VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta podnikatelská

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Šimon Vicen

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

ZAVEDENÍ STANDARDU ISO 27701 DO FIRMY VYUŽITÍM GAP ANALÝZY

IMPLEMENTATION OF STANDARD ISO 27701 IN THE COMPANY USING GAP ANALYSIS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Šimon Vicen

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Šimon Vicen**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

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:

Zavedení standardu ISO 27701 do firmy využitím Gap analýzy

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem této práce je analyzovat stav systému pro implementování rozšiřujícího standardu ISO 27701: 2019 v konkrétní společnosti. Tahle společnost tímto standardem rozšiřuje již zavedený standard ISO 27001. V práci je hodnoceno kontrolní prostředí předepsaném požadavků normy ISO 27701: 2019. Přínosem této práce je vyhodnocení analýzy, které vyplývají ze zavedení doporučeného standardu k řešení zvýšeného množství bezpečnostních hrozeb a ochraně bezpečnostních informací.

Základní literární prameny:

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

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

ABSTRAKT

Táto práca se zaoberá analýzou stavu systému pre implementáciu rozširujúceho štandardu ISO 27701:2019 v konkrétnej spoločnosti. Spoločnosť týmto štandardom nadväzuje na už zavedený štandard ISO 27001. V práci je hodnotené kontrolné prostredie obsahujúce požiadavky normy ISO 27701:2019. Teoretická časť práce obsahuje poznatky z oblasti bezpečnosti informácii, popisuje sadu noriem ISO 27000 a taktiež popisuje európske a české právne akty vzťahujúce sa na bezpečnosť informácii. V ďalšej časti je vypracovaná analýza spoločnosti s následným aplikovaním opatrení pri zavedení rozširujúceho štandardu ISO 27701. Prínosom tejto práce je vyhodnotenie analýzy, ktorá vyplýva zo zavedenia doporučeného štandardu k riešeniu zvýšeného množstva bezpečnostných hrozieb a ochrane bezpečností informácii.

KĽÚČOVÉ SLOVÁ

GDPR, ISMS, bezpečnosť informácii, PDCA cyklus, ISO 27701, ISO 27001, Gap analýza, kybernetiká bezpečnosť

ABSTRACT

This thesis analysis current state of the system for implementation of standard ISO 27701: 2019 extension. This standard extends already established standard ISO 27001. The thesis evaluates set of controls to the requirements of standard ISO 27701: 2019. Theoretical part contains information regarding the information security, describes a set of ISO 27000 standards as well as European and Czech legal acts related to information security. Following analysis of the company is performed with the application of security measures while implementing the extension standard ISO 27701. Contribution of this thesis is evaluation of the analysis which results from implementation of recommended standard to address the increased number of security threats and the protection of security information.

KEYWORDS

GDPR, ISMS, information security, PDCA cycle, ISO 27701, ISO 27001, Gap analysis, cyber security

VICEN, Šimon. *Implementation of standard ISO 27701 in the company using Gap analysis*. Brno, , 79 s. Diplomová práca. Vysoké učení technické v Brně, Faculty of Business and Management, Ústav informatiky. Vedúci práce: prof. Ing. Petr Sedlák, CSc.

VYHLÁSENIE

Vyhlasujem, že svoju diplomovú prácu na tému „Implementation of standard ISO 27701 in the company using Gap analysis“ som vypracoval samostatne pod vedením vedúceho diplomovej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som poďakoval vedúcemu diplomovej práce pánovi Ing. Petrovi Sedlákovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Obsah

Zoznam obrázkov

Úvod

V posledných rokoch je zaznamenávaný rapídne stúpajúci sa trend počtu kybernetických útokov po celom svete. Vzhľadom na to, že každá z firiem dennodenne spracováva, zhromažďuje, uchováva, či iným spôsobom narába s osobnými údajmi a citlivými dátami, zvyšuje sa nebezpečenstvo poškodenia, odcudzenia informácii, či iného zásahu do vnútornej integrity firmy. Prirodzenou reakciou menších, väčších spoločností a organizácií je zvýšenie prítomnosti množstva bezpečnostných prvkov voči narastajúcim hrozbám na zaistenie bezpečnostného prostredia pre svoje dáta a informácie.

Snaha firiem o dosiahnutie komplexného riadenia IT bezpečnosti však zlyháva na vybudovaní štruktúrovaných postupov, ako tento cieľ dosiahnuť. Spoločnosti inklinujú k zabezpečovaniu jednotlivých oblastí pomocou technologických opatrení, ale vo väčšine prípadov bez vopred prepracovanej stratégie. Dochádza tak často k množstvu bezpečnostných nedostatkov a zachytení iba časti ohrozujúcich útokov.

Hlavným prínosom tejto práce je vytvoriť určitú metodiku, resp. návod na to, ako si túto stratégiu bezpečnosti informácií vytvoriť. Je cielená prioritne pre Firmu XY, ale je využiteľná pre rôzne iné menšie či väčšie firmy a zdôrazňuje, aké je dôležité, aby firmy túto stratégiu mali integrovanú. Referenčným modelom, ktorým by sa stratégia mala dosiahnuť, je štandard ISO/IEC 27701. Tento referenčný model je celkom nový štandard, vydaný v auguste 2019, teda nie je veľa spoločností, ktoré ho už implementovali do svojich štruktúr. Štandard je však veľmi dôležitou nadstavbou známeho štandardu pre systém riadenia informačnej bezpečnosti ISO/IEC 27001 a robí bezpečnosť štruktúru bezpečnosti informácii úplnou. Z tohto dôvodu je nutné mať ISO/IEC 27001 už zavedený v čase procesu tejto implementácie.

1 Ciele práce, metódy a postupy spracovania

Cieľom tejto práce je analyzovať súčasný stav systému riadenia bezpečnosti informácií pre implementovanie rozširujúceho štandardu ISO/IEC 27701: 2019 v zvolenej konkrétnej spoločnosti a následne vytvoriť plán pre implementáciu konkrétnych bezpečnostných opatrení pre Firmu XY.

Na to, aby bolo možné dosiahnuť stanovené ciele práce, je v prvom rade nutné oboznámiť sa s konceptom a poznatkami v oblasti bezpečnosti informácií. Dôraz je kladený najmä na systém riadenia bezpečnosti informácií, známy ako ISMS, na ktorý štandard ISO/IEC 27701 nadväzuje. V práci sú priblížené inštitúcie zaoberajúce sa bezpečnosťou informácií, rada noriem ISO/IEC 27000, s menovaním najznámejších štandardov z tejto rady. Zmapovaná je aj legislatíva, vyhlášky a zákony vzťahujúce sa k tejto téme, a to z pohľadu európskych a českých právnych aktov, keďže je dôležité aby ich spoločnosť rešpektovala, tak ako sa nimi riadila.

Proces vedúci k zmene analyzovaného súčasného stavu do stavu požadovaného je obsiahnutý v sekcii Implementácia nadväzujúceho štandardu ISO/IEC 27701. Následne sú popísané nástroje využité na riadenie bezpečnosti informácií, medzi ktoré patrí Gap analýza a Analýza dopadu.

Výstupom práce je na vybranej firme demonštrovať porovnanie aktuálneho stavu zabezpečenia informácií s požiadavkami ISO/IEC 27701 a v ďalšej časti navrhnúť odporúčania pre opatrenia, ktorým treba venovať zvýšenú pozornosť, aby spoločnosť mohla efektívne chrániť svoje dáta a informácie.

2 Teoretické východiská práce

2.1 Systém riadenia bezpečnosti informácií

Je treba si uvedomiť, že každá zo spoločností, firiem či organizácií v rámci procesov svojho fungovania skôr či neskôr príde do kontaktu so značným množstvom informácií, ktoré zhromažďuje a spracúva. Tieto informácie sú nevyhnutnými aktívami pri dosiahnutí vytýčených cieľov. Ohrozenie týchto informácií, či už cieleným útokom, dôsledkom prírodných vplyvov alebo chybou v systéme, dochádza k narušeniu integrity, dostupnosti a dôvernosti informácií a toto riziko, môže mať signifikantný dopad na správny chod organizácie.

Vhodným riešením vytvorenia organizovanej bezpečnostnej politiky, efektívneho stanovenia svojich plánovaných cieľov, tak ako docielenia súladu so zákonnými nariadeniami je zavedenie systému, ktorý sa zaoberá riadením informácií.

Systém riadenia informácií zavádza rodina štandardov ISO/IEC 27000 tzv. ISMS alebo Systém riadenia bezpečnosti informácii. Viac o jednotlivých štandardoch spadajúcich do rodiny štandardov budem hovoriť v nasledujúcich častiach tejto práce. Správnym nastavením ISMS, monitorovaním, vylepšovaním zvolených opatrení a vytváraním nových v reakcii na identifikáciu vzniknutých potenciálnych rizík je možno dosiahnuť efektívnej ochrany dát a informácií.

2.2 ISMS

ISMS je možno definovať ako systematický postup pozostávajúci z procesov, technológií a nástrojov, ktorý slúži ako ochrana firemných dát a informácií a ich spracovanie pomocou efektívneho risk manažmentu. Je to dokumentovaný systém riadenia informácií bezpečnosti, ktorý je aplikovaný vyčlenenej oblasti organizácie.

ISMS je založené na princípe využitia PDCA tzv. Demingovho modelu a skladá sa zo štyroch etáp:

1. **Ustanovenie ISMS** - určenie rozsahu a zodpovedností
2. **Zavedenie a správa ISMS** - výber bezpečnostných opatrení
3. **Monitorovanie ISMS** - spätná väzba a hodnotenie zavedenia
4. **Zlepšovanie a údržba** - odstraňovanie chýb a nedostatkov

Zameriava sa na tri kľúčové aspekty:

- Dôvernosť: informácia nie je prístupná oprávneným procesom, skupinám alebo ľuďom.
- Integrita: informácia je neporušená a presná, chránená pred poškodením.
- Dostupnosť: informácia je k dispozícii, použiteľná pre užívateľov s oprávneným prístupom

[1]

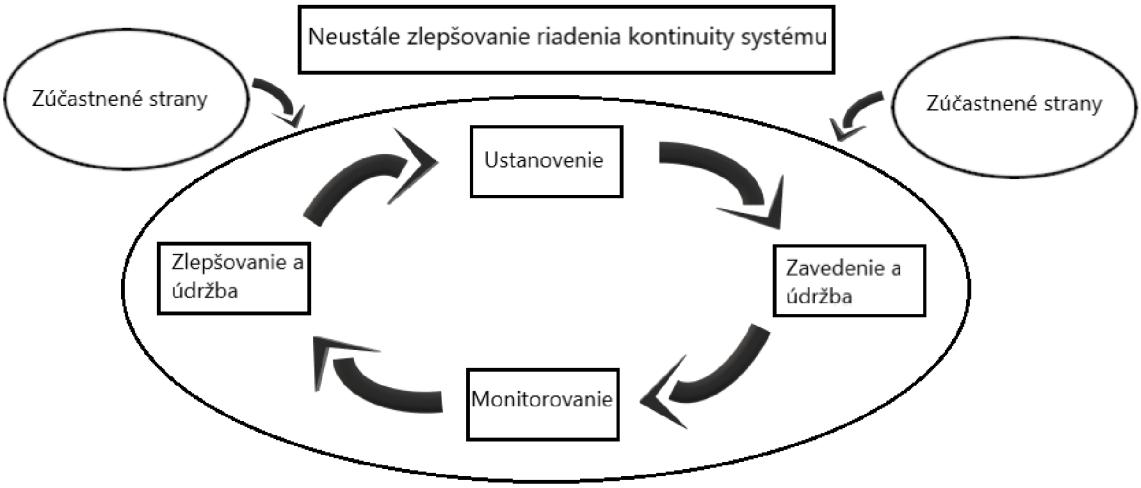
2.2.1 Plán pracovného postupu - PDCA-Demingov cyklus

Jedná sa o metódu postupného zlepšovania napr. aplikácii, služieb, procesov, či kvality výrobkov a dát. Z obecného modelu Demingového cyklu vychádza aj český zákon o kybernetickej bezpečnosti, ktorý riadi štruktúru, definuje ciele a zámery a riadi procesnú integráciu. Tomuto zákonu sa práca bude venovať v ďalších kapitolách v rámci tejto práce (viď 2.5.3). Demingov cyklus prebieha formou opakovania štyroch základných činností:

1. **Plan** - plánovanie dopredu premysleného zlepšenia.
2. **Do** - realizácia plánovania.
3. **Check** - overenie výsledkov realizácie voči pôvodnému plánu
4. **Act** - dodatočné úpravy vlastného prevedenia a plánovania a jej plošná implementácia zlepšenia do praxe.

Plan - Plánuj

Prvá fáza, je fáza plánovania. Pred tým ako je vykonaná zmena, zavedené zlepšenie, musí byť situácia v organizácii analyzovaná. Prvoradé je problém pochopiť a rozumieť jeho podstate.



Obr. 2.1: PDCA-Demingov cyklus, spracovanie: autor textu

Plánovanie prebieha v jednotlivých oblastiach:

- Definovať plán cieľov zlepšenia
- Definovať spôsob plánovanej zmeny
- Definovať vplyvy plánovanej zmeny
- V akej miere prebieha zlepšenie a následné meranie
- Určenie termínov zavedenia zlepšenia

V prípade zavedenia ISMS sa vo fáze "Plan" postupuje nasledovne:

- Definovanie oblasti pôsobnosti ISMS
- Definovanie systematického postupu pri ohodnotení rizík
- Definovanie politiky informačnej bezpečnosti
- Vypracovanie procedúr hodnotenia rizík a následná realizácia
- Definovanie cieľa bezpečnosti informácií v danej oblasti
- Vystavenie prehlásenia o aplikovateľnosti vybraných opatrení
- Výber implementovaných cieľov a opatrení
- Analýza a vyhodnotenie spôsobov ako zvládať zhodnotenie rizík

Do - Urob

Fáza "Do" predstavuje koncept samotnej implementácie. Napája sa na proces zlepšenia po jeho naplánovaní. Dôležitý aspekt, ktorý je nutné brať do úvahy je ľudský faktor.

V prípade zavedenia ISMS sa vo fáze "Do" postupuje nasledovne:

- Vypracovanie dokumentácie plánu zvládania rizík - definovanie procedúr a procesov v roli bezpečnostných opatrení, tak ako podrobnú bezpečnostnú politiku
- Realizácia opatrení umožňujúcich detekciu a riešenie bezpečnostných incidentov
- Implementácia opatrení určených v rámci riešenia bezpečnostných rizík
- Vypracovanie programu systematickej výchovy k bezpečnostnému povedomiu a zaškolenie relevantných pracovníkov
- Zaobstaranie dostatočných zdrojov pre vykonanie činností ISMS

Check - Kontroluj

V tejto fáze sa uskutočňuje kontrola a porovnanie dosiahnutých výsledkov s plánovanými. Hodnotená je efektivita zlepšenia. Kontrolná fáza zahŕňa činnosti, medzi ktoré patrí meranie, kontrola, analýza získaných dát a na záver hodnotenie.

V prípade zavedenia ISMS sa vo fáze "Check" postupuje nasledovne:

- Testovanie, monitorovanie ohodnotenie činnosti riadenia ISMS
- Ohodnotenie výsledkov, zhromažďovanie a vytváranie dôkazov
- Generovanie správ, ktoré manažment má za úlohu analyzovať
- Meranie a posúdenie účinnosti systému riadenia a zavedených opatrení voči bezpečnostnej politike

Act - Vykonaj

Na základe výsledkov analýzy z predchádzajúcej fázy sa vykonajú jednotlivé činnosti. V prípade, že dôjde k zlyhaniu a nesplnenia stanovených cieľov, proces sa vráti o fázu späť, alebo až na začiatok k plánovaniu, kde je nutné vyhľadať príčinu zlyhania. Ak sa podarí chybu napraviť následným procesom je štandardizácia zmeny.

V prípade zavedenia ISMS sa vo fáze "Act" postupuje nasledovne:

- Revízia, vykonanie úprav a zmien na základe analýzy od manažmentu
- Identifikácia, realizácia, aplikovanie, dokumentácia zlepšení ISMS

PDCA cyklus je možné využiť vo viacerých oblastiach:

- výroba
- manažment (i funkčné manažmenty)
- procesy
- logistika
- vývoj softvéru
- všade tam, kde je zlepšenie.

[2][3]

2.2.2 Bezpečnosť informácií

Bezpečnosť informácií sa zaoberá ochranou informácií, tak ako ochranou prístupu k nim. Je vybudovaná na troch hlavných pilieroch: dôvernosť, dostupnosť a integrita. Tieto tri termíny sú kľúčovými aspektmi systému riadenia bezpečnosti informácií.

Prioritou ochrany informácií v organizácii je zistiť bezpečnosť objektu a jej majetku uplatnením obecných bezpečnostných opatrení a postupov. Tento aspekt zahrňuje bezpečnosť informačných a komunikačných technológií, aktíva organizácie a prácu s informáciami v digitálnej aj papierovej podobe, tak ako aj informácie podané ústnou formou. Na všetky z týchto foriem komunikácií sa z pohľadu bezpečnosti zameriava ISMS. Ak nie je zabezpečenie dostatočné, či ISMS dobre zavedené, môže sa vyskytnúť bezpečnostná udalosť alebo v horšom prípade aj bezpečnostný incident.

Kybernetická bezpečnostná udalosť

Kybernetická bezpečnostná udalosť je stav systému služby alebo siete poukazujúc na možnosť porušenia bezpečnostnej politiky alebo zlyhania bezpečnostného opatrenia. Kybernetická bezpečnostná udalosť sa nemusí vyskytnúť nevyhnutne. V technickej kritickej infraštruktúre však vznikajú udalosti veľmi často. Pod kritickou infraštruktúrou rozumieme výrobné