. Konají se pravidelné týmové meetingy, ale také one-to-one rozhovory se zaměstnanci pro jejich osobní zhodnocení a shrnutí proběhlých činností. Zmiňované týmové meetingy mívají jak školící roli, tak roli pro upevňování týmu (teambuildingy). Školení si připravují zaměstnanci sami, dle své odbornosti a svého zaměření, anebo je pozván externí specialista. Co se týče vzdělávání vůbec, tato oblast není opomíjena ani v dalších oblastech. Pravidelně jsou nakupovány různé online kurzy (zaměřené především na nové technologie a programování) a zaměstnanci si mezi sebou v rámci *Slacku* sdílejí novinky z oboru. Přestože je vidět očividná snaha vedení o péči o zaměstnance, nabízí tato oblast ještě spoustu dalších možností a příležitostí, a to jak k upevnění pracovních vztahů mezi zaměstnanci (například workshopy), tak k jejich větší motivaci.

2.2.6 Kultura firmy

Faktor kultury (či také sdílených hodnot) firmy koexistuje s předchozím faktorem zaměřeným na spolupracovníky. To, že společnost XYZ současně prochází firemním redesignem (změna firemního designu, přehodnocení prezentace společnosti a budování jejího jména a pozice na trhu), poukazuje spolu s dalšími drobnými poznatky, získaných s osobních rozhovorů, na nízkou firemní kulturu a na nepříliš jasnou identitu společnosti

v této oblasti. I když by se dalo říci, že tato oblast neovlivňuje business společnosti, můžeme zde nacházet negativní nepřímé vlivy. Například snížení atraktivity mezi potenciálními zaměstnanci, tedy programátory, kteří jsou již tak obecně ceněným lidským pracovním zdrojem, ale také mezi potenciálními zákazníky, jež ocení stabilnější firmy, přičemž onu stabilitu mohou právě hodnotit dle firemní kultury a prezentace. Za jednu z příčin této nízké firemní kultury lze označit přílišné zapojení externích společností a OSVČ do primárních projektů společnosti. Každopádně společnost XYZ již tuto problematiku aktivně řeší, a protože tématem této diplomové práce není náprava interního fungování společnosti v oblasti řízení lidských zdrojů, pouze si dovoluje na tento nedostatek upozornit a předat ho dále ke zvážení vedení společnosti XYZ.

2.2.7 Schopnosti

Z osobních rozhovorů se zaměstnanci společnosti XYZ vyplynulo, že nejvýznamnější manažerskou osobou je majitel firmy. Přes všechny zmíněné výtky v předchozích dvou faktorech lze závěrem k rozboru „7 S faktorů“ zapsat, že z pohledu manažerského má majitel většinu základních vlastností důležitých pro úspěšné řízení společnosti, a to jak z hlediska znalostního, tak i z osobnostního. Spolu se současným projektovým manažerem vytváří respektované vedení, ve které zaměstnanci a obchodní partneři věří, což je podstatný faktor pro další vývoj této mladé společnosti.

2.3 GAP analýza

V rámci GAP analýzy bude konkrétně definováno, v jaké situaci se společnost XYZ současně nachází vzhledem k nařízení (tzv. stav „Kde jsme?“ dle terminologie GAP analýzy), z čehož vyplynou návrhy a doporučení pro dodržení pravidel nařízení, na základě kterých se společnost dostane do tzv. stavu „Kde chceme být?“.

Dále GAP analýza slouží jako jeden z důležitých výstupů pro prokázání souladu s GDPR (viz zjišťování současné situace ve společnosti a následně podávané návrhy a opatření). Oblastmi, kterými se GAP analýza zabývá jsou:

- angažovanost vedení,
- uzly zpracování osobních údajů,

- identifikace zpracování osobních údajů,
- datové toky,
- popsání současné bezpečnosti dat ve společnosti,
- souhrnná zpráva o nálezech a doporučeních.

2.3.1 Angažovanost vedení

Vedení společnosti XYZ, čímž je myšlen majitel a projektový manažer, je zapojeno do celého procesu a plně podporuje celkový projekt návrhu ochrany osobních dat dle obecného nařízení EU 2016/679 ze dne 27. dubna 2016, takže je zajištěna relevantnost prováděných analýz, které tak budou odpovídat skutečnosti, tudíž i pak návrhy a doporučení budou pro organizaci hodnotné.

2.3.2 Uzly zpracování osobních údajů

Následující část se zabývá uzly zpracování osobních údajů.

Uzlem zpracování osobních údajů se myslí místo, kde jsou osobní data shromažďována a zpracovávána.

Z pohledu uzavíraných smluv se jedná o:

- pracovní smlouvy uzavírané se zaměstnanci pracujícími na plný úvazek,
- dohody o provedení práce uzavírané se studenty pracujícími na částečný úvazek,
- smlouvy o dílo uzavírané s OSVČ,
- smlouvy o mlčenlivosti uzavírané se zaměstnanci a OSVČ,
- obchodní smlouvy uzavírané se zákazníky podnikajícími jako OSVČ.

Údaje ze smluv jsou pak využívány externí mzdovou účtárnou pro účely vedení účetnictví.

Při uplatňování slev na dani jsou společnosti XYZ jako zaměstnavateli předávány další osobní údaje jako:

- potvrzení o studiu.

Dalšími sběrnými místy osobních údajů jsou:

- online kontaktní formulář umístěný na stránkách společnosti XYZ,
- životopisy uchazečů na otevřené pracovní pozice přijímány elektronicky (vedeny v elektronické podobě na počítači majitele a projektového manažera a tisknuty do podoby papírové za účelem výběrového řízení),
- online tabulkový soubor s výpisem dovolených všech zaměstnanců (jméno a příjmení, termín a místo dovolené),
- elektronický dokument obsahující kontaktní údaje (telefonní čísla, e-mailové adresy) na zaměstnance, spolupracující OSVČ a zástupce spolupracujících právních společností, který je sdílen pouze mezi majitelem a projektovým manažerem, a údaje z něho dále využívány v jejich e-mailových klientech a mobilních telefonech,
- facebookové stránky společnosti XYZ sloužící výhradně pro firemní prezentaci, na kterých jsou zveřejňovány fotografie a videa se zaměstnanci, jež jsou na nich případně označováni.

Za specifická sběrná místa lze považovat užívané služby třetích stran, neboť ta využívají pracovní e-mailové adresy zaměstnanců a minimálně jejich jména, což je již dostatečná kombinace pro identifikaci subjektu osobních údajů. Jedná se zejména o dříve zmiňovaný:

- *Slack*,
- dále *Asanu*,
- a program *Paymo*, který monitoruje odpracovaný čas na konkrétních projektech, a který je instalován na počítačích a noteboocích zaměstnanců.

V případě těchto služeb, a dalších jiných, neboť počet používaných programů a služeb je variabilní, jsou zaměstnanci velmi dobře srozuměni s jejich užíváním, neboť si je vždy i sami zřizují a jedná se o služby nezbytné pro jejich práci ve firmě – viz komunikace, řízení projektů. Tyto údaje jsou uchovávány online u zmiňovaných poskytovatelů, kteří za uvedené údaje i zodpovídají, také jsou správci těchto osobních údajů a společnost XYZ nenese za jejich zpracování odpovědnost. I přesto by ale bylo namístě mít písemně potvrzeno, že zaměstnanec souhlasí se zakládáním účtů u třetích stran, které je nezbytné pro vykonávání jeho pracovní náplně, aby se vyhnulo zbytečným sporům.

Dalším výstupem této části je identifikace firemních zařízení a předmětů, které jsou nositeli vypsaných uzlů, a u kterých by měla být zajištěna dostatečná ochrana vzhledem k povaze údajů, jež uchovávají. Všechna tato zařízení a předměty jsou až na výjimky (viz mobilní telefony) umístěny ve společné kanceláři typu „open-space“, která je sdílena všemi zaměstnanci včetně projektového manažera a majitele společnosti. Konkrétně se jedná o tato zařízení a předměty:

- stolní počítač majitele,
- počítač projektového manažera,
- server pro zálohování firemních dat,
- firemní mobil majitele,
- firemní mobil projektového manažera,
- tiskárna,
- uzamykatelná skříň na dokumenty.

Ostatní zaměstnanci využívají pro práci vlastní notebooky, které tedy využívají i k osobním účelům, a které jsou proto primárně hodnoceny jako jejich vlastní osobní majetek. Jelikož však žádný z nich nenese výše zmíněný uzel, v rámci kterého je společnost XYZ správcem, budou dále řešeny až v návrhové části, kde bude navrhnuto jejich zabezpečení, jak kvůli ochraně zaměstnanců, tak kvůli situaci, kdy společnost XYZ v roli zpracovatele pro své klienty musí zajistit dostatečnou bezpečnost a soulad s nařízením GDPR.

Zmiňovaný server je v kanceláři umístěn zcela volně a je komukoli přístupný. Především je využíván pro zálohování dat ze stolních počítačů majitele a projektového manažera, přičemž na něj mohou zálohovat svá pracovní data i ostatní zaměstnanci.

2.3.3 Identifikovaná zpracování osobních údajů

Po identifikaci uzlů zpracování osobních údajů přichází identifikace jednotlivých zpracování osobních údajů vycházejících z dotazníku A, B, doplněného C a D. U těchto zpracování jsou vypsány nejdůležitější body pro zjištění současné situace, která bude důležitým vstupem pro část s vlastními návrhy a doporučeními, jež bude napravovat zjištěné nedostatky. Dotazníky byly vyplněny v součinnosti s vedením společnosti.

U jednotlivých zpracování OÚ se řeší:

- vztah organizace ke zpracování (zda je správcem),
- zda organizace využívá zpracovatele,
- subjekty údajů (respektive řešená skupina subjektů),
- právní základ zpracování,
- zda byl poskytnut souhlas,
- rozsah zpracování (subjekty, které dané zpracování obsahuje),
- jaké jsou konkrétní identifikátory (jaké osobní údaje se shromažďují),
- zda je informování subjektů povinné (a je-li tomu tak, zda bylo provedeno),
- informace o zahrnutí do řízení incidentů,
- způsob uložení osobních údajů,
- doba jejich zpracování,
- interní odpovědnost za dané zpracování,
- výpis pracovníků společnosti seznamujících se s danými osobními údaji.

Pro zpracování osobních údajů ve společnosti XYZ byly definovány tři hlavní skupiny subjektů údajů. První jsou zaměstnanci, druhou jsou subjekty v rámci dodavatelsko-odběratelských vztahů a třetí, více zobecněnou skupinou, jsou tzv. „jiné osoby“ zahrnující odesílatele webového formuláře na stránkách společnosti XYZ a uchazeče o zaměstnání v této organizaci.

Z nejvýznamnějších skupin subjektů zpracování jsou pro společnost XYZ zaměstnanci, a to především z důvodů zákonných a personálně-mzdové agendy, ale také organizačních a propagačních potřeb.

V rámci skupiny osobních údajů zaměstnanců zpracovávaných ze zákonné povinnosti a za účelem personální a mzdové činnosti byly identifikovány následující zpracování osobních údajů:

- zpracování OÚ v rámci pracovní smlouvy,
- zpracování OÚ v rámci DPP,
- zpracování OÚ v rámci potvrzení o studiu.

Kvůli daňovým, zákonným či jiným povinnostem se k pracovním smlouvám či k DPP uzavíraných se zaměstnanci mohou vázat další dokumenty či dodatky, které mohou navíc obsahovat i další subjekty OÚ, než je daný zaměstnanec (například jeho

rodinné příslušníky). Ačkoli se v současnosti toto společnosti XYZ netýká, je třeba, aby tento fakt brala na zřetel a v případě zpracování takového „dodatečného“ dokumentu (jako například již řešené potvrzení o studiu) i taková zpracování zařadila do seznamu zpracování.

Zpracování OÚ za účelem personální a mzdové činnosti nesou shodné body v několika případech:

- vztah organizace ke zpracování: správce,
- využíván zpracovatel: ano – externí mzdová účtárna,
- subjekty údajů: zaměstnanec,
- právní základ zpracování: plnění zákonných a smluvních povinností, plnění personální a mzdové agendy,
- rozsah zpracování: zaměstnanec,
- informování subjektů údajů: ne, tato zpracování to nevyžadují,
- řízení incidentů: incident není řízen,
- uložení osobních údajů: fyzické, elektronické (jak u správce, tak zpracovatele),
- doba zpracování: dle současných zákonných povinností,
- interní odpovědnost za zpracování: majitel společnosti,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti.

Zpracování OÚ v rámci pracovní smlouvy:

- souhlas: ne,
- identifikátory: jméno, příjmení, rodné číslo / datum narození, místo narození, číslo občanského průkazu, trvalé bydliště, číslo bankovního účtu, podpis.

Zpracování OÚ v rámci dohody o provedení práce:

- souhlas: ano – ke zpracování poskytnutých osobních údajů vč. rodného čísla pouze za účelem personální a mzdové agendy a v zájmu dodržení právních povinností uložených zaměstnavateli zvláštními zákony,
- identifikátory: jméno, příjmení, rodné číslo / datum narození, místo narození, číslo občanského průkazu, trvalé bydliště, číslo bankovního účtu, podpis.

Zpracování OÚ v rámci potvrzení o studiu:

- souhlas: ne,
- nejčastější identifikátory: název vzdělávací instituce, studijního programu, jméno a příjmení, datum a místo narození, aktuální akademický rok (od–do), stupeň a typ studia.

Z GDPR vyplývá, že není vhodné mít ve smlouvě uvedený souhlas (viz jeho dobrovolnost a nepodmíněnost), proto je vhodné připravit dodatky k DPP či sepsat nové dohody.

V rámci zpracovávaných osobních údajů zaměstnanců z organizačních a propagačních důvodů byla identifikována tato zpracování:

- zpracování OÚ v rámci seznamu dovolených,
- zpracování OÚ v rámci facebookových stránek společnosti.

I tato zpracování OÚ zaměstnanců z organizačních a propagačních důvodů sdílejí stejná kritéria:

- vztah organizace ke zpracování: správce,
- využíván zpracovatel: ne,
- subjekty údajů: zaměstnanec,
- právní základ zpracování: žádný,
- souhlas: ne,
- rozsah zpracování: zaměstnanec,
- řízení incidentů: incident není řízen,
- doba zpracování: neomezená,
- interní odpovědnost za zpracování: majitel společnosti,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti, projektový manažer.

Za problematický bod lze označit dobu zpracování, která by měla být pro každé zpracování osobních údajů jasně definována časovým intervalem.

Zpracování OÚ v rámci seznamu dovolených:

- identifikátory: jméno a příjmení,
- informování subjektu údajů: ne, leč zaměstnanci tyto údaje zadávají sami,

- uložení osobních údajů: elektronické (online tabulkový dokument dosažitelný prostřednictvím sdíleného odkazu).

Ačkoli zaměstnanci zadáváním informací o jejich dovolené jsou logicky informováni o tomto sdíleném dokumentu, je vhodné zajistit i písemné potvrzení o této informovanosti a souhlas ke zpracování definovaných osobních dat. Především je však nutné dostát lepšímu zabezpečení co se týče přístupnosti dokumentu a bude vhodné i přehodnotit, kdo všechno tyto informace smí vidět a zda je nutné, aby jednotliví zaměstnanci viděli dovolené svých kolegů, neboť i v tomto bodě může dojít ke spornému bodu, ve kterém se zbytečně sdílejí informace (neboť nepřítomnosti zaměstnance v jeho bydlišti může být zneužito), a ve kterém zaměstnanci může vadit vůbec takové informace sdílet s osobami, s nimiž to není nezbytně nutné.

Zpracování OÚ v rámci facebookových stránek společnosti:

- identifikátory: obrazový a zvukový záznam zaměstnance, případně jeho další identifikace prostřednictvím odkazu na jeho facebookový profil,
- informování subjektu údajů: ne, ale subjekt by měl být informován,
- uložení osobních údajů: elektronické (facebookové stránky společnosti XYZ).

V případě facebookových stránek společnosti je nezbytné, aby o tom zaměstnanci byli informováni a společnost měla jejich souhlas s těmito údaji pracovat a vůbec je uchovávat.

Vedle zaměstnanců je neméně důležitá skupina subjektů zpracování z oblasti dodavatelsko-odběratelských vztahů. V této skupině byla vypracována následující zpracování:

- zpracování OÚ v rámci smlouvy o díle,
- zpracování OÚ v rámci obchodní smlouvy.

Společnými atributy dvou výše zmíněných zpracování jsou:

- vztah organizace ke zpracování: správce,
- využíván zpracovatel: ano – externí mzdová účtárna,
- právní základ zpracování: plnění zákonných a smluvních povinností,
- souhlas: ne,

- identifikátory: jméno a příjmení, bydliště vázané k podnikání, IČ, telefonní číslo, e-mail, číslo bankovního účtu, podpis;
- informování subjektu údajů: ne, tato zpracování to nevyžadují,
- řízení incidentů: incident není řízen,
- uložení osobních údajů: fyzické, elektronické (skříňka, počítač majitele, počítač projektového manažera),
- doba zpracování: dle současných zákonných povinností,
- interní odpovědnost za zpracování: majitel společnosti,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti, projektový manažer.

Zpracování OÚ v rámci smlouvy o díle:

- subjekty údajů: jednající (OSVČ),
- rozsah zpracování: jednající.

Zpracování OÚ v rámci obchodní smlouvy:

- subjekty údajů: klient (OSVČ),
- rozsah zpracování: klient.

Společným zpracováním pro zaměstnance OSVČ je:

- zpracování OÚ v rámci smlouvy o mlčenlivosti.

Zpracování OÚ v rámci smlouvy o mlčenlivosti:

- vztah organizace ke zpracování: správce,
- využíván zpracovatel: ne,
- subjekty údajů: zaměstnanci / OSVČ,
- právní základ zpracování: žádný,
- souhlas: ano,
- rozsah zpracování: zaměstnanec / OSVČ,
- identifikátory: jméno a příjmení, datum narození, rodné číslo v případě zaměstnanců, IČO v případě OSVČ, trvalé bydliště, telefon, e-mail,
- informování subjektu údajů: ne, tato zpracování to nevyžadují,
- řízení incidentů: incident není řízen,
- uložení osobních údajů: fyzické, elektronické (skříňka, počítač majitele),

- doba zpracování: 5 let,
- interní odpovědnost za zpracování: majitel společnosti,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti.

Jelikož je ve smlouvě o mlčenlivosti poskytován souhlas, je třeba vytvořit smluvní dodatek či sepsat smlouvu novou.

Zaměstnanci, spolupracující fyzické osoby, ale také zástupci právních společností, se kterými společnost XYZ spolupracuje, se společně objevují v kontaktním dokumentu, ze kterého vzniklo:

- zpracování OÚ v rámci elektronického kontaktního dokumentu.

Zpracování OÚ v rámci elektronického kontaktního dokumentu:

- vztah organizace ke zpracování: správce,
- využíván zpracovatel: ne,
- subjekty údajů: zaměstnanci, spolupracující OSVČ a zástupci spolupracujících společností,
- právní základ zpracování: žádný,
- souhlas: ne,
- rozsah zpracování: zaměstnanci, OSVČ, zástupci spolupracujících společností,
- identifikátory: jméno a příjmení, telefon, e-mail,
- informování subjektu údajů: ne, ale měl by být informován,
- řízení incidentů: incident není řízen,
- uložení osobních údajů: elektronické (sdílený online dokument mezi majitelem a projektovým manažerem, osobní údaje uloženy též v jejich mobilních telefonech a e-mailových klientech),
- doba zpracování: po dobu spolupráce (trvání smluvního vztahu),
- interní odpovědnost za zpracování: majitel společnosti,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti, projektový manažer.

U zpracování OÚ v rámci elektronického kontaktního dokumentu je třeba získat souhlas nejen k uchovávání identifikovaných osobních údajů v rámci řešeného

dokumentu, ale i k dalšímu využívání (viz mobilní zařízení, e-mailoví klienti), přičemž by se měl nastavit i konkrétní hraniční strop doby zpracování u těchto údajů.

Poslední řešenou skupinou subjektů zpracování ve společnosti XYZ je skupina subjektů označena jako „jiné osoby“, což jsou takové subjekty, které nelze v řešené společnosti generalizovat jako tomu bylo u předchozích dvou skupin subjektů, a to kvůli svým specifikům. Jedná se o:

- zpracování OÚ v rámci webového kontaktního formuláře,
- zpracování OÚ v rámci životopisů uchazečů.

Přestože jsou zpracování vůči sobě vzhledem k řešeným subjektům rozličnější, než tomu bylo u předchozích případů, nalézáme i zde identické atributy, z kterýchžto se některé opakují napříč všemi zpracováními:

- vztah organizace ke zpracování: správce,
- využíván zpracovatel: ne,
- subjekty údajů: jiné osoby,
- právní základ zpracování: žádný,
- souhlas: ne,
- informování subjektu údajů: ne, ale subjekt by měl být informován,
- řízení incidentů: incident není řízen,
- interní odpovědnost za zpracování: majitel společnosti.

Je zřejmé, že u obou zpracování OÚ (webového kontaktního formuláře, životopisů uchazečů) je třeba dodat souhlasy ke zpracování osobních údajů, i když v případě životopisů lze argumentovat, že uchazeč svým zasláním životopisu se zpracováním souhlasí, přesto je třeba takovou situaci ošetřit a dle způsobu získání životopisu na to reagovat.

Zpracování OÚ v rámci webového kontaktního formuláře:

- rozsah zpracování: osoba odesílající formulář,
- identifikátory: jméno (není explicitně vyžadováno příjmení, respektive celého jména v podobě „jméno a příjemní“), e-mailová adresa,
- uložení osobních údajů: elektronické (obsah formuláře přichází jako elektronická zpráva na e-mailovou adresu majitele společnosti),
- doba zpracování: nezbytně dlouhá pro další komunikaci,

- interní odpovědnost za zpracování: majitel společnosti,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti.

Zpracování OÚ v rámci životopisů uchazečů:

- rozsah zpracování: uchazeč o zaměstnání,
- nejčastější identifikátory: jméno a příjmení, e-mailová adresa, telefonní číslo, datum narození,
- uložení osobních údajů: elektronické (počítač majitele anebo/a počítač projektového manažera), případně fyzické (životopis vytisknut),
- doba zpracování: po dobu přijímacího řízení,
- interní odpovědnost za zpracování: majitel společnosti, projektový manažer,
- pracovníci společnosti seznamující se s osobními údaji: majitel společnosti, projektový manažer.

Jak u zpracování osobních údajů v rámci webového kontaktního formuláře, tak v rámci životopisů uchazečů jsou vágně definované délky zpracování, u kterých by se měla určit alespoň maximální doba zpracování.

Po důkladné analýze a četných konzultacích byla získána výše uvedená zpracování osobních údajů. Ke všem byl poskytnut detailní popis a komentáře, jež najdou využití v kapitole zabývající se návrhem řešení. U všech zpracování byl taktéž zjištěn nedostatek v neexistujícím řízení případných incidentů, který by měl být odstraněn. V případě situací, kdy společnost XYZ vystupuje jako zpracovatel pro své klienty, a kdy její zaměstnanci pracují s osobními údaji zákazníků klientů společnosti XYZ prostřednictvím databází, ke kterým zaměstnanci potřebují přístup kvůli vykonání zadané práce, je třeba brát na zřetel, že taková místa existují a zajistit správné bezpečnostní postupy, které budou předmětem návrhové části této diplomové práce. Jejich počet a podoba je proměnlivá a nelze je jednoznačně definovat zobecňujícím přístupem pro všechny případy, spíše je vhodnější nadefinovat vhodný postup řešení práce s nimi.

2.3.4 Datové toky

Pomocí diagramů toku dat bude promítnuta práce s daty probíhající v rámci identifikovaných zpracování osobních údajů ve společnosti XYZ. Diagramy toku dat jsou

zpracovány v programu *MS Visio Professional 2016* za využití jeho obrazců DFD (kruh značí proces/stav, plný obdélník entitu, tečkovaný ohraničený obdélník úložiště dat a šipky činnosti/procesy).

Následující diagram uvádí čtenáře do kontextu a zobrazuje základní procesy na nulté úrovni, které budou dále rozepsány do potřebných detailů opět pomocí diagramů toku dat, jež budou doplněny o zjednodušený doprovodný textový popis upřesňující některé méně zřejmé skutečnosti.

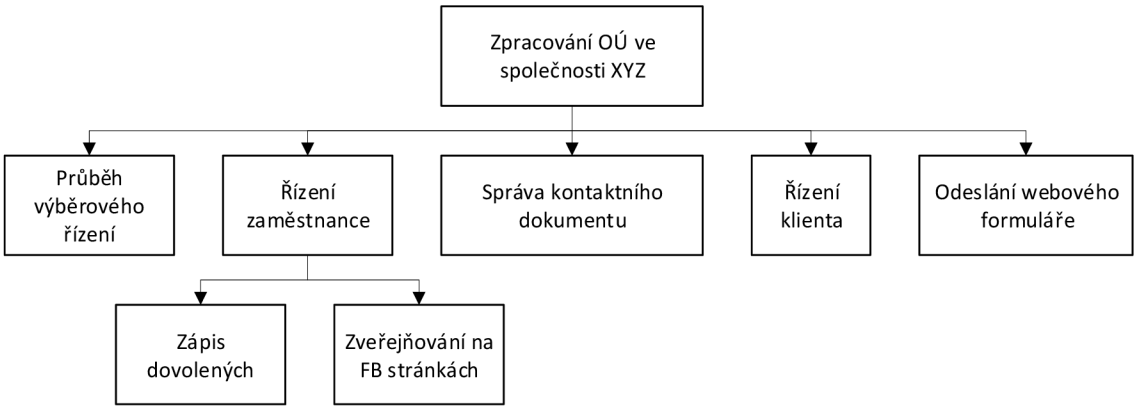


Diagram č. 1: Zpracování OÚ ve společnosti XYZ

(Vlastní zpracování)

Jako první vystupuje tok dat v rámci průběhu výběrového řízení, kde jako subjekt zpracování OÚ vystupuje uchazeč o zaměstnání poskytující životopis v elektronické podobě majiteli a projektovému manažerovi. Životopis je následně uchováván v jejich e-mailových klientech a vytisknut pro účely výběrového řízení. Za odstranění životopisu opět zodpovídá majitel či projektový manažer (záleží na konkrétní situaci).

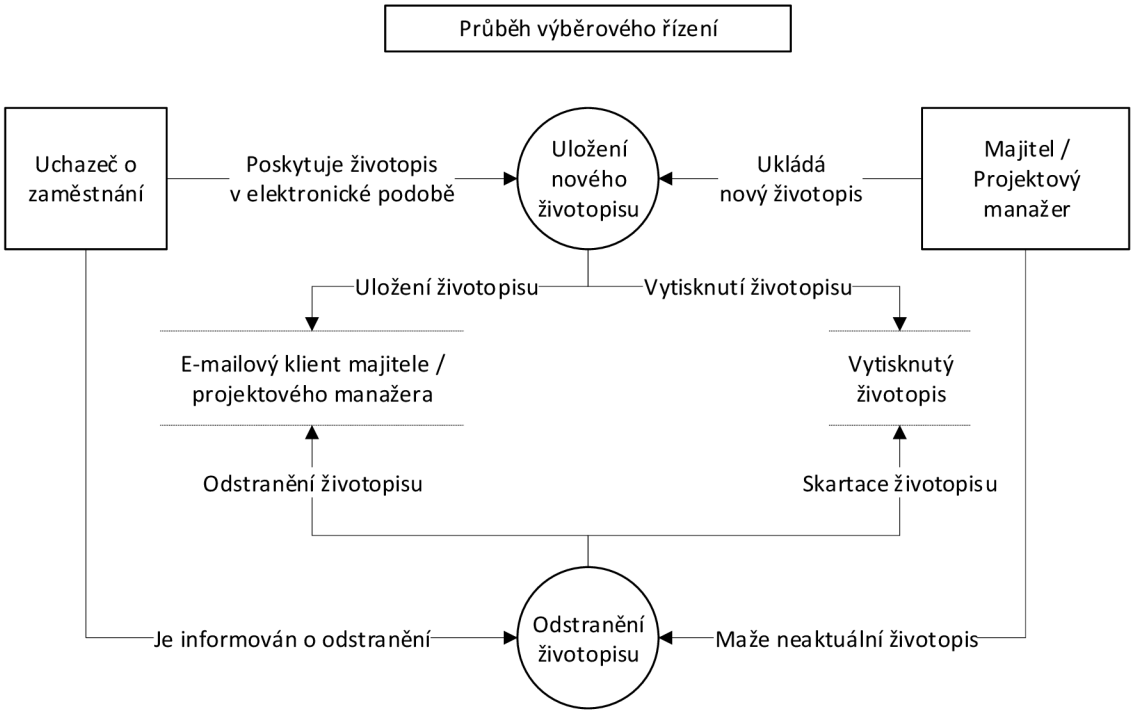


Diagram č. 2: Tok dat při průběhu výběrového řízení

(Vlastní zpracování)

Druhým procesem zpracování osobních údajů z pohledu toku dat je řízení zaměstnance, na které navazuje zápis dovolených a zveřejňování údajů zaměstnanců na firemních FB stránkách, jelikož oba zmíněné procesy se zaměstnancem souvisí, resp. zaměstnanec je hlavním subjektem osobních údajů. Zaměstnancem se v tomto datovém toku nemyslí nejen zaměstnanec na hlavní pracovní úvazek a zaměstnanec na dohodu o provedení práce, ale taktéž OSVČ spolupracující se společností XYZ (v roli dodavatele - například externí programátor/ka PHP). Důležitým dodatkem je, že OSVČ se dovolené a FB stránky netýkají, leč jako obecně, ani zde v datových tocích nelze vyobrazit rozhodovací procesy.

Tentokrát zde vystupuje jako subjekt zpracování OÚ zaměstnanec, s jehož údaji pracuje majitel a externí mzdová účtárna.

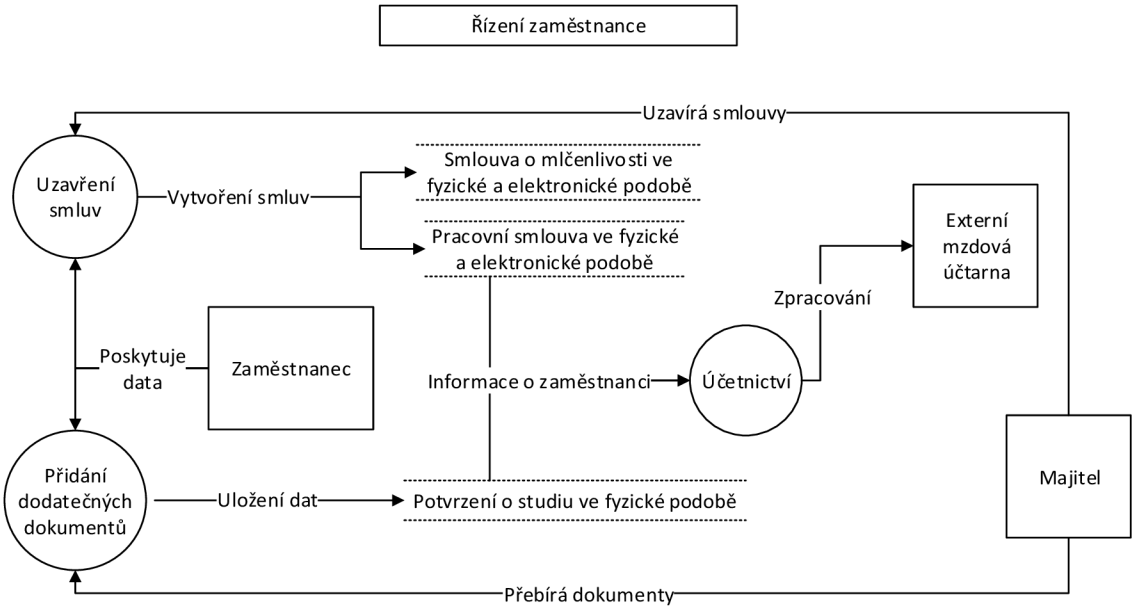


Diagram č. 3: Tok dat při řízení zaměstnance

(Vlastní zpracování)

Zápis dovolených je podstatně jednodušší a vystupuje v něm pouze jedno úložiště dat v podobě online sdíleného tabulkového dokumentu.

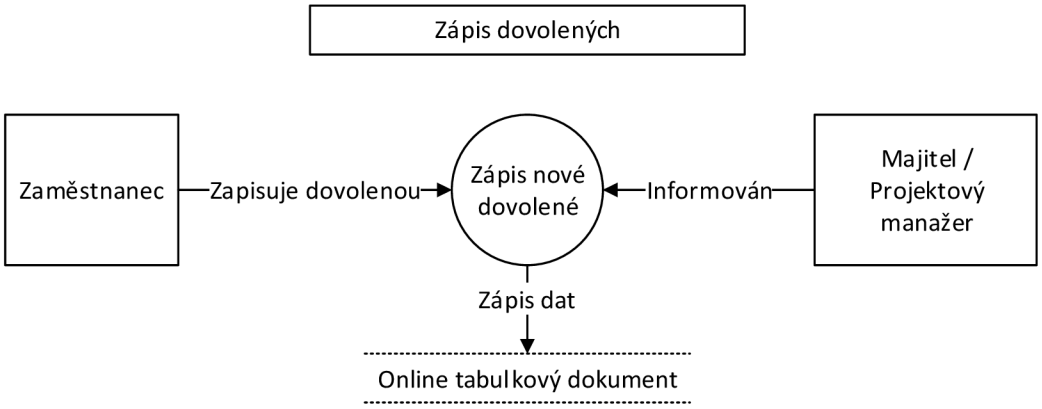


Diagram č. 4: Tok dat při zápisu dovolených

(Vlastní zpracování)

Při zveřejňování příspěvků na facebookových stránkách společnosti XYZ přidává příspěvky majitel či projektový manažer, přičemž zaměstnanec by měl být o této situaci informován.

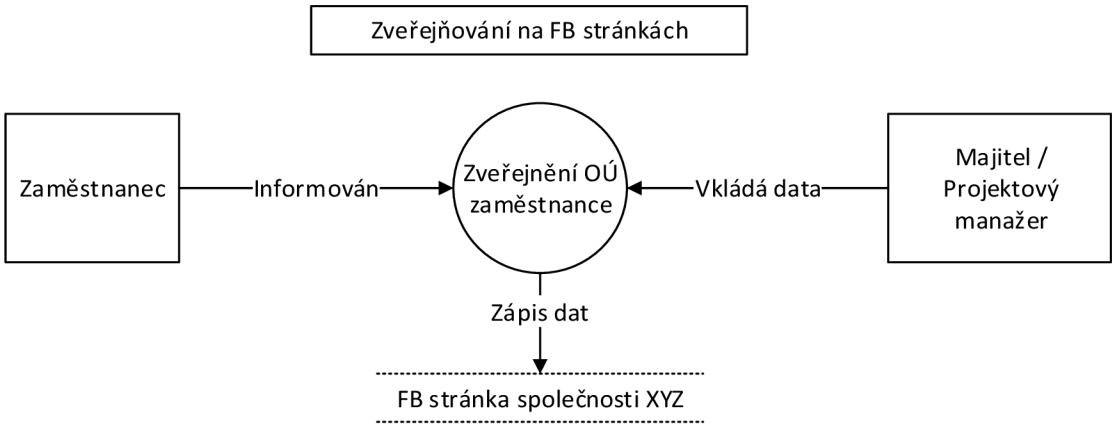


Diagram č. 5: Tok dat při zveřejňování na FB stránkách

(Vlastní zpracování)

U kontaktního dokumentu vystupuje několik subjektů zpracování OÚ – zaměstnanec, OSVČ (jak v roli dodavatele, tak odběratele) a zástupce spolupracující společnosti. Ačkoli primárním úložištěm dat je řešený sdílený online dokument, osobní údaje z něho jsou dále užívány i v mobilních telefonech a e-mailových klientech.

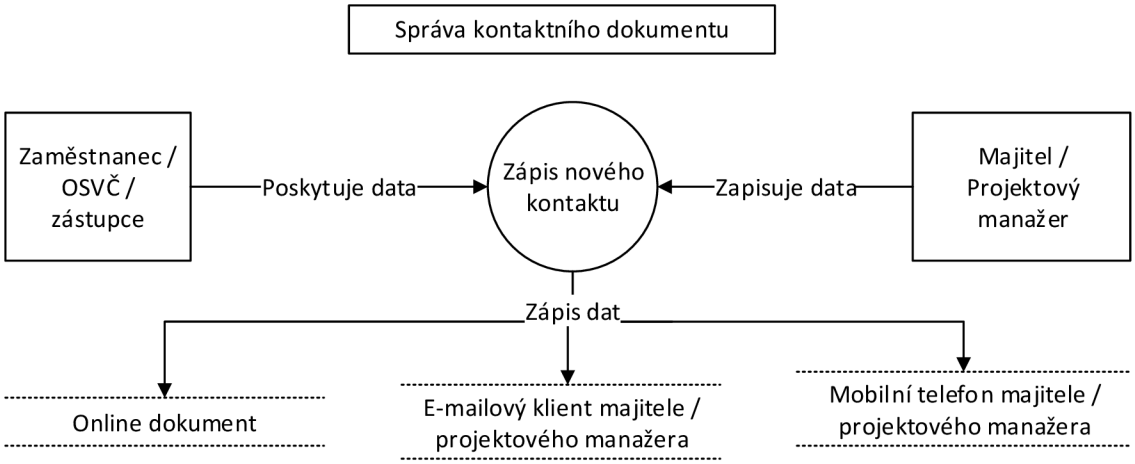


Diagram č. 6: Tok dat při správě kontaktního dokumentu

(Vlastní zpracování)

Subjektem OÚ při řízení klienta je samotný klient. S daty, které poskytuje do obchodní smlouvy, přichází do styku majitel a projektový manažer. Externě poté mzdová účtárna.

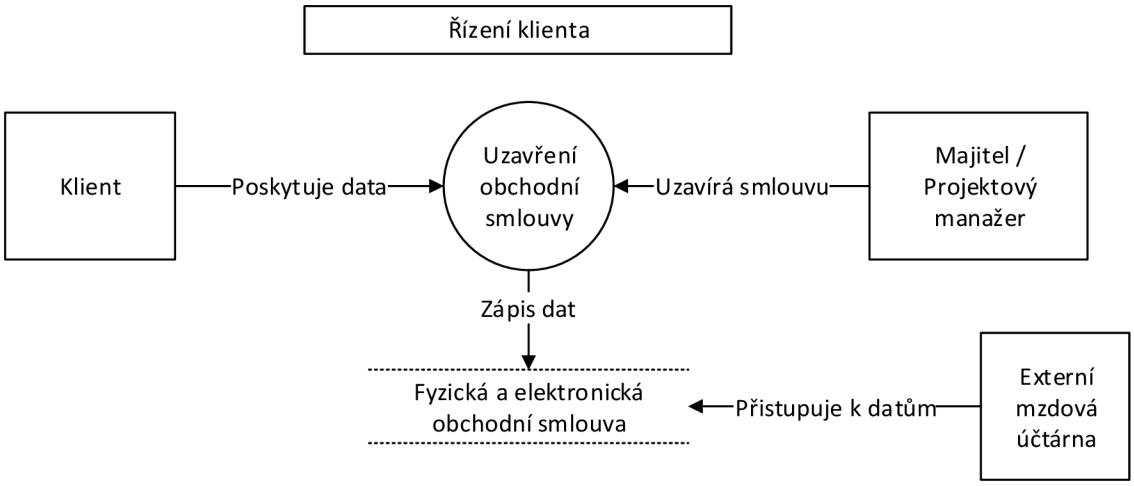


Diagram č. 7: Tok dat při řízení klienta

(Vlastní zpracování)

Mimo zaměstnanecké vztahy a dodavatelsko-odběratelský řetězec stojí zpracování OÚ, ke kterému dochází během odeslání webového kontaktního formuláře společnosti XYZ. Zde je subjektem OÚ návštěvník stránky odesílající formulář. Úložištěm dat se myslí e-mailová schránka majitele, který též jako jediný přistupuje k získaným datům z formuláře.

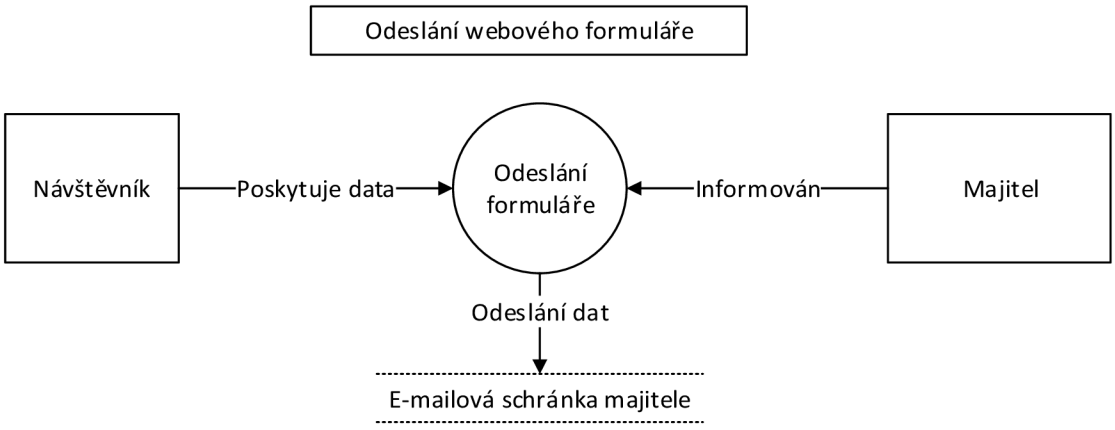


Diagram č. 8: Tok dat při odeslání webového formuláře

(Vlastní zpracování)

Pomocí předešlých diagramů toků dat došlo k lepší vizualizaci práce s osobními údaji a především k přehlednější identifikaci zapojených subjektů a dotčených datových úložišť.

2.3.5 Současná bezpečnost

Následující část zhodnotí současnou bezpečnost dat dle doposud zjištěných informací a konzultací s vedením společnosti XYZ. Na bezpečnost dat bude nahlédnuto ze čtyř různých úhlů pohledu, a to dle fyzické bezpečnosti, bezpečnosti toku dat, bezpečnosti lidských zdrojů a nakonec dle politik pro bezpečnost dat.

Fyzická bezpečnost

Společnost XYZ sídlí v komplexu, ve kterém je i několik dalších společností, tudíž zde existuje společný vchod. Ten je od 8:00 do 20:00 volně otevřen, avšak v této době sleduje pohyb u vstupu recepční. Mimo uvedený časový interval je přístup povolen pouze zaměstnancům s čipovou kartou a heslem (tj. pro otevření hlavních vchodových dveří je nutné přiložit kartu a zadat heslo). Prostor je monitorován, avšak za zpracování těchto osobních údajů zodpovídá správce budovy. Dalším možným přístupovým bodem do budovy je příjezdová cesta vedoucí k parkovišti budovy, ta je však chráněna závorou, kterou lze zvednout pouze čipovou kartou. Kancelář samotné společnosti XYZ se pak nachází ve čtvrtém patře, které je dostupné schodištěm či výtahem fungujícím na čipovou kartu. Kancelář má samozřejmě uzamykatelné dveře, ale mimo majitele a zaměstnance má přístup do kanceláře i správce budovy (viz klíče) a uklízečky zajišťující úklid jednou týdně.

Vedení elektřiny je v budově propojené, přičemž společnost XYZ nemá žádný záložní zdroj energie v případě výpadku elektrického proudu. Co se týče požární ochrany, na chodbách jsou umístěny hasící přístroje. Riziko vytopení vodou je minimalizováno, neboť v kanceláři není napojen žádný vodovodní rozvod a sociální zařízení jsou o několik kanceláří vzdáleny.

V kanceláři zůstávají vždy dva stolní počítače (majitele a projektového manažera), které jsou chráněny uživatelským heslem (OS Windows 10). Fyzicky nejsou nijak připevněny. V kanceláři je také menší server, který je lehce odpojitelný

a odcizitelný, navíc umístěný přímo u dveří. Přístup k datům, které nese, není nikterak současně zabezpečen.

Zmiňované čipové karty a klíče ke kanceláři mají všichni zaměstnanci společnosti.

Bezpečnost toku dat

Správu sítě v budově zajišťuje její správce. Včetně monitoringu sítě, tudíž by měl zajistit nejen její bezpečnost, ale také detekci narušení sítě a další kroky pro promptní řešení vzniklého incidentu.

Síť společnosti XYZ je oddělena od sítí ostatních společností (vlastní VLAN síť). Všechny počítače a notebooky se k internetu připojují prostřednictvím kabelů. Existuje zde možnost i připojení přes WiFi, které zajišťuje zabezpečený router, jenž má silné heslo a navíc filtruje zařízení dle povolených MAC adres. Jestliže se chce na WiFi připojit někdo dočasně, pak může využít nezaheslovanou WiFi poskytovanou správcem budovy, což vzhledem k bezpečnosti není doporučováno.

Pro zajištění hrozeb ze sítě mají všichni zaměstnanci na svých zařízeních nainstalovaný Avast Business Antivirus, který mimo základní antivirovou ochranu nabízí ochranu před malwarem, ransomwarem a spywarem. Obsahuje i behaviorální štít, CyberCapture, celkový test, kontrolu Wi-Fi sítě, firewall, webový a e-mailový štít, antispam a sandbox.

U sdílených online dokumentů není striktně ošetřeno, kdo smí k dokumentům přistupovat, což např. u seznamu s dovolenými by bylo vhodné regulovat na majitele, popř. projektového manažera.

Avšak zabezpečení webového kontaktního formuláře pomocí metody POST je dostačující.

Bezpečnost lidských zdrojů

Není striktně sledováno, kdo a v jakou dobu se v kanceláři nachází, ale existují kamery na chodbě kanceláře společnosti, které je možné využít v případě nutnosti identifikace osob.

Kvůli mzdové agendě a dalším účetním činnostem přichází často do styku externí mzdová účtárna, se kterou neexistuje smluvní ošetření, ve kterém je zaneseno, že účtárna zodpovídá za práci se získanými osobními údaji. Chybí i smluvní ošetření odpovědnosti

partnerů společnosti, o jejich odpovědném nakládání s osobními údaji, s jimiž přicházejí do styku při vykonávání práce pro společnost XYZ.

Politiky bezpečnosti dat

Co se týče dokumentace ve společnosti XYZ vůbec, neexistují žádné směrnice o jejich uchovávání, tj. dokumentace není oficiálně řízena. Fyzické uložení dokumentů ve skříni v kanceláři není dostačující, neboť skříň je sice uzamykatelná, ale vzhledem ke své velikosti a váze snadno manipulativní.

Protože neexistují žádné směrnice, zavedené oficiální postupy pro práci na počítači, zajištění bezpečnosti dat ani elektronická úschova dokumentů, nic z toho není prokazatelné.

S neexistující bezpečnostní politikou práce na počítači (včetně heslové politiky) souvisí i neprokazatelnost společnosti XYZ, co se týče bezpečnosti osobních údajů klientů, resp. zákazníků klientů, se kterými zaměstnanci společnosti přichází do styku v roli zpracovatele.

Také neexistuje žádná směrnice či oficiální postup, jak se serverem zacházet, tudíž neexistuje vůbec přehled o nahraných datech, která jsou navíc dostupná všem přistupujícím k úložišti.

2.3.6 Souhrnná zpráva o nálezech a doporučeních

Cílem souhrnné zprávy je podat na základě zjištěných nálezech taková doporučení, kterážto posunou společnost XYZ do stavu „kde chceme být“, aby byl zajištěn soulad s GDPR. Tato vstupní zpráva je jedním z dokumentů prokazující odpovědný přístup správce.

V prvé řadě je nutné ošetřit smluvní vazby, a to za odborné právní konzultace, která zajistí soulad smluv z pohledu GDPR, případně nejlépe ponese odpovědnost za správnost jejich sestavení. Vzhledem k tomu, že v některých smlouvách se objevil souhlas, je nezbytné, aby smlouvy byly přepsány či k nim byly vytvořeny dodatky.

Dále je třeba vytvořit zpracovatelské smlouvy s externími subjekty, čímž se myslí konkrétně mzdová účtárna, ale také externí spolupracující OSVČ a společnosti,

resp. dodavatelé. Vhodným krokem je, aby společnost XYZ nabídla totéž svým klientům, pro které je ona v roli zpracovatele.

U zjištěných zpracování osobních údajů zajistit definování doby zpracování, získání souhlasů a provedení informovanosti (tam, kde je to nutné).

Také je třeba vypracovat doposud chybějící dokumentace, resp. směrnice, jasně určující řešená fakta a postupy. Jedná se o směrnici o řízení dokumentů (jak ve fyzické, tak elektronické podobě), směrnici o bezpečnostní politice práce na počítači (zahrnující jak heslovou politiku, tak bezpečnost práce s daty) a směrnici týkající se serveru (jeho zabezpečení, prováděných činnostech, uchovávaných datech).

Z výše uvedeného vyplývá, stejně tak jako z role zpracovatele osobních údajů, ve které se společnost XYZ nachází, aby došlo k implementaci ISMS systému, alespoň v té části dotýkající se ochrany dat. V rámci toho by měla vyplynout další bezpečnostní opatření a taktéž by mělo dojít k zajištění řízení incidentů, jenž u všech identifikovaných zpracování osobních údajů chybí.

Neméně důležité je i fyzické zabezpečení serveru a skříně obsahující řešené dokumenty.

Závěrem souhrnná zpráva předkládá stručný výpis bodů vycházejících z výše vypsaného a z celkové GAP analýzy, které jsou navrženy k naplnění, aby společnost XYZ došla k souladu s GDPR:

- ošetření současných smluv za odborné právní konzultace,
- vytvoření zpracovatelských smluv,
- u zpracování osobních údajů určit doby zpracování, získat potřebné souhlasy, provést nezbytné informovanosti a zajistit řízení incidentů,
- směrnice (řízení dokumentů, bezpečnostní politika práce na počítači, o serveru),
- alespoň částečná implementace ISMS s ohledem na bezpečnost dat,
- fyzické zabezpečení skříně na dokumenty a serveru.

2.4 DPIA

DPIA řeší řízení rizik pro práva subjektů osobních údajů. Její součástí je identifikace zpracování OÚ a procesů, posouzení rizik spojených se zpracováním OÚ, zásady ochrany OÚ a celkové řízení těchto rizik (monitoring, přezkoumávání), přičemž všechny kroky by měly být řádně dokumentovány a výstupem by měla být zpráva o DPIA.

Jelikož DPIA je povinné pouze pro taková zpracování, která přináší vysoké riziko pro práva a svobody fyzických osob, je v případě společnosti XYZ zřejmé, že žádného zpracování se toto netýká. Každopádně i přes to je doporučeno posouzení provést kvůli možnosti odhalení možných nedostatků a dostání povinnosti posouzení mít, jestliže dozorující úřad v případě kontroly uzná za vhodné DPIA vypracovat (viz nepřesné určení ze strany GDPR takových případů, kdy je nutné DPIA provést).

2.4.1 Identifikace zpracování OÚ a procesů

Pro identifikaci procesů (viz datové toky a jejich slovní popis v GAP analýze) a identifikovaných zpracování OÚ budou využity již zjištěné výstupy z GAP analýzy.

GAP analýza přinesla výpis následujících zpracování:

- zpracování OÚ v rámci pracovní smlouvy,
- zpracování OÚ v rámci dohody o provedení práce (DPP),
- zpracování OÚ v rámci potvrzení o studiu,
- zpracování OÚ v rámci seznamu dovolených,
- zpracování OÚ v rámci facebookových stránek společnosti,
- zpracování OÚ v rámci smlouvy o díle,
- zpracování OÚ v rámci obchodní smlouvy,
- zpracování OÚ v rámci smlouvy o mlčenlivosti,
- zpracování OÚ v rámci elektronického kontaktního dokumentu,
- zpracování OÚ v rámci webového kontaktního formuláře,
- zpracování OÚ v rámci životopisů uchazečů.

2.4.2 Posouzení rizik spojených se zpracováním OÚ

Jak bylo z úvodu této kapitoly určeno, vypsaná zpracování nehrozí vysokým rizikem dopadu na svobody a práva fyzických osob. Jedná se především o osobní údaje zpracovávané v rámci zaměstnaneckého poměru a dodavatelsko-odběratelském řetězci, která jsou navíc většinou nutná pro plnění zákonných a smluvních povinností.

Osobní údaje vázající se k seznamu dovolených, FB stránkám a kontaktnímu dokumentu nejsou takové povahy, aby mohly zapříčinit ono vysoké riziko dopadu.

2.4.3 Zásady ochrany OÚ

V rámci smluv je doporučeno provést za odborné konzultace minimalizaci zpracovávaných osobních údajů. Stejně tak je navrženo provést pseudonymizaci v případě zpracování OÚ v rámci seznamu dovolených a v rámci elektronického kontaktního dokumentu.

2.4.4 Závěr k DPIA

Po zapracování doporučení a návrhů do jednotlivých zpracování je doporučeno sepsat zprávu DPIA, na které by se měl podílet správce (tj. vedení organizace) a osoba v roli DPO. Ačkoli z titulu zaměstnávání není nutné zaměstnávat DPO a současná situace ve společnosti XYZ takovou osobu ani na plný úvazek nevyžaduje, je navrhováno, aby taková osoba na částečný úvazek existovala a zajišťovala bezpečnost osobních údajů.

2.5 Zhodnocení analytické části

Za asistovaného zhodnocení v podobě konzultací s vedením společnosti byl zjištěn současný stav společnosti XYZ. V prvé řadě byl proveden rozbor „7 S faktorů“, a poté již následovala GAP analýza a DPIA. GAP analýza zajistila angažovanost vedení, identifikovala uzly zpracování OÚ a samotná zpracování OÚ. Také analyzovala datové toky a přinesla stručný popis procesů s nimi souvisejících. Popsala současnou bezpečnost společnosti, a to především s ohledem na data a nakonec podala návrhy a doporučení v podobě souhrnné zprávy.

DPIA využilo mnohých výstupů z GAP analýzy a navrhlo minimalizaci a pseudonymizaci některých zpracování. Ačkoli společnosti XYZ nevyplynula přímá povinnost mít DPO, byl podán návrh takovou osobu alespoň na částečný úvazek zajistit. Zbylá část DPIA – zpráva o DPIA – bude řešena v návrhové kapitole.

Analytická část tak poskytla dostatečné vstupní informace a již konkrétní analýzy, jejichž výstupy budou vhodně uplatněny nejen v návrhové části této práce, ale i v samotné společnosti, které poskytly praktické zmapování důležitých oblastí a identifikovaly dosud neřešené záležitosti.

3 VLASTNÍ NÁVRH ŘEŠENÍ

Vlastní návrh řešení obsahuje další z nejvýznamnějších oblastí této práce. V úvodu je návrh ochrany osobních dat v souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016 pojatý jako řízená změna postavena na princpiech Lewinova modelu, což pomohlo vyústit ve způsob verifikace. Po definici řízené změny následuje riziková politika řešící především analýzu rizik. Na to jsou navázány návrhy bezpečnostních opatření.

Kapitola Návrh synchronizace s GDPR zpřesňuje nezbytné oblasti pro uvedení v soulad. Podobný upřesňující význam má následující Řízení lidských zdrojů řešené podrobněji, protože zaměstnanci jsou z hlavních subjektů osobních údajů společnosti XYZ.

Nakonec je podán návrh plánu implementace zbylých činností nutných k realizaci včetně časového a ekonomické zhodnocení. Vlastní návrh řešení je ukončen závěrečným slovem zaměřeným na budoucnost společnosti XYZ, ale i slovem o informační bezpečnost obecně.

Protože diplomová práce řeší citlivé téma osobních údajů a informační bezpečnosti vůbec, společnost XYZ si nepřeje být identifikována, a navíc některé informace považuje za své vlastnictví, nebylo proto možné vše dostatečně popsat do potřebné hloubky.

3.1 Řízení změny

Uvedení společnosti XYZ do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016 je řízenou změnou. Její řízení je postaveno na principech Lewinova modelu řízené změny, který zodpovídá základní otázky týkající se nutnosti změny, nositele změny, definování intervenčních oblastí a samotné intervence a odkazuje též na důležitost závěrečného zhodnocení, a proto tento model řízené změny bude využit jako základní podkladový rámec pro další řešení v této práci.

3.1.1 Síly inicializující proces změny

Základní inicializující silou naší změny, kterou je navržení ochrany osobních dat dle obecného nařízení EU 2016/679 ze dne 27. dubna 2016 ve společnosti XYZ, je právě samotné nařízení, jež nabývá účinnosti 25. května 2018 a které je nutné dodržet z legislativních důvodů, jinak hrozí společnosti udělení správních pokut, které mají pro podobně drobné podniky likvidační charakter. Tudíž ze základního logického předpokladu, že společnost chce pokračovat ve své činnosti, je takřka z existenčních důvodů nezbytné, aby byla změna provedena.

Předchozí provedené analýzy potvrdily povinnost synchronizace s nařízením GDPR, stejně tak to potvrdil i současný nedostatečný stav bezpečnosti osobních údajů.

3.1.2 Identifikace agenta změny

Jako nositel této změny, tj. agent, vystupuje řešitel této diplomové práce a posléze jmenovaný DPO. Sponzory změny jsou majitel a projektový manažer. Z důvodu široké odbornosti, kterou řešená problematika vyžaduje, jsou v rámci celého procesu řešení změny problematické body konzultovány se specialisty – např. s právním poradcem se zaměřením na lidské zdroje, bezpečnostním konzultantem či mzdovou účetní.

Vzhledem k nutnosti zavedení změny, není očekáván odpor ze strany zaměstnanců. Přestože její zavedení přinese nové informace, procesy a školení, tj. vyšší zátěž, zaměstnanci jsou obeznámeni se situací, že nařízení se týká všech podobných společností, ve kterých by mohli nalézt uplatnění. Naopak v tomto pohledu může být zajímavá situace OSVČ, kteří povinnosti kolem zavedení nařízení mohou vzít už jako neunesitelné, spolu s dalšími činnostmi potřebnými pro jejich činnost, a rozhodnou se pro zaměstnanecký právní vztah, což způsobí společnosti XYZ možnou ztrátu partnera, jestliže nedojde k vzájemné dohodě o jiné formě právní spolupráce.

3.1.3 Identifikace intervenčních oblastí

Zásahy do ochrany osobních údajů se dotknou již zmiňované oblasti lidských zdrojů a dodavatelsko-odběratelského řetězce. Mimo to, že je pracováno s osobními údaji

zaměstnanců, dále právě zaměstnanci (programátoři) budou pracovat s osobními údaji prostřednictvím databází, ke kterým mnohdy potřebují ke své práci přístup kvůli operacím, které s nimi (či nad nimi) provádí. Z toho důvodu bude tato situace vyžadovat smluvní úpravy, vhodné nastavení procesů, bezpečnosti a provedení proškolení.

Dodatkové smluvní ošetření se dotkne i externích společností či OSVČ, kteří pro společnost XYZ provádějí práce spojené s přístupem k těmto osobním údajům. Z druhé strany pohledu to samé musí společnost XYZ poskytnout svým zákazníkům a spolupracujícím společnostem, tj. potvrdit svůj soulad s nařízením a smluvně se k němu zavázat.

Primárně je tedy nezbytné vyřešit oblast řízení lidských zdrojů a dodavatelsko-odběratelského řetězce a zabezpečit práci zaměstnanců s osobními údaji zákazníků klientů společnosti XYZ.

Pohled na působící síly: lehký odpor lze očekávat z řad zaměstnanců, kteří se budou muset přizpůsobit novým opatřením, popř. postupům. Ale jsou obeznámeni se situací, že nařízení je nezbytné splnit, a tak chápou nutnost změny. Naopak v tomto pohledu může být zajímavá výše zmiňovaná situace OSVČ, kteří povinnosti kolem zavedení nařízení mohou vzít už jako neunesitelné, spolu s dalšími činnostmi potřebnými pro jejich činnost, a rozhodnou se pro zaměstnanecký právní vztah, což způsobí společnosti XYZ možnou ztrátu partnera, jestliže nedojde k vzájemné dohodě o jiné formě právní spolupráce. Z pohledu sil podporujících projekt lze zmínit vedení společnosti, které chce dostát legislativním povinnostem, a také můžeme očekávat pozitivní přístup od klientů, kteří ocení přípravu a soulad s GDPR, stejně tak jako větší bezpečnost jejich osobních údajů.

3.1.4 Intervence

Při dodržení terminologie modelu řízené změny musíme v rámci změny vyřešit fáze rozmrazení, vlastní změny a zamrazení.

Rozmrazení se týká přípravných kroků zaměřených na analýzu společnosti a problematiky. První analytické kroky proběhly v rámci předchozí kapitoly, kde byla společnost XYZ popsána pomocí „7 S faktorů“, provedla se GAP analýza a DPIA, na což bude navazovat analýza rizik a návrh opatření dle normy ISO/IEC 27001 (příloha A)

a příručky vydanou organizací ENISA (jejíž oficiální anglický název je: „Guidelines for SMEs on the security of personal data processing“).

V rámci vlastní změny budou navržená opatření implementována. Aplikace bezpečnostních opatření bude vycházet z ISO/IEC 27002. O normy řady 27000 bude opřeno na základě výsledků analytické části, kdy zavedení ISMS je jedním z dobrých předpokladů souladu s GDPR. Primárním cílem však není plnohodnotná implementace ISMS, pouze návrh, který se zaměřuje na bezpečnost ochrany osobních údajů dle GDPR.

Dále obsahem vlastní změny budou činnosti, které vzešly z GAP analýzy, a jsou obsaženy v souhrnné zprávě o nálezech a doporučeních (viz kapitola 2.3.6), a DPIA:

- návrh ošetření současných smluv za odborné právní konzultace,
- návrh minimalizace zpracovávaných osobních údajů na základě odborných konzultací (především ve smlouvách),
- návrh pseudonymizace zpracovávaných osobních údajů,
- návrh vytvoření zpracovatelských smluv,
- u zpracování osobních údajů navrhnout doby zpracování, získání potřebných souhlasů, provést nezbytné informovanosti a zajistit řízení incidentů,
- návrh směrnic (řízení dokumentů, bezpečnostní politika práce na počítači, o serveru),
- návrh fyzického zabezpečení skříně na dokumenty a zabezpečení serveru.

Jelikož zaměstnanci jsou významným subjektem osobních údajů řešené společnosti bude jim věnována zvýšená pozornost v podobě náhledu na zpracování osobních údajů dle Stanoviska 2/2017 ke zpracování osobních údajů na pracovišti od WP29 a také návrhem školení zaměstnanců.

Fází zamrazení v tomto případě není žádná činnost, jedná se spíše o přístup a zavedení rutiny činností deklarovaných ve vlastních změně tak, aby požadavky pro splnění GDPR byly vskutku v praxi dodržovány, společnost se v této oblasti stabilizovala a docházelo k pravidelné kontrole celého procesu bezpečnosti ochrany osobních údajů včetně sledování nových rizik. Proto již před implementační fází je doporučeno jmenovat odpovědnou osobu za udržení kvalitního stavu bezpečnosti ochrany osobních údajů, dle GDPR označovanou jako DPO.

3.1.5 Verifikace dosažených výsledků

Jelikož naplnění dosažených výsledků u této změny uvedení společnosti XYZ do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016 nelze nikterak jednoduše kvantifikovat, protože například přímo neovlivní tržby firmy či produktivitu pracovníků, bude naplnění změny zkontrolováno dle splnění navržených činností, které jsou shrnuty v předchozí kapitole o intervenci, jelikož jejich splnění je předpokladem uvedení společnosti XYZ v soulad s GDPR. Je nezbytné dodat, že tak musí býti učiněno do 25. května 2018.

Návrh seznamu činností doporučených ke splnění pro uvedení společnosti XYZ do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016:

- analýza společnosti pomocí „7 S faktorů“,
- GAP analýza,
- DPIA,
- analýza rizik,
- návrh bezpečnostních opatření a jejich aplikace,
- návrh ošetření současných smluv za odborné právní konzultace,
- návrh minimalizace zpracovávaných osobních údajů na základě odborných konzultací (především ve smlouvách),
- návrh pseudonymizace zpracovávaných osobních údajů,
- návrh vytvoření zpracovatelských smluv,
- u zpracování osobních údajů navrhnout doby zpracování, získání potřebných souhlasů, provést nezbytné informovanosti a zajistit řízení incidentů,
- návrh směrnic (řízení dokumentů, bezpečnostní politika práce na počítači, o serveru),
- návrh fyzického zabezpečení skříně na dokumenty a zabezpečení serveru,
- upřesnění bezpečnosti OÚ zaměstnanců (dle WP29),
- školení zaměstnanců.

3.2 Riziková politika

Riziková politika zahrnuje identifikaci a ohodnocení aktiv včetně identifikace hrozeb a určení jejich pravděpodobností, na základě čehož je sestavena matice zranitelností a poté matice rizik. Nakonec jsou navržena bezpečnostní opatření včetně základních návrhů jejich aplikace.

Tato kapitola vyžadovala velkého zapojení vedení společnosti XYZ, aby obsah rizikové politiky měl co nejrelevantnější obsah. Také se využilo norem ISO/IEC řady 27000 a doporučení od ENISA se zachováním kontextu organizace.

Analýza rizik není vytvářena pro plnohodnotné nasazení ISMS. Jejím cílem je dosažení souladu s GDPR, k jehož dosažení využívá návrhy bezpečnostních opatření užívaných pro zavedení ISMS, jako efektivních nástrojů jeho naplnění. Téže je brán zřetel na budoucí vývoj společnosti XYZ, která vytvořené rizikové politiky může využít při snaze aplikace dalších bezpečnostních opatření, například za účelem implementace plnohodnotného ISMS.

3.2.1 Identifikace a ohodnocení aktiv

Pro ohodnocení identifikovaných aktiv byla sestavena hodnotící tabulka (viz níže), jejíž hodnotící škála se pohybuje od 1 do 5, přičemž ke každé hodnotě je definována míra rizika a jeho dopad. Hodnota identifikovaného aktiva se počítá pomocí součtového algoritmu: **(dostupnost + důvěrnost + integrita) / 3**.

Tabulka č. 1: Stanovení hodnocení aktiva
(Zdroj: Vlastní zpracování)

Míra rizika	Dopad rizika	Váha aktiva
bezvýznamné riziko	žádný dopad	1
akceptovatelné riziko	zanedbatelný dopad	2
nízké riziko	potíže a finanční ztráty	3
nežádoucí riziko	vážné potíže a velké ztráty	4
nepřijatelné riziko	existenční potíže	5

Aktiva byla identifikována v součinnosti s vedením společnosti XYZ, při identifikaci byl brán zřetel především na identifikaci takových aktiv, která souvisí s osobními údaji. U každého aktiva je pak uvedena hodnota dostupnosti, důvěrnosti a integrity (vždy v rozmezí 1–5) včetně výsledné hodnoty aktiva.

Tabulka č. 2: Identifikace a ohodnocení aktiv

(Zdroj: Vlastní zpracování)

Typ	Aktivum	Dostupnost	Důvěrnost	Integrita	Váha
Informace	1. Data o zaměstnancích	3	5	4	4
	2. Data o dodavatelích	3	4	4	4
	3. Data o klientech	3	5	4	4
	4. Data klientů	5	5	5	5
	5. Zálohy dat	5	5	5	5
Hardware	6. Server	5	5	5	5
	7. Stolní počítače	3	4	4	4
	8. Notebooky	5	4	4	4
	9. Mobilní telefony	5	3	2	3
	10. Router	4	4	3	4
SW	11. Operační systém	3	4	4	4
	12. Antivir	3	4	4	4
Služby	13. Elektronická pošta	3	4	5	4
	14. Webové stránky	3	2	2	2
	15. Internetové připojení	4	4	4	4

Do dat o zaměstnancích jsou zahrnuta i data o uchazečích o zaměstnání. Daty o dodavatelích jsou myšleny nejen zástupci dodavatelských společností (jejichž data se například objevují v seznamu kontaktů), ale též OSVČ.

Jako nerizikovější aktiva se jeví data klientů, zálohy dat a server. Daty klientů jsou myšleny data zákazníků klientů, nejtypičtějším příkladem jsou databáze uživatelů e-shopu, které obsahují velké množství subjektů (až v řádech tisíců).

3.2.2 Identifikace hrozeb a určení jejich pravděpodobností

Součinnosti vedení společnosti XYZ bylo využito i při identifikaci hrozeb, která vychází především z Přílohy C ISO/IEC normy 27005 a vodítka organizace ENISA (Guidelines for SMEs on the security of personal data processing). Finální identifikované hrozby jsou definovány a upraveny pro kontext řešené společnosti.

Pravděpodobnosti identifikovaných hrozeb byly stanoveny pomocí předem definované stupnice pro stanovení pravděpodobnosti hrozby – prezentované v tabulce níže.

Tabulka č. 3: Stanovení hodnocení hrozeb
(Zdroj: Vlastní zpracování)

Pravděpodobnost hrozby	Hodnota
Velmi nízká	1
Nízká	2
Střední	3
Vysoká	4
Velmi vysoká	5

Dle vodítka ENISA mohou hrozby působit ve čtyřech oblastech (síťové a technické zdroje, procesy/procedury spojené se zpracováním osobních dat, osoby/strany zapojené do zpracování osobních dat, sektor businessu a rozsah zpracování). Pro tyto oblasti byly identifikovány hrozby dle Přílohy C ISO/IEC normy 27005 a dle kontextu organizace.

Pravděpodobnosti hrozeb byly určeny za konzultace s majitelem společnosti XYZ.

Tabulka č. 4: Identifikace hrozeb a jejich pravděpodobností

(Zdroj: Vlastní zpracování)

Hrozba	Pravděpodobnost
1. Požár	1
2. Zničení zařízení	3
3. Neoprávněné vniknutí do kanceláře	5
4. Vzdálená špionáž	2
5. Krádež dokumentů	4
6. Krádež zařízení	4
7. Vyzrazení	2
8. Externí online útok	2
9. Únik dat	4
10. Bezpečnostní chyba SW/služby	3
11. Chybné fungování zařízení	3
12. Chybné fungování aplikačního programového vybavení	3
13. Chyba údržby	4
14. Neoprávněné použití zařízení	5
15. Poškození dat	4
16. Nezákonné zpracování dat	2
17. Chyba v používání	4
18. Zneužití oprávnění	2
19. Odepření činnosti	2

Jako nejvíce pravděpodobné hrozby vyšly takové hrozby, jež se vážou k fyzické bezpečnosti (vniknutí do kanceláře, krádež dokumentů, …), bezpečnostní politice

a k lidskému faktoru vůbec (neoprávněné použití zařízení, chyba údržby, chyba v používání, …).

3.2.3 Sestavení matice zranitelnosti a matice rizik

Při sestavování matice zranitelnosti je hodnota zranitelnosti (V) určena odborným odhadem (opět za konzultace s vedením společnosti XYZ a při braní zřetele na kontext organizace) s ohledem na váhu aktiva (A) a pravděpodobnost hrozby (T). Hodnotící škála je opět od 1 do 5, kde 1 je pro velmi nízkou zranitelnost, 3 pro střední zranitelnost a 5 pro kritickou zranitelnost.

Vzhledem k přehlednosti má matice zranitelnosti (stejně tak matice rizik dále v textu) zkrácený popis hrozeb, leč dostatečně vypovídající, nebude-li si však čtenář jist popisem, je možné si jej vyjasnit v předchozí tabulce s identifikovanými hrozbami a jejich pravděpodobnostmi.

Na informační aktiva je nahlíženo především z jejich samotné podstaty. Hrozby útočící na jejich nosiče (čímž jsou myšlena zařízení) či zpracovatele (software a služby) jsou brány v úvahu u aktiv hardwarových, softwarových a služeb. Proto například u aktiv typu data není řešena hrozba Zničení zařízení, což je vyznačeno číslicí nula (0), a tato hrozba je zohledněna u hardwarových aktiv (tedy zařízení), jako např. u stolního počítače.

Vzdálená špionáž, externí online útok, chyba údržby a chyba v používání jsou hrozby, které ohrožují všechna aktiva, tudíž by jim měla být věnována zvýšená pozornost, především při aplikaci opatření.

Tabulka č. 5: Matice zranitelnosti

(Zdroj: Vlastní zpracování)

Zranitelnost (V)		Aktivum	Data o zaměstnancích	Data o dodavatelích	Data o klientech	Data klientů	Zálohy dat	Server	Stolní počítače	Notebooky	Mobilní telefony	Router	Operační systém	Antivir	Elektronická pošta	Webové stránky	Internetové připojení
		A	4	4	4	5	5	5	4	4	3	4	4	4	4	2	4
Hrozba	T																
Požár	1		0	0	0	0	0	5	4	3	2	4	0	0	0	0	4
Zničení zařízení	3		0	0	0	0	0	4	3	3	2	3	0	0	0	0	0
Neopráv. vniknutí	5		0	0	0	0	0	5	4	4	2	4	0	0	0	0	0
Špionáž	2		3	2	3	4	4	3	2	2	1	3	3	2	2	1	3
Krádež dokumentů	4		4	3	3	0	0	0	0	0	0	0	0	0	0	0	0
Krádež zařízení	4		0	0	0	0	0	5	4	3	2	4	0	0	0	0	0
Vyzrazení	2		2	2	3	3	3	0	0	0	0	0	0	0	0	0	0
Online útok	2		3	2	3	4	4	4	3	3	2	3	4	3	3	2	3
Únik dat	4		4	4	4	5	5	0	0	0	0	0	0	0	0	0	0
Bezp.chyba SW / služby	3		0	0	0	0	0	0	0	0	0	0	4	4	4	3	4
Chybné fn. zařízení	3		0	0	0	0	0	4	4	4	3	3	0	0	0	0	0
Chybné fn. ap.p.vybav.	3		0	0	0	0	0	0	0	0	0	0	3	3	3	2	3
Chyba údržby	4		4	4	4	4	4	5	4	4	3	4	4	4	2	1	4
Neopráv. použití	5		0	0	0	0	0	5	5	5	3	4	0	0	0	0	0
Poškození dat	4		2	3	3	4	4	0	0	0	0	0	0	0	0	0	0
Nezákonné zpracování	2		3	4	4	5	5	0	0	0	0	0	0	0	0	0	0
Chyba v používání	4		4	3	3	4	4	5	4	4	3	4	4	4	2	1	3
Zneužití oprávnění	2		0	0	0	0	0	3	3	3	1	2	3	2	3	2	4
Odepření činnosti	2		0	0	0	0	0	3	2	2	1	3	4	2	2	1	3

Tabulka č. 6: Matice rizik

(Zdroj: Vlastní zpracování)

Míra rizika (R)		Aktivum	Data o zaměstnancích	Data o dodavatelích	Data o klientech	Data klientů	Zálohy dat	Server	Stolní počítače	Notebooky	Mobilní telefony	Router	Operační systém	Antivir	Elektronická pošta	Webové stránky	Internetové připojení
		A	4	4	4	5	5	5	4	4	3	4	4	4	4	2	4
Hrozba	T																
Požár	1		0	0	0	0	0	25	16	12	6	16	0	0	0	0	16
Zničení zařízení	3		0	0	0	0	0	60	36	36	18	36	0	0	0	0	0
Neopráv. vniknutí	5		0	0	0	0	0	125	80	80	30	80	0	0	0	0	0
Špionáž	2		24	16	24	40	40	30	16	16	6	24	24	16	16	4	24
Krádež dokumentů	4		64	48	48	0	0	0	0	0	0	0	0	0	0	0	0
Krádež zařízení	4		0	0	0	0	0	100	64	48	24	64	0	0	0	0	0
Vyzrazení	2		16	16	24	30	30	0	0	0	0	0	0	0	0	0	0
Online útok	2		24	16	24	40	40	40	24	24	12	24	32	24	24	8	24
Únik dat	4		64	64	64	100	100	0	0	0	0	0	0	0	0	0	0
Bezp.chyba SW / služby	3		0	0	0	0	0	0	0	0	0	0	48	48	48	18	48
Chybné fn. zařízení	3		0	0	0	0	0	60	48	48	27	36	0	0	0	0	0
Chybné fn. ap.p.vybav.	3		0	0	0	0	0	0	0	0	0	0	36	36	36	12	36
Chyba údržby	4		64	64	64	80	80	100	64	64	36	64	64	64	32	8	64
Neopráv. použití	5		0	0	0	0	0	125	100	100	45	80	0	0	0	0	0
Poškození dat	4		32	48	48	80	80	0	0	0	0	0	0	0	0	0	0
Nezákonné zpracování	2		24	32	32	50	50	0	0	0	0	0	0	0	0	0	0
Chyba v používání	4		64	48	48	80	80	100	64	64	36	64	64	64	32	8	48
Zneužití oprávnění	2		0	0	0	0	0	30	24	24	6	16	24	16	24	8	32
Odepření činnosti	2		0	0	0	0	0	30	16	16	6	24	32	16	16	4	24

Pro matici rizik se míra rizika (R) počítá jako součin váhy aktiva (A), pravděpodobnosti výskytu hrozby (T) a zranitelnosti (V). Tj. **R = A x T x V**.

Uvažuje se o nízké (0–49), střední (50–99; vyznačeno žlutě) a vysoké (100 a více; vyznačeno červeně) míře rizika.

Nejvyšší míry rizika se objevují ve spojitosti se serverem, u kterého hrozí neoprávněné vniknutí do kanceláře (momentálně je snadno přístupný a mohou z něho být nepozorovaně stáhnutá data, aniž by to někdo zaznamenal), samotná krádež zařízení, chyba údržby, neoprávněné použití zařízení a chyba používání. Další významnou hrozbou je únik dat (data klientů, záloha dat) a neoprávněné použití zařízení objevující se u stolního počítače a notebooku.

Rizika o vysoké míře by měla být odstraněna primárně, dále je třeba minimalizovat či odstranit rizika v úrovni střední míry. Provede se tak bezpečnostními opatřeními. Nízkou míru rizika je možné po zvážení akceptovat.

3.3 Návrh bezpečnostních opatření

Návrh bezpečnostních opatření vychází z Přílohy A normy ISO/IEC 27001, zjištěních rizik a požadavků GDPR. Návrhy aplikací bezpečnostních opatření čerpají z normy ISO/IEC 27002. Že je odkazováno na zmíněné normy ISO/IEC řady 27000 lze poznat z nadpisů následujících kapitol, které vycházejí z názvů oblastí těchto norem. Na zřetel je brán i fakt, že současným cílem není návrh implementace úplného ISMS, ale využití jeho přístupu pro uvedení společnosti XYZ do souladu s nařízením GDPR.

Z důvodů zachování anonymizace společnosti XYZ a jejich interních informací, jsou návrhy bezpečnostních opatření uvedeny jen v takové míře, jak jen je to možné.

Dále je navrhováno, aby implementaci navrhnutých bezpečnostních opatření zajišťovala osoba, jež bude zajišťovat udržování informační bezpečnosti a soulad s GDPR nadále i po implementaci tohoto inicializačního projektu (nejlépe jmenovaný DPO).

3.3.1 A.5 Politiky bezpečnosti informací

A.5.1.1 Politiky pro bezpečnost informací: vytvoření politik, které budou především řešit práci s informacemi, management dokumentů, bezpečnou práci na počítači (řízení přístupu, práce na dálku, ochrana před malwarem…), zálohování, kryptografická opatření a fyzickou bezpečnost. Veškeré politiky musí být schváleny vedením společnosti XYZ, které bude podporovat jejich dodržování.

A.5.1.2 Přezkoumání politik pro bezpečnost informací: je třeba jmenovat osobu povinnou za udržování GDPR (a nejlépe informační bezpečnosti vůbec) ve společnosti (nejlépe DPO). Ta v pravidelných oficiálně definovaných intervalech bude přezkoumávat politiky a dle potřeb je aktualizovat.

3.3.2 A.6 Organizace bezpečnosti informací

A.6.1.1 Role a odpovědnosti bezpečnosti informací: především u jednotlivých zaměstnanců je třeba jasně definovat jejich role a odpovědnosti za činnosti, které provádějí, a aktiva, se kterými pracují. S přidělením odpovědností by zaměstnancům měly být přiřazeny odpovídající pravomoci, jež jim pomohou dostát závazkům. Toto vše by mělo být zdokumentováno a respektováno.

A.6.1.2 Princip oddělení povinností: spočívá v zamezení užívání aktiv, oprávnění, apod. neoprávněnými osobami, aby především v případě společnosti XYZ nedocházelo k neúmyslným modifikacím.

A.6.1.5 Bezpečnost informací v řízení projektů: spolu s jasným definováním metodologie vedení projektů je třeba do řízení projektů implementovat napřímo i bezpečnost informací, tzv. by default a by design.

A.6.2.1 Politika mobilních zařízení: palčivým problém společnosti XYZ je nevyřešená práce na osobních noteboocích zaměstnanců, které tedy ani nezůstávají v prostorách kanceláře.

Je-li nezbytné, aby zaměstnanec (či spolupracující OSVČ) využíval mobilního zařízení (čímž je myšlen především notebook), je nutné aby:

- před začátkem samotné práce písemně potvrdil užívání vlastního mobilního zařízení a dalších povinností (dodržování bezpečnostních opatření, mlčenlivosti atd.),
- se definovaly požadavky na fyzickou bezpečnost (při přenosu, na veřejných místech…) – obezřetný přístup, dodržování pravidel, popř. fyzická ochrana bezpečnostním zámkem,
- došlo k oddělení účtu pro osobní a pracovní účely (řízení přístupu),
- byl hlídán instalovaný software, udržovaly se aktuální verze, především instalace oprav,
- byla zavedena ochrana před malwarem,
- aby se instaloval software pro možnost vzdálené deaktivace,
- a stanovily se intervaly pravidelných záloh.

V případě odcizení zařízení by měl zaměstnanec informovat svého zaměstnavatele, aby mohl učinit nezbytné kroky a minimalizovat dopady škod, kterým je nejlépe se vyhnout.

A.6.2.2 Práce na dálku: dalším neřešeným problémem společnosti XYZ je práce na dálku. Osoby využívající tohoto způsobu práce by měly být ošetřeny odlišnými politikami, než zaměstnanci „běžní“ pracující v kanceláři. Mělo by se jednat především o stanovení omezení týkajících se fyzické bezpečnosti místa práce (zabezpečení komunikace, ochrana před neoprávněným užitím zařízení…), vymezením povolené práce (například s jakým typem informací může daný zaměstnanec pracovat) a pracovní doby.

3.3.3 A.7 Bezpečnost lidských zdrojů

A.7.1.1 Prověřování: před smluvním uzavřením pracovního vztahu by měla být nastavena u žadatele prověrka. Ta by měla minimálně zahrnovat ověření totožnosti, životopisu, vzdělání a odborných znalostí. Jestliže pracovní pozice vyžaduje práci s obzvláště citlivými osobními údaji, měl by být vyžádán i výpis z trestního rejstříku.

A.7.1.2 Podmínky pracovního vztahu: u sepisování smluv by měl být brán zvýšený zřetel na vyčerpávající popis odpovědnosti, povinností, ale i pravomocí zaměstnance a zaměstnavatele. Již v této fázi musí být přijaty politiky společnosti a podepsána smlouva o mlčenlivosti. Smluvně by mělo být pokryto i duševní vlastnictví vzniklé práce

v rámci pracovní náplně pro společnost včetně potvrzení seznámení se s bezpečností politikou společnosti.

A.7.2.1 Odpovědnost vedení organizace: za relevantní rozdělení rolí a odpovědností odpovídá vedení organizace, které musí oficiálně plně podporovat veškeré bezpečnostní politiky a nejlépe motivovat zaměstnance v jejich dodržování, což souvisí i s podporou vzdělávání a školení v oblasti informační bezpečnosti.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací: je doporučeno ustanovit program vzdělávání o informační bezpečnosti, který bude pravidelně poskytovat různé formy vzdělávání s ohledem na jednotlivé role zaměstnanců. Odpovědnost za tento program by měla nést osoba zodpovědná za informační bezpečnost ve společnosti (nejlépe DPO).

A.7.2.3 Disciplinární řízení: v rámci společnosti XYZ by mělo formální definování disciplinárního řízení především působit jako preventivní nástroj odstrašující od případných přestupků či nabádající k důslednějšímu dodržování vyžadovaných kroků zamezujících vzniku narušení bezpečnosti informací. V případě potřeby zajistí disciplinární řízení předem definovaný a spravedlivý přístup.

A.7.2.3 Odpovědnosti při ukončení nebo změně pracovního vztahu: činnosti a odpovědnosti při ukončení pracovního vztahu by měly být zakotveny v pracovní smlouvě, popř. smlouvě o mlčenlivosti. Jedná se především o zachování mlčenlivostí v uvedených oblastech po určitou definovanou dobu i po době ukončení smluvního závazku. Mezi odpovědnostmi a činnostmi by mělo být též definováno, jakým způsobem budou vymazány data z používaných zařízeních (vč. osobních).

3.3.4 A.8 Řízení aktiv

A.8.1.1 Seznam aktiv: vytvoření seznamu aktiv včetně mapování jejich životního cyklu v rámci organizace (po definovaný čas do minulosti). Zodpovídá osoba zodpovědná za informační bezpečnost.

A.8.1.2 Vlastnictví aktiv: seznam aktiv doplnit o jeho vlastníka, který písemně potvrdí odpovědnost za jeho řádnou údržbu, jež může být dle daného aktiva blíže specifikována.

A.8.2.1 Klasifikace informací: pro kontext společnosti XYZ je důležité, aby u každého projektu byla provedena řádná klasifikace informací a byly definovány osobní údaje, které spadají pod ochranu fyzických subjektů definovaných dle GDPR. Především je nutné brát zvýšenou pozornost při práci pro lékařské kliniky apod., jejichž databáze obsahují dokonce citlivé osobní údaje.

3.3.5 A.9 Řízení přístupu

A.9.1.1 Politika řízení přístupu: řízení přístupu by mělo být hlídáno především u stolních počítačů a notebooků používaných k práci. Odpovědnost udržování bezpečného přístupu k zařízení by měla náležet vlastníku aktiva, který jej bude přezkoumávat a udržovat dle definovaných politik.

Je navrhováno, aby politiky pokryly i fyzickou oblast – čímž je myšlen řízený přístup do kanceláře a stanovení práv, rolí a odpovědností, co se týče přístupu k informacím v listinné podobě (lze například zakoupit bezpečnostní trezor).

A.9.2.1 Registrace a zrušení registrace uživatele: zaměstnancům je z důvodů pracovní činnosti zřizován přístup do budovy (přes kartu a heslo), a také přístupy do online webových aplikací sloužících pro komunikaci (*Paymo*, *Slack*, *Asana*). Je vhodné vést o uživatelích všech zmíněných platforem seznam a při ukončení pracovního vztahu jim co nejdříve tyto přístupy zrušit.

Jednotlivé projekty mohou vyžadovat specifické registrace. Ty by měly být v rámci dokumentace projektu zaznamenány a v případě ukončení prací na projektu tyto uživatelské účty zrušit.

A.9.2.6 Odebrání nebo úprava přístupových práv: toto opatření navazuje na předchozí o registraci a zrušení registrace uživatele. Ať již dojde k ukončení smluvního vztahu či k jeho změně, měla by přístupová práva být zrušena, v případě změny pak vytvořena nová. Jestliže odcházející spolupracovník zná obecnější přístupové hesla apod. (např. do databáze projektu), měla by být co nejdříve pozměněna.

A.9.4.1 Omezení přístupu k informacím: ve společnosti XYZ by toto opatření mělo mířit především na služby pro komunikaci a řízení projektů (*Slack*, *Asana*), v rámci kterých by uživatelé měli mít přístup jenom do nezbytných oblastí pro jejich práci. Totéž

platí i pro FTP přístupy, verzovací platformy atd. (záleží na typu projektu), kde by měla být též nastavena taková práva omezující přístup jenom do nezbytně nutných oblastí.

A.9.4.3 Systémy správy hesel: je třeba vytvořit a dodržovat systém správy hesel. Může tak být dosaženo prostřednictvím nějaké služby třetí strany pro správu hesel. Tak či onak je třeba zajistit, že hesla budou po prvním přihlášení měněna a též bude nastaven interval pravidelného měnění hesel. Jestliže hovoříme o heslech, myslí se tím hesla do programů a služeb nutných pro pracovní činnosti, které jsou v závislosti na proměnlivosti projektů též často se měnící. Proto by se systém správy hesel mohl zohledňovat i při řízení samotného projektu.

A.9.4.5 Řízení přístupu ke zdrojovým kódům programů: u zdrojových kódů uložených na FTP či verzovacích platformách je navrhováno monitorovat přístup včetně jeho omezení pouze na nezbytně nutné osoby. Jelikož je běžné, že zdrojové kódy jsou kvůli pracovním povinnostem ukládány na zařízení zaměstnanců, je nutné stanovit bezpečný postup zacházení se zdrojovými kódy, aby se také zabránilo neúmyslným modifikacím. S tím souvisí i přehled programů, které se zdrojovými kódy webových stránek a aplikacemi mohou pracovat, což minimalizuje neoprávněné přístupy jiných programů, které by takový přístup mít neměly.

3.3.6 A.10 Kryptografie

A.10.1.1 Politika použití kryptografických opatření: pro dosažení důvěrnosti, integrity a dostupnosti informací je doporučováno zavést politiky bezpečnosti informací za pomoci kryptografických opatření, které budou v rámci společnosti XYZ obecně vyžadovány (a dodržovány). Tyto politiky by měly především mířit na šifrování informací uložených na serveru v kanceláři a na šifrování disků, případně částí disků, které nesou informace nutné k zabezpečení zařízení užívaných k pracovním povinnostem.

3.3.7 A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1.1 Fyzický bezpečnostní perimetr: budova, ve které sídlí společnost XYZ je již chráněna správcem této budovy (ochrana vstupů na karty, hesla, recepce, kamerový

systém, detekční požární systém, hasící zařízení…). Zvýšený důraz by měl být aplikován na samotné prostory kanceláře společnosti XYZ, která je chráněna pouze zamykacími dveřmi. Jelikož je v kanceláři umístěna skříň s osobními údaji (zaměstnanců, dodavatelů, odběratelů), měla by být kancelář považována za prostor vyžadující vyšší bezpečnostní pozornost, na což navazují následující opatření.

A.11.1.2 Fyzické kontroly vstupu: je navrhováno, aby se zřídil bezpečnostní přístup i u dveří pro vstup do kanceláře. Bude tím zajištěn monitoring příchodů a odchodů, jasně se určí, kdo vše má přístup do kanceláře, což při současném stavu, kdy jsou dveře pouze na zámek, není možné. Během pracovní doby, kdy v kanceláři bude vždy alespoň jedna odpovědná osoba, může být monitoring přístupů zmírněn. Avšak v době nepřítomnosti odpovědné osoby či mimo pracovní dobu, by měl být monitoring nastaven na maximální úroveň a měl by sledovat veškeré příchody a odchody.

A.11.2.1 Umístění zařízení a jeho ochrana: řešené opatření by ve společnosti XYZ mělo především mířit na server a stolní počítače (majitele a projektového manažera). Zařízení by měla být fyzicky bezpečně upevněna takovým způsobem, aby nemohlo dojít k jejich odcizení, stejně tak by měly být fyzicky zabezpečeny vstupy, které zabrání neoprávněnému připojení k zařízení a případnému stažení a zneužití obsažených dat.

A.11.2.4 Údržba zařízení: u veškerých zařízení uvedených v seznamu aktiv by měla být pravidelně prováděna údržba, která bude dokumentována pro její doložení. Za údržbu odpovídá vlastník aktiva (zařízení) definovaný v rámci managementu aktiv. V případě odborné opravy či servisu je třeba zajistit autorizovaného a důvěryhodného odborníka, který se zaváže nezneužít přístupu k uchovávaným informacím a zajistí jejich bezpečnost v průběhu opravy či servisu.

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace: ačkoliv jsou zařízení užívaná pro vyhotovení práce společnosti XYZ v soukromém vlastnictví zaměstnance či OSVČ, měly by se dle již zmiňovaných politik zavázat k jejich dodržování. To se týká i fyzické bezpečnosti těchto zařízení, resp. aktiv vystupujících sice jako soukromé vlastnictví, ale používané jménem organizace. Zařízení by neměla být nechávána bez dozoru, především na veřejnosti. Zřetel by měl být brán i na ochranu zařízení, například před elektromagnetickým zářením, které by mohlo poškodit zařízení a tím pádem i uchovávané informace. Jako další vhodná opatření se jeví politika prázdného stolu a obrazovky monitoru (řešená v následujícím opatření v textu dále)

a zabezpečená komunikace. Rozhodně se vyhnout připojení přes nezabezpečené veřejné sítě.

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení: především s ohledem na možnost uložení osobních údajů a jiných neveřejných informací na paměťovém médiu zařízení je nutné zajistit bezpečnou likvidaci tohoto média. Likvidaci lze provést fyzicky, pomocí softwarového nástroje či oběma způsoby, leč je nutné zajistit, aby data uchovaná na paměťovém médiu nebylo možné obnovit. Podobné trvalé odstranění uchovávaných dat na paměťovém médiu je třeba provádět i při opakovaném používání zařízení.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru: listinné dokumenty, které obsahují především neveřejné informace a osobní údaje, by neměly být volně ponechávány v kanceláři, obzvláště je-li opuštěná. Je třeba dodržovat, že takové dokumenty budou uzamčeny ve skříni, k níž budou mít přístup pouze pověřené osoby. Nepoužívané stolní počítače či notebooky by neměly být opuštěny bez odhlášeného uživatele, jehož přihlášení je dostatečně zabezpečeno dle nastavených pravidel.

3.3.8 A.12 Bezpečnost provozu

A.12.1.1 Dokumentované provozní postupy: tyto postupy by měly především nového zaměstnance snáze uvést do fungování společnosti a seznámit jej s rutinními postupy. Popřípadě v případě kontroly přednést minimálně obecný přehled o provozním fungování společnosti XYZ. Pokyny by měly odkazovat na základní požadavky na konfiguraci systémů, práci s informacemi, hlášení neobvyklých jevů, především pak ty bezpečnostního charakteru. Dokumentace by měla obsahovat i kontakty různých podpor včetně popisu případů jejich použití.

A.12.3.1 Zálohování informací: zálohování informací by mělo být v souladu s ustanovenými politikami. O zálohách je navrhováno vést záznamy včetně postupů obnovy. Především by se měly provádět zálohy i na server umístěný mimo lokalitu kanceláře, pro případ rozsáhlejší havárie, kdy by server pro zálohování umístění v místě kanceláře postrádal význam, protože by byl zničen spolu s ostatními zařízeními. Jelikož zálohovací zařízení ponese osobní údaje a neveřejné informace, je třeba zajistit šifrování včetně pravidelných kontrol zařízení pro zajištění jeho správného chodu.

A.12.4.1 Zaznamenávání událostí formou logů: toto opatření je především doporučeno zavést u zálohovacího serveru pro větší zajištění dohledu nad prací se serverem. Dále je vhodné logovat přístupy k takovým databázím, které obsahují osobní údaje, což umožní lépe sledovat činnosti s danými daty.

3.3.9 A.13 Přenos informací

A.13.2.1 Politiky a postupy při přenosu informací: zaměstnanci by si měli být vědomi klasifikace informací a obzvláště nutnosti zvýšené pozornosti při manipulaci s osobními údaji, se kterými pracují, a které dále přeposílají kvůli komunikaci. Toto vše by měly pokrýt politiky pro přenos informací, které by měly obsáhnout i užívání pracovní e-mailové schránky a korespondence s ní spojenou. Jako například definování doby uchovávání a způsob likvidace zpráv.

V neposlední řadě je třeba určit postupy, díky kterým se minimalizuje prozrazení důvěrných informací.

3.3.10 A.14 Akvizice, vývoj a údržba systémů

A.14.2.1 Politika bezpečného vývoje: k zajištění bezpečnosti vyvíjených webových stránek a aplikací by měly existovat aktuální popsané standardy nutně dodržované bezpečnosti informací, které zasáhnou vývoj již od jeho samotného počátku. Politika by měla zahrnout požadavky na vývojové prostředí, úložiště a bezpečnost užívaných technologií, které lze například dosáhnout užíváním otestované doporučované nejnovější verze. Užívání nových technologií by se mělo udržovat kvůli bezpečnosti i v již existujících aplikacích (například přepsat kód z PHP 5.x na PHP 7.x).

Ovšem projekt od projektu se objevují nová a nová specifika, a proto by bezpečnost vývoje měla být zanesena do povinné součásti každého návrhu projektu, u kterého je třeba vysledovat zranitelná místa a odstranit je.

A.14.2.5 Principy budování bezpečných systémů: jelikož společnost XYZ plánuje do budoucna vytvářet vlastní CMS a platformu pro e-shop, bude vhodné implementovat bezpečnost do všech vrstev architektury, které budou pravidelně překontrolovány pro udržení aktuálnosti bezpečnostních principů.

A.14.2.6 Prostředí bezpečného vývoje: toto opatření by mělo vycházet z již stanovených politik, přičemž se vždy budou zohledňovat specifika projektů. Důležité je, že součástí bezpečného vývoje nejsou pouze technologie, ale také procesy a především lidé, resp. obzvláště vývojáři pracující ve vývojovém prostředí.

A.14.2.7 Outsourcovaný vývoj: zvýšený dohled s příchodem GDPR si vysloužíspolupracující společnosti a OSVČ. GDPR tento fakt řeší zpracovatelskými smlouvami, ale i přesto si může společnost XYZ vyžádat jistý způsob monitoringu a intervaly kontrol dodržování informačních bezpečnostních principů u zpracovatelů. Ostatně zodpovídá svým klientům za bezpečnost dat, které jí byly poskytnuty, tudíž je její povinností přenášet dodržování ochrany osobních údajů do dalších částí dodavatelsko-odběratelského řetězce.

3.3.11 A.15 Dodavatelské vztahy

A.15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy: politika by měla zahrnovat základní obecné požadavky na dodavatele (kterými jsou ve společnosti XYZ většinou OSVČ pracující jako programátoři) v oblasti bezpečnosti informací. Dále by měla tato politika nabádat společnost XYZ k vytvoření seznamu dodavatelů a vedení informací o nich (především co se týče již zjištěného zabezpečení), ale také o informacích, a hlavně o osobních údajích, ke kterým dodavatel v rámci vyhotovení své práce přistupuje.

U takovéto politiky bezpečnosti informací je navrhováno stanovit intervaly a způsoby monitoringu a kontroly dodavatelů, stejně tak aplikace těchto opatření do smluv, aby byla zajištěna jejich realizace.

A.15.1.2 Bezpečnostní požadavky v dohodách s dodavateli: jedním z hlavních bezpečnostních požadavků na dodavatele bude požadavek ze strany společnosti XYZ o prokázání souladu s GDPR, a to v tom případě, bude-li dodavatel při své práci přicházet do styku s osobními údaji, za které nese odpovědnost společnost XYZ. Tak či onak bude s dodavatelem (resp. dle terminologie GDPR zpracovatelem) uzavřena zpracovatelská smlouva, jež vše podstatné pokryje. Nejlépe se do zpracovatelské smlouvy přímo nadefinují bezpečnostní požadavky společnosti XYZ po zpracovateli, který svým podpisem potvrdí jejich splnění. I přesto by měly být v požadavcích zaneseny již řešené

možnosti kontroly a monitoringu ze strany společnosti XYZ, zda bezpečnostní požadavky jsou vskutku dodržovány.

3.3.12 A.16 Řízení incidentů bezpečnosti informací

A.16.1.1 Odpovědnosti a postupy: vytvoření odpovědností a postupů je v rukou managementu, jehož odpovědností je s nimi seznámit své zaměstnance. Postupy stanovují způsob monitoringu a sledování vzniku případných bezpečnostních incidentů. Vyhledávání možných zranitelných bezpečnostních míst.

Nezbytné je vytvoření postupů při hlášení bezpečnostních incidentů včetně podávání zpráv o nich, stejně tak postupů, jak na bezpečnostní incidenty reagovat.

Management by měl zajistit kompetentnost zaměstnanců popsané situace zvládat.

A.16.1.2 Hlášení událostí bezpečnosti informací: definování povinnosti hlášení bezpečnostní události, která náleží jak zaměstnancům, tak spolupracujícím osobám a společnostem. Hlášení by mělo proběhnout co nejrychleji a podávaná zpráva by měla mít předem definovanou strukturu s popisem bezpečnostní události, slabého místa apod., přičemž nahlašující osoba musí znát místo (resp. příjemce), kam (resp. kterému) bezpečnostní událost nahlásit.

A.16.1.4 Posouzení a rozhodnutí o událostech bezpečnosti informací: kontaktní místo, jenž obdrží hlášení o bezpečnostní události, má na starost dle předem stanovené stupnice hodnocení určit, zda se jedná o bezpečnostní událost či incident. Svá rozhodnutí dokumentuje.

A.16.1.5 Reakce na incidenty bezpečnosti informací: jestliže kontaktní místo označí bezpečnostní událost jako bezpečnostní incident, musí být nastaveny kroky reagující na situaci. Především by měl být co nejdříve kontaktován správce osobních údajů, jestliže došlo k jejich úniku, a to dle GDPR do 72 hodin. Řízení incidentu pokračuje nejlépe podle předem definovaných postupů, které se vypořádávají s bezpečnostním incidentem a zajišťují nápravu. Po vyřešení situace se celý incident zdokumentuje a provede se zpětná vazba sloužící jako ponaučení pro další řízení bezpečnostních incidentů.

A.16.1.7 Shromažďování důkazů: opatření existuje především z důvodů právních a disciplinárních řízení. Shromažďování je třeba zahájit co nejdříve, jelikož existuje vysoká pravděpodobnost, že se viník pokusí důkazy zničit. Pokud je již ze začátku u identifikované bezpečnostní události patrné, že jde proti současné právní legislativě, je vhodné událost řešit již od samého zárodku za součinnosti s policií.

Neméně důležité jsou definice postupů pro identifikaci, shromažďování, získávání a uchovávání důkazů.

3.3.13 A.18 Soulad s požadavky

A.18.1.1 Identifikace odpovídající legislativy a smluvních požadavků: odpovědnost vedení seznamu konkrétních zákonů, nařízení apod., které společnost XYZ musí dodržovat, náleží vedení organizace. Ta by měla zajistit i jejich aktuálnost a dodržování.

A.18.1.4 Soukromí a ochrana osobních údajů: toto opatření úzce souvisí s GDPR. Především by měla být určena osoba, která za ochranu osobních údajů bude zodpovídat, dle GDPR se jedná o DPO.

A.18.2.2 Shoda s bezpečnostními politikami a normami: dle předem stanovených kroků budou probíhat pravidelné kontroly shody reality s bezpečnostními politikami a normami. Pokud dojde k nesouladu, bude zajištěna náprava, přičemž platí pravidlo vše řádně zdokumentovat nejen pro interní potřeby organizace, ale i pro potřeby případných externích kontrol.

3.4 Návrh pro synchronizaci s GDPR

Kapitola shrnuje a upřesňuje činnosti navrhované pro synchronizaci s GDPR. V prvé řadě se řeší nápravy zpracování osobních údajů zjištěných v analytické části, poté se navrhuje provedení pseudonymizace u seznamu dovolených a elektronického kontaktního dokumentu, úprava smluv a jejich přepracování a vytvoření směrnic s konkrétním výpisem navrhovaných bezpečnostních opatření nutných k implementaci.

Nakonec se přibližuje návrh řešení fyzického zabezpečení skříně na dokumenty a serveru, sestavení zprávy DPIA a jmenování DPO.

3.4.1 Náprava vybraných zpracování OÚ

Z analytické části této diplomové práce vyplynuly návrhy k identifikovaným zpracováním OÚ, které mířily na doby zpracování, získání souhlasů, provedení informovanosti a řízení incidentů. Protože řízení incidentů je již zmíněno v kapitole 3.3.12 o řízení incidentů, nebude zde více řešeno.

Zpracování OÚ v rámci pracovní smlouvy, **zpracování OÚ v rámci dohody o provedení práce**, **zpracování OÚ v rámci potvrzení o studiu:** u těchto zpracování je nutné informovat zaměstnance o externím zpracování mzdovou účtárnou (prostřednictvím e-mailové zprávy vyžadující potvrzení, hromadnou schůzí s kontrolovanou účastí, jiným písemným dokumentem zajišťujícím podpisem informovanost zaměstnance). Za dobu zpracování je odpovědná externí mzdová účtárna, minimálně dle povinných zákonem určených lhůt.

Zpracování OÚ v rámci seznamu dovolených: získat písemný souhlas zaměstnanců s vedením tohoto seznamu, který bude zahrnovat i provedení informovanosti o fungování tohoto seznamu, čímž se myslí doba zpracování (která je stanovena na stáří záznamu o dovolené maximálně tři měsíce zpět od posledního dne její realizace) a samotné zapisování dovolených, které může provést nejen zaměstnanec (po oficiální dohodě s majitelem o dovolené), ale také majitel (taktéž po oficiální vzájemné dohodě). Lze očekávat, že souhlas nemusí být udělen. Jelikož takové neudělení nebude považováno jako neslučitelná věc pro výkon pracovních činností, dojde mezi zaměstnavatelem a zaměstnancem ke vzájemné individuální dohodě obou stran.

Zpracování OÚ v rámci facebookových stránek společnosti: i zde zajistit písemný souhlas zaměstnanců k uveřejňování jejich obrazového a zvukového záznamu či zmínění jejich jména a příjmení v příspěvku na oficiálních facebookových stránkách společnosti XYZ. Doba zpracování je určena na sedm let od zveřejnění záznamu, resp. příspěvku.

Zpracování OÚ v rámci smlouvy o díle, zpracování OÚ v rámci obchodní smlouvy: doba zpracování dle současné legislativy.

Zpracování OÚ v rámci elektronického kontaktního dokumentu: získat písemné souhlasy ke zpracování OÚ od osob uvedených v tomto seznamu. Souhlas by měl navíc obsahovat i informovaní o všech místech zpracování, ve kterých se osobní údaje budou

nacházet. Doba zpracování je určena na 2,5 roku (poté lze samozřejmě získat souhlas znovu, resp. jej obnovit, avšak nedojde-li k tomu, musí se dle definovaných politik a postupů ze všech míst řádně odstranit).

Zpracování OÚ v rámci webového kontaktního formuláře: ke kontaktnímu webovému formuláři musí být přidán checkbox (tj. zaškrtávací tlačítko), kterým odesílatel formuláře bude souhlasit se zpracováním osobních údajů v rámci e-mailové korespondence. Doba zpracování: jeden měsíc od přijetí každé nové zprávy (s každou zprávou v rámci komunikace bude zacházeno zvlášť).

Zpracování OÚ v rámci životopisů uchazečů: při poskytování pracovní nabídky přes pracovní portál či vlastní webové stránky přímo do inzerátu zahrnout, že reakcí na nabídku uchazeč o pozici souhlasí se zpracováním osobních údajů, které kvůli žádosti o pozici samovolně zasílá. Jestliže uchazeč pošle životopis přímo na e-mailovou adresu uvedenou na stránkách společnosti, je třeba mu prvotně zaslat pouze odpověď o souhlasu se zpracováním osobních údajů. Bez něho nikterak nereagovat a do týdne od obdržení zprávy ji odstranit, nepotvrdí-li uchazeč zpracování (o omezené týdenní lhůtě by měl být uchazeč v rámci prvotní e-mailové zprávy žádající o souhlas ke zpracování též informován). V obou případech (zasláním OÚ přes pracovní portál či webové stránky společnosti XYZ nebo přímým kontaktováním společnosti XYZ prostřednictvím e-mailové komunikace) by měl být uchazeč v souhlasu informován, že s e-mailovou korespondencí, poskytnutým životopisem a dalšími údaji důležitých pro výběrové řízení, přijde do styku majitel, projektový manažer a některý ze zaměstnanců kvůli odborné konzultaci. Dále musí být zmíněno, že některé tyto údaje mohou být vytisknuty. Doba zpracování: jeden měsíc od zaslání výsledku o přijetí/nepřijetí uchazeči, poté smazáno ze všech úložných míst a skartováno.

Kvůli skartování životopisů (ale i dalších listinných dokumentů obsahující osobní údaje) je doporučeno společnosti XYZ zakoupit skartovací zařízení.

3.4.2 Pseudonymizace zpracovávaných OÚ

U **zpracování OÚ v rámci seznamu dovolených** je navrhováno nepoužívat jméno a příjmení zaměstnance, pouze identifikační číslo, které bude v rámci seznamu dovolených každému zaměstnanci přiřazeno. Tudíž dostane-li se neoprávněná osoba k dokumentu, neměla by minimálně být schopna určit, k jakým osobám se dané zápisy dovolených vztahují. Způsob určení identifikačního čísla nebude z bezpečnostních důvodů zmiňován.

Zpracování OÚ v rámci elektronického kontaktního dokumentu vyžaduje podobný, leč složitější způsob pseudonymizace. Tentokrát budou existovat tři tabulkové seznamy. První z nich bude obsahovat identifikační číslo, jméno a příjmení a libovolné pole pro název společnosti. Druhý seznam obsáhne identifikační číslo a telefonní číslo a třetí seznam opět číselný identifikátor, ale tentokrát spolu s e-mailovou adresou. Opět by tyto tři seznamy měly být odděleny a pouze majitel společnosti XYZ a její projektový manažer by měli být schopni dát tyto seznamy dohromady.

Následující pomocné tabulky s testovými daty prezentují princip fungování pseudonymizace u elektronického kontaktního dokumentu.

Tabulka č. 7: První seznam el. kontaktního dokumentu
(Zdroj: Vlastní zpracování)

ID	Jméno, příjmení	Společnost (libovolné)
…	…	…
23	Jméno Příjmení	Název společnosti
…	…	…

Tabulka č. 8: Druhý seznam el. kontaktního dokumentu
(Zdroj: Vlastní zpracování)

ID	Telefonní číslo
…	…
23	+420 123 456 789
…	…

Tabulka č. 9: Třetí seznam el. kontaktního dokumentu

(Zdroj: Vlastní zpracování)

ID	E-mailová adresa
…	…
23	ukazka@emailoveadresy.cz
…	…

3.4.3 Smluvní ošetření

U vzoru smlouvy dohody o provedení práce byl identifikován nedostatek kvůli obsažení souhlasu ve smlouvě, a také zbytečnému množství osobních údajů (viz minimalizace zpracovávaných osobních údajů). Proto bylo navrženo vytvoření vzoru smlouvy nové. Protože úvazky na DPP nepřesahují částku 10 000 Kč, není nutné uvádět místo a datum narození, stejně tak číslo občanského průkazu (dle konzultací s externí mzdovou účtárnou).

Celkové přepracování je navrženo také u vzoru smlouvy o mlčenlivosti. Zde byl sice identifikován nežádoucí souhlas, ale analýza právních odborníků přinesla výstup doporučující vytvořit vzor smlouvy o mlčenlivosti nový.

Novou doposud neřešenou smlouvou je smlouva zpracovatelská, která bude sepsána se všemi spolupracujícími společnostmi a osobami v roli dodavatelů, resp. zpracovatelů, jak je definuje GDPR. Zpracovatelské smlouvy by měly vycházet ze stanovených politik a zahrnovat specifika, které se vztahují k pracovním činnostem jednotlivých zpracovatelů.

Návrh vzoru DPP a smlouvy o mlčenlivosti je přiložen v příloze. Kvůli jedinečnosti a interní bezpečnostní politice společnosti XYZ vzor zpracovatelské smlouvy nebyl dovolen ke zveřejnění.

3.4.4 Směrnice

Jedním z bodů, které byly v analytické části této práci doporučeny k vypracování pro dosažení shody s GDPR, bylo vytvoření směrnic, respektive zdokumentovat politiky

a postupy, které budou patřit mezi důkazy realizace daných bezpečnostních opatření, a které je samozřejmě třeba dodržovat.

Toto zdokumentování má mířit především na řízení dokumentů, bezpečnost práce na počítači a bezpečnou práci se serverem. Zmiňované oblasti byly již pokryty v rámci navrhovaných opatření, ale jelikož se jedná o klíčové činnosti k naplnění, aby došlo k synchronizaci s GDPR, je jejich návrh zavedení zdůrazněn i v této části. Konkrétně se jedná o návrh zavedení těchto bezpečnostních opatření:

- A.6.2.1 Politika mobilních zařízení,
- A.6.2.2 Práce na dálku,
- A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací,
- A.9.4.3 Systémy správy hesel,
- A.9.4.5 Řízení přístupu ke zdrojovým kódům programů,
- A.11.1.1 Fyzický bezpečnostní perimetr,
- A.11.2.1 Umístění zařízení a jeho ochrana,
- A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace,
- A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru,
- A.12.3.1 Zálohování informací,
- A.14.2.1 Politika bezpečného vývoje,
- A.14.2.7 Outsourcovaný vývoj,
- A.15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy,
- A.16 Řízení incidentů bezpečnosti informací,
- A.18 Soulad s požadavky.

Výše vypsané návrhy bezpečnostních opatření jsou bez odkladu navrhovány k implementaci před datem 25. 5. 2018, kdy musí být požadavky GDPR splněny. Zbylá nezmíněná opatření lze implementovat zpětně a společnost XYZ může postupem času usilovat o kompletní zavedení ISMS včetně jeho certifikace.

3.4.5 Fyzické zabezpečení skříně na dokumenty a zabezpečení serveru

Tato kapitola více rozebírá bezpečnostní opatření A.11.1.1 Fyzický bezpečnostní perimetr.

U skříně na dokumenty je navrhováno její fyzické připevnění ke stěně (např. hmoždinkami), aby se zamezilo její snadné manipulovatelnosti. To, že je skříň uzamykatelná, je již splněno. Pouze je třeba jasně definovat, kdo má přístup, respektive klíče do této skříně, a také co se stane, dojde-li ke ztrátě klíče apod. Dále je doporučováno kontrolovat obsah skříně v pravidelných intervalech.

Server, který je momentálně volně umístěn v kanceláři, by měl být nejlépe přesunut mimo prostory kanceláře, protože dojde-li k rozsáhlejším škodám v kanceláři (požár, vykradení), postrádá zálohování na serveru význam, je-li umístěn v kanceláři jako většina zařízení. Doporučeno je umístit server do společné serverovny v budově, která je řádně fyzicky zabezpečena a má kontrolovaný přístup. U serveru musí být také zakryty porty, aby se zamezilo neoprávněnému připojení. Přesto, co se týče zálohování a co by mělo řešit bezpečnostní opatření A.12.3.1 Zálohování informací, je zálohování informací úplně mimo budovu kanceláře společnosti XYZ.

3.4.6 Sestavení zprávy DPIA

V analytické části bylo po navrhovaných úpravách ve zpracováních osobních údajů navrženo, aby v návrhové části došlo k sestavení zprávy DPIA. Vzhledem k jejímu obsahu se jedná převážně o neveřejné informace, které si společnost XYZ nepřeje zveřejňovat, proto zde zpráva nemůže být blíže představena.

3.4.7 Jmenování DPO

Celou prací se proplétají doporučení pro zavedení pozice DPO. Tedy pověřence pro ochranu osobních údajů, který bude zajišťovat dodržování GDPR (a nejlépe celkové oblasti informační bezpečnosti) včetně školení a kontrol současného stavu a požadavků.

Pozici DPO je doporučeno vytvořit především kvůli plánům společnosti XYZ v blízké budoucnosti. Společnost XYZ plánuje vytvořit vlastní CMS a e-shop (resp. platformy), které bude nabízet zákazníkům. Nejspíš se dostane do situace, kdy se stane spolupracujícím správcem, čímž ponese spolu s klientem odpovědnost za zpracovávané osobní údaje, tudíž dojde k navýšení požadavkům na řízení osobních údajů, i když záleží na přerozdělení rolí mezi správci. Každopádně zatížení bude

rozhodně větší, než je tomu nyní, kdy společnost XYZ je vůči svým klientům pouze v roli zpracovatele.

DPO by měl být jmenován již před sestavováním zprávy DPIA a samotnými implementačními pracemi, u kterých by měl být přítomen.

Určitě by bylo přehnané mít ve společnosti XYZ pověřence na plný úvazek. Navíc společnost na další takový úvazek nemá finanční kapacity. Nabízí se proto dvě možnosti. Jmenovat na částečný úvazek stávajícího zaměstnance, který má dostatečný background o informační bezpečnosti a GDPR vůbec, čímž by se získala výhoda toho, že DPO by znal organizaci na velmi dobré úrovni. Anebo se zajistí externí specialista, který se pozice DPO chopí.

Tato diplomová práce se přiklání k první variantě, tedy k DPO z řad zaměstnanců, bude-li mít některý zaměstnanec s relevantními předpoklady zájem.

3.5 Řízení lidských zdrojů

Kapitola o řízení lidských zdrojů nahlíží blíže na zpracování osobních údajů na pracovišti, protože se zaměstnanci ukázali jako hlavní subjekty údajů pro společnost XYZ, která je v roli jejich správce.

Návrhy v jednotlivých oblastech vycházejí ze Stanoviska 2/2017 ke zpracování osobních údajů na pracovišti vydané WP29.

Závěrečná kapitola o školení zaměstnanců klade především důraz na prvotní školení o GDPR a zavedení pravidelných schůzek na toto téma, a to v režii jmenovaného DPO.

3.5.1 Zpracování během přijímacího řízení

Při náboru či v průběhu přijímacího řízení by se společnost XYZ měla zaměřit na zpracování jen těch osobních údajů nezbytných pro přijímací řízení. Rozhodně by neměla využívat osobních profilů na sociálních sítích, aby o kandidátovi zjistila více informací, a už vůbec by se neměla dostat do situace, kdy takto získané informace použije při výběrovém řízení.

3.5.2 Zpracování při prověřování v průběhu zaměstnání

I tato část se vztahuje k sociálním sítím, neboť se stávají silným (ale ne příliš vhodným) nástrojem pro sběr i těch nejcitlivějších osobních údajích o zaměstnancích. Proto ani v průběhu zaměstnaneckého poměru by vedení společnosti XYZ nemělo prověřovat své zaměstnance na jejich osobních sociálních profilech.

Výjimkou může být bývalý zaměstnanec, který podepsal dohodu o mlčenlivosti s platností i po ukončení pracovního vztahu, ve které se zavázal k mlčenlivosti v určitých oblastech a byl informován, že bude monitorován v rámci jeho veřejné komunikace (například na jeho profilu LinkedIn), zda mlčenlivost opravdu dodržuje.

3.5.3 Zpracování při dohledu nad užíváním informačních a komunikačních technologií

Jelikož většina zařízení, se kterými zaměstnanci společnosti XYZ pracují, jsou jejich soukromým majetkem, lze v tomto ohledu zvolit alternativní nemonitorovaný přístup, který se ohlíží na fakt této formy vlastnictví, a tudíž i na soukromé činnosti zaměstnanců, které nelze (nemůže) monitorovat.

Znemožnění monitoringu bude vykompenzováno vypracováním dostatečně podrobných politik o bezpečnosti práce na počítači, se kterými zaměstnanci musí souhlasit, aby mohli používat svá osobní zařízení, a ve kterých se zavážou je udržovat se svým nejlepším vědomím a svědomím (je rozdíl mezi únikem dat kvůli okradení a únikem dat kvůli nedbalosti při plnění svých povinností).

3.5.4 Monitorování domova a práce na dálku

Při možnosti práce na dálku či z domova nemohou být zajištěna všechna bezpečnostní opatření takovým způsobem, jako přímo na pracovišti. Navýšení tohoto rizika by společnost XYZ měla kompenzovat vhodnými technologiemi vybraných také dle posouzení jednotlivých zaměstnanců (jako důvěryhodnější se jeví stálý spolehlivý zaměstnanec pracující 2 či 3 dny do měsíce z domova než externí zaměstnanec permanentně pracující na dálku, například z důvodu častého cestování).

Na zařízení zaměstnance může být instalován software monitorující práci s myší a klávesnicí. Zavedení takového softwaru však musí být zaměstnancem odsouhlaseno, neboť to není rozhodně standardní způsob monitoringu zaměstnanců.

3.5.5 BYOD

Na soukromých noteboocích zaměstnanců budou striktně odděleny části pro soukromé a pracovní účely (nejlépe uživatelskými účty), kde do pracovních částí bude mít zaměstnavatel přístup, i co se týče případného monitoringu, protože jako zpracovatel svých klientů zodpovídá za jimi svěřené osobní údaje, nad jejichž zpracováním potřebuje mít dohled.

Detaily tohoto nastavení by měly zaštítit již řešené navrhované politiky.

3.5.6 Transparentnost a právní důvody

Požadavek na transparentnost o zpracování vychází ze samotného GDPR. Společnost XYZ musí informovat své zaměstnance o veškerých zpracováních jejich osobních údajů.

Ze samotného pracovního poměru zaměstnanec-zaměstnavatel vyplývají právní povinnosti ke zpracování osobních údajů zaměstnance zaměstnavatelem, ke kterým není potřeba souhlas zaměstnance, ba naopak by pracovní vztah neměl být založen na souhlasu, který je dle GDPR mj. odvolatelný, tudíž jeho odvoláním by zaměstnanec mohl bagatelizovat celou smlouvu, ve které byl uveden.

Většinu zpracování osobních údajů zaměstnanců zastřešuje společnost XYZ pod oprávněný zájem, kterým je zpracování v souvislosti se zaměstnáním (což lze dále rozkládat na mzdovou, personální agendu apod.).

3.5.7 Školení zaměstnanců

V rámci implementačního plánu navrhovaného v této diplomové práci by se určitě mělo objevit prvotní školení zaměstnanců, které obsáhne všechny podstatné informace o důvodu a příčinách řízení této změny, což bude primárně zahrnovat informace o GDPR, ale také musí být zmíněny přínosy.

Mezi přínosy lze určitě uvést standardizace postupů, které by měly urychlit a usnadnit zaměstnancům práci, zvýšení bezpečnosti (a to i zařízení, které používají zaměstnanci) a celkový posun organizace kupředu v rámci jejího vývoje, neboť při zpracovávání této práce se narazilo na mnohá místa, které nabízejí prostor k vylepšení, jež byla i navrhnuta, a budou-li návrhy realizovány, povznese se společnost XYZ zase o další úroveň výše.

Prvotního školení lze využít i k získání většiny souhlasů od zaměstnanců a provede se potřebná informovanost, a to takovým způsobem, že se sepíše listina obsahující strukturu školení a zaměstnanci jí podepíšou, čímž potvrdí, že byly o všem zmíněném informováni. Souhlasy se vyřeší zvlášť a jednotlivě, aby se odvoláním jednoho souhlasu nezrušily souhlasy ostatní.

Již toto školení by mělo býti v roli DPO, který seznámí zaměstnance se svojí rolí a odpovědnostmi. Dále definuje pravidelné schůzky týkající se informační bezpečnosti ve společnosti XYZ.

3.6 Navrhovaný plán implementace

K dovršení komplexnosti diplomové práce přináší tato kapitola návrh plánu implementace. V první části shrnuje závěry zjištěné při analýzách a zkoumání společnosti, které jsou důležité pro výběr podstatných činností pro uvedení společnosti XYZ do souladu s GDPR. Ty jsou pak prezentovány v druhé kapitole. Nakonec je představen návrh časového plánu implementace, jehož nejpozději možný termín ukončení je doporučen na 24. května 2018.

3.6.1 Zajištění splnění GDPR

Ačkoli by bylo nejvýhodnější, aby společnost XYZ implementovala plnohodnotné ISMS, není to v současné době v jejich silách (z pohledu volných pracovních sil i z finančních prostředků). Proto se tento návrh plánu implementace zaměřuje na ty nejnutnější činnosti a bezpečnostní opatření pro splnění podmínek GDPR, přičemž lze tento plán nazvat prvotním, neboť společnost může využít nyní neaplikovaných doporučení a bezpečnostních opatření v budoucnu, a to za cílem postupného zavedení celého ISMS a jeho certifikace.

V kapitole 3.1.5 Verifikace dosažených výsledků byly stanoveny kontrolní body potvrzující splnění podmínek GDPR:

- analýza společnosti pomocí „7 S faktorů“,
- GAP analýza,
- DPIA,
- analýza rizik,
- návrh bezpečnostních opatření a jejich aplikace,
- návrh ošetření současných smluv za odborné právní konzultace,
- návrh minimalizace zpracovávaných osobních údajů na základě odborných konzultací (především ve smlouvách),
- návrh pseudonymizace zpracovávaných osobních údajů,
- návrh vytvoření zpracovatelských smluv,
- u zpracování osobních údajů navrhnout doby zpracování, získání potřebných souhlasů, provést nezbytné informovanosti a zajistit řízení incidentů,
- návrh směrnic (řízení dokumentů, bezpečnostní politika práce na počítači, o serveru),
- návrh fyzického zabezpečení skříně na dokumenty a zabezpečení serveru,
- upřesnění bezpečnosti OÚ zaměstnanců (dle WP29),
- školení zaměstnanců.

Kapitola 3.4.4 Směrnice vymezila návrh na nejnutnější bezpečnostní opatření k aplikaci:

- A.6.2.1 Politika mobilních zařízení,
- A.6.2.2 Práce na dálku,
- A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací,
- A.9.4.3 Systémy správy hesel,
- A.9.4.5 Řízení přístupu ke zdrojovým kódům programů,
- A.11.1.1 Fyzický bezpečnostní perimetr,
- A.11.2.1 Umístění zařízení a jeho ochrana,
- A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace,
- A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru,
- A.12.3.1 Zálohování informací,

- A.14.2.1 Politika bezpečného vývoje,
- A.14.2.7 Outsourcovaný vývoj,
- A.15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy,
- A.16 Řízení incidentů bezpečnosti informací,
- A.18 Soulad s požadavky.

V rámci vypracování této diplomové práce byly splněny všechny verifikační body, pouze je nutné naplnit body o bezpečnostních opatřeních a směrnicích, a to aplikací vymezených bezpečnostních opatření vypsaných výše, které splní i fyzické zabezpečení skříně a serveru (viz A11.1.1 Fyzický bezpečnostní perimetr upřesněný v 3.4.5 Fyzické zabezpečení skříně na dokumenty a zabezpečení serveru).

Než se však společnost XYZ pustí do implementačního plánu, měla by mít již jmenovaného DPO, který se do něj zapojí a nejlépe jí bude řídit.

Implementační plán by měl být zakončen školením zaměstnanců.

3.6.2 Plán podle obsažených činností

Tabulka níže prezentuje závěrečnou podobu navrhovaných činností pro dokončení souladu s GDPR ve společnosti XYZ.

Tabulka č. 10: Obsahový plán navrhované implementace

(Zdroj: Vlastní zpracování)

Název	Doba pro zavedení (v hodinách)
A.6.2.1 Politika mobilních zařízení	7
A.6.2.2 Práce na dálku	4
A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací	5
A.9.4.3 Systémy správy hesel	4
A.9.4.5 Řízení přístupu ke zdrojovým kódům programů	3
A.11.1.1 Fyzický bezpečnostní perimetr	5
A.11.2.1 Umístění zařízení a jeho ochrana	2
A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace	2
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru	4
A.12.3.1 Zálohování informací	8
A.14.2.1 Politika bezpečného vývoje	5
A.14.2.7 Outsourcovaný vývoj	4
A.15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy	7
A.16 Řízení incidentů bezpečnosti informací	18
A.18 Soulad s požadavky	15
Školení zaměstnanců včetně příprav	8

Celkově si implementace vyžádá **101 hodin**. Doby zavedení byly stanoveny na základě odborných zkušeností konzultanta informační bezpečnosti.

3.6.3 Časový plán

Vedení společnosti XYZ vymezilo implementačním pracím maximálně 20 hodin pracovního týdne, s čímž musí časový plán počítat, mimo nevyhnutelné nejpozději možné datum ukončení implementace do 24. 5. 2018 včetně.

Navrhovaný časový plán prezentovaný tabulkou níže obsahuje sloupec „Název“ se zkrácenými popisy jednotlivých bezpečnostních opatření a školení. Další sloupce reprezentují jednotlivé týdny. Zelené buňky značí realizaci činnosti v daném týdnu a zapsaný text v zelené buňce dobu realizace (v hodinách).

Tabulka č. 11: Časový plán navrhované implementace
(Zdroj: Vlastní zpracování)

Název	1.týden	2.týden	3.týden	4.týden	5.týden	6.týden
A.6.2.1	7 h					
A.6.2.2	4 h					
A.7.2.2	5 h					
A.9.4.3	4 h					
A.9.4.5		3 h				
A.11.1.1		5 h				
A.11.2.1		2 h				
A.11.2.6		2 h				
A.11.2.9		4 h				
A.12.3.1		4 h	4 h			
A.14.2.1			5 h			
A.14.2.7			4 h			
A.15.1.1			7 h			
A.16				18 h		
A.18				2 h	13 h	
Školení					6 h	2 h

Poznámka k rozložení školení: 2 hodiny alokované do 6. týdne značí čas samotného školení (6 hodin v předchozím týdnu náleží přípravě na školení).

Časový plán navrhované implementace vychází na šest týdnů. Pro dostatečnou rezervu je navrhováno vytvořit časový polštář o minimální velikosti dvou týdnů, což

znamená, že projekt by měl být zahájen nejpozději osm týdnů před 25. 5. 2018. Implementátor by měl vzít v úvahu probíhající státní svátky, které realizaci projektu mohou mírně prodloužit a pozměnit.

3.7 Ekonomické zhodnocení návrhu implementace

Při klasickém rozdělení na náklady a výnosy můžeme v tomto případě kvantifikovat pouze náklady. Výnosy nelze vyčíslit. Návrh ochrany osobních dat v souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016 sice přinese standardizaci postupů a procesů, které urychlí a usnadní práci, také navýší informační bezpečnost, což zvedne i prestiž a důvěryhodnost společnosti XYZ v očích klientů a taktéž především dojde k souladu s povinným nařízením GDPR, avšak přínos v peněžních částkách nelze přímo určit.

Zato náklady navrhovaného plánu díky odborně určeným dobám trvání lze odhadnout mnohem blíže včetně dodatečně využitého materiálu.

3.7.1 Předpokládané náklady navrhovaného plánu

Jelikož časový plán navrhované implementace byl odhadnut na 101 hodin je nasnadě při hodinové sazbě 500 Kč určit celkovou částku nákladů: **50 500 Kč**.

Dále byly odhadnuty náklady na materiál pro upevnění skříně, serveru a počítačů včetně ochrany USB portů zmíněných zařízení na: **5 000 Kč**. Cena může kolísat na základě vybraných konkrétních produktů.

A jako poslední částka vystupuje vymezených **15 000 Kč** určených především na nákup softwarových služeb (pro správu hesel a šifrování).

3.7.2 Shrnutí

Celkové předpokládané náklady jsou **70 500 Kč**. Postavíme-li však tuto částku proti pokutám za nedodržení GDPR, které by byly pro společnost XYZ likvidační, měla by být taková částka pro vedení společnosti akceptovatelná.

U obou druhů nákladů se jedná o jednorázové náklady. Mnoho činností si budou žádat průběžnou kontrolu a aktualizace. Měly by být však součástí pracovních povinností stanoveného DPO, a proto se můžeme bavit o jeho měsíční mzdě jako o měsíčních nákladech. Jelikož hodinové měsíční požadavky na DPO budou od společnosti XYZ fluidní, nejlepším řešením bude placení DPO od hodiny. Při sazbě 500 Kč na hodinu a předpokládané potřebě 20 hodin měsíčně (u kterých byly zohledněny i finanční možnosti společnosti) lze tyto měsíční náklady vyčíslit na 10 000 Kč.

3.8 Výhled do budoucna závěrem

Protože doposud ve společnosti XYZ nebyla informační bezpečnost příliš řešena, musí vedení společnosti XYZ počítat s dalšími zásahy, které by navíc mělo samo iniciovat, minimálně plně podporovat DPO v jeho činnostech a návrzích. Tento důraz na budoucí vývoj v informační bezpečnosti je kladen především kvůli plánovaným (a již zmiňovaným) vlastním produktům – CMS, e-shop. Ty nejspíše postaví společnost do pozice spolupracujícího správce, a tím pádem bude kladen značnější tlak i na samotnou bezpečnost vůbec. Ale mimo tuto novou roli by se měla společnost XYZ chopit odpovědnosti aplikovat informační bezpečnost do svých produktů by design a by default.

Vytvoření GDPR je jedním ze znaků zvyšovaného důrazu na bezpečnost osobních údajů v celé společnosti, která si po několika bezpečnostních incidentech (například nedávný únik dat Facebooku z více jak 50 miliónů uživatelských profilů) začala postupně uvědomovat význam osobních údajů a jejich citlivost. Což dokazuje vyhotovení ePrivacy, které bude více mířit na ochranu osobních údajů fyzických osob. Proto by společnost XYZ měla svévolně přecházet k plnohodnotné implementaci ISMS dle norem ISO/IEC řady 27 000, která se již v této práci ukázala jako dobrou cestou (viz odkaz ve vodítku ENISA na tyto normy). Při aplikaci dalších bezpečnostních opatření může být využito zde zjištěných výstupů, nebudou-li prováděny s příliš velkým odstupem. Na co by se však v blízké budoucnosti měla společnost XYZ zaměřit, respektive její DPO, je adaptační zákon k GDPR. Ten se nepodaří uvést v účinnost do 25. 5. 2018, tudíž vyjde až po tomto datu. Každopádně se neočekávají přílišné úpravy oproti původnímu nařízení GDPR. Přesto je třeba sledovat aktuální dění, flexibilně reagovat a přizpůsobovat se okolním i vnitřním podmínkám organizace.

4 ZHODNOCENÍ A PŘÍNOSY PRÁCE

Hlavním cílem této práce bylo podat návrhy a doporučení pro uvedení vybrané společnosti do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016, což bylo splněno, a navíc byl navrhnut implementační plán obsahující navrhované činnosti nutné pro dosažení souladu s GDPR včetně upozornění na datové omezení k 25. květnu 2018, kdy implementace musí být dokončena.

V návrhové části byly řešeny i další navrhovaná bezpečnostní opatření dle norem řady ISO/IEC 27000 pro budoucí užití, která nejsou součástí navrhovaného implementačního plánu této diplomové práce. Bylo tak učiněno s ohledem na fakt, že společnost XYZ plánuje vlastní CMS a e-shop, které je nejspíš postaví do role spolupracujícího správce vyžadující větší zaměření na ochranu osobních údajů. Z téhož důvodu je navrhována pozice DPO, který bude především v budoucnu zastávat důležitou úlohu při ochraně osobních údajů, při programování a navrhování architektur těchto produktů. Prozatím bude DPO zastávat nezbytnou úlohu nejen v oblasti ochrany osobních údajů, ale také informační bezpečnosti vůbec, ovšem s ohledem na časové omezení, které si společnost XYZ kvůli finančním důvodům nemůže nyní dovolit překročit.

Na základě doporučení literatury a ENISA se k navrhování souladu s GDPR přistupovalo skrze návrh implementace norem řady 27000, tudíž společnost XYZ toho může v budoucnu využít a v tomto duchu pokračovat a směřovat k zavedení ISMS.

Přínosem práce je především zmapování společnosti XYZ z pohledu ochrany osobních údajů. Společnost je současně správcem pouze osobních údajů v rámci zaměstnaneckých vztahů a v rámci dodavatelsko-odběratelského řetězce. U všech zjištěných nesouladů zpracování OÚ byly navrženy a provedeny nápravy. A při splnění navrhovaného implementačního plánu s užitím navrhovaných bezpečnostních opatření a doporučení dojde společnost XYZ především k souladu s GDPR.

Dílčí cíl vyhotovení teoretického pozadí splňuje první kapitola, která vytvořila základní teoretický rámec k řešeným tématům. Provedly se i nezbytné analýzy, které blíže identifikovaly společnost a zanalyzovaly její současný stav především s ohledem na informační bezpečnost a zpracování osobních údajů. Nechybí ani nezbytná analýza rizik a samotný návrh vlastního řešení.

ZÁVĚR

Hlavní cíl této práce – podat návrhy a doporučení pro uvedení vybrané společnosti do souladu s obecným nařízením EU 2016/679 ze dne 27. dubna 2016 byl splněn.

Po sepsání základního teoretického pozadí byla vytvořena analytická a návrhová část. Kapitoly jsou vzájemně propojeny – analytická část doplňuje návrhovou, přičemž obě byly vytvořeny za úzké spolupráce s vedením řešené společnosti.

Byly navrženy nutné bezpečnostní opatření a také byly podány taková další doporučení, aby řešená společnost mohla dojít k synchronizaci s GDPR. Nad rámec těchto nezbytných kroků byl vytvořen i návrh implementačního plánu včetně ekonomického zhodnocení. Také byly navrženy bezpečnostní opatření vhodné k budoucí implementaci kvůli plánům, které má řešená společnost v blízké budoucnosti.

A proto lze závěrem říci, že tato diplomová práce dosáhla svých cílů a při dodržení jejich návrhů a doporučení může dostat vybraná společnost zákonným povinnostem a splnit požadavky GDPR.

SEZNAM POUŽITÉ LITERATURY

(1) GLEICK, James. *Informace: historie, teorie, záplava.* Praha: Dokořán, 2013. Zip (Argo: Dokořán). ISBN 978-80-7363-415-5.

(2) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(3) DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

(4) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

(5) *Evropský parlament* [online]. 2018 [cit. 2018-05-08]. Dostupné z: http://www.europarl.europa.eu/portal/cs

(6) NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

(7) HUDECOVÁ, Lucia, Lucie NECHVÁTALOVÁ a Štěpán VÝBORNÝ. *Ochrana soukromí versus svoboda projevu médií*. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6521-5.

(8) ENISA. *Guidelines for SMEs on the security of personal data processing* [online]. Heraklion: ENISA, 2017 [cit. 2018-05-09]. ISBN 978-92-9204-209-7. Dostupné z: DOI 10.2824/867415.

(9) Pseudonymizace osobních údajů. *GDPR.cz* [online]. Praha: Mgr. Eva Škorničková [cit. 2018-05-09]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/

(10) Stanovisko 2/2017 ke zpracování osobních údajů na pracovišti. In: *Úřad pro ochranu osobních údajů* [online]. Brusel: Pracovní skupina podle článku 29, 2017

[cit. 2018-05-09]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=28920

(11) ŠKUBAL, J. *Ochrana osobních údajů zaměstnanců ve světle GDPR* [seminář]. Brno: Hotel Avanti, 21.2.2018.

(12) Spoluautoři českého zákona o GDPR: Pro obce je důležitých 10 paragrafů, občanů se příliš nedotkne. *Ekonomický deník* [online]. 2018, 8.5.2018 [cit. 2018-05-09]. Dostupné z: http://ekonomicky-denik.cz/spoluautori-ceskeho-zakona-o-gdpr-pro-obce-je-dulezitych-10-paragrafu-obcanu-se-prilis-nedotkne/

(13) Tisková zpráva: Nařízení o ePrivacy jako doplněk k GDPR. *Úřad pro ochranu osobních údajů* [online]. Praha: Úřad pro ochranu osobních údajů, ©2013 [cit. 2018-05-09]. Dostupné z: https://www.uoou.cz/tiskova-zprava-narizeni-o-nbsp-eprivacy-jako-doplnek-k-nbsp-gdpr/d-27454/p1=1017

(14) IPTV a OTT: Sledování televize přes internet. *Kvalitní internet* [online]. Praha: EUROSIGNAL, ©2017 [cit. 2018-05-09]. Dostupné z: https://www.kvalitni-internet.cz/iptv-ott-sledovani-televize-pres-internet

(15) RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-80-214-3510-0.

(16) ISO/IEC 27000. *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. 5. vydání. Švýcarsko: Mezinárodní organizace pro normalizaci, 2018.

(17) ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(18) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(19) ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(20) ENISA. *Handbook on Security of Personal Data Processing* [online]. Heraklion: ENISA, 2018 [cit. 2018-05-10]. ISBN 978-92-9204-251-6. Dostupné z: DOI 10.2824/569768.

(21) KUBÍČKOVÁ, Lea a Karel RAIS. *Řízení změn ve firmách a jiných organizacích*. Praha: Grada, 2012. Expert (Grada). ISBN 978-80-247-4564-0.

(22) GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. Brno: Computer Press, 2010. ISBN 978-80-251-2621-9.

(23) KOCH, Miloš a Bernard NEUWIRTH. *Datové a funkční modelování*. Vyd. 4., rozš. Brno: Akademické nakladatelství CERM, 2010. ISBN 978-80-214-4125-5.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM DIAGRAMŮ

SEZNAM ZKRATEK

DPIA	Data Protection Impact Assessment (překládáno jako Posouzení vlivu na ochranu osobních údajů)
GDPR	General Data Protection Regulation (překládáno jako Obecné nařízení o ochraně osobních údajů)
CMS	Content Management System (překládáno jako Systém pro správu obsahu)
HPP	Hlavní pracovní poměr
OSVČ	Osoba samostatně výdělečně činná
HR	Human Resources (překládáno jako Lidské zdroje)
OÚ	Osobní údaje
DPP	Dohoda o provedení práce
PHP	Rekurzivní zkratka pro „PHP: Hypertext Preprocessor“ (překládána jako „PHP: Hypertextový preprocesor“)
FB	Facebook
OS	Operační systém
VLAN	Virtual Local Area Network (překládáno jako Virtuální místní počítačová síť)
MAC	Media Access Control (překládáno jako Řízení přístupu na médiu)
ISMS	Information Security Management System (překládáno jako Systém řízení bezpečnosti informací)
ISO/IEC	The International Organization for Standardization and the International Electrotechnical Commission (překládáno jako Mezinárodní organizace pro standardizaci a Mezinárodní elektrotechnická komise)
ENISA	European Union Agency For Network and Information Security (překládáno jako Evropská agentura pro bezpečnost sítí a informací)

DPO	Data Protection Officer (překládáno jako Pověřenec pro ochranu osobních údajů)
EU	Evropská unie
SMEs	Small and Medium-sized Enterprises (překládáno jako Malé a střední podniky)
WP29	Article 29 Working Party (překládáno jako Pracovní skupina podle článku 29)
SW	Software
FTP	File Transfer Protocol (překládáno jako Protokol pro přenos souborů)
ID	Identifikátor
BYOD	Bring Your Own Device (překládáno jako Přines si své vlastní zařízení)
ÚOOÚ	Úřad pro ochranu osobních údajů
OTT	Over the Top
ČR	Česká republika
DFD	Data Flow Diagram (překládáno jako Diagram toku dat)

SEZNAM PŘÍLOH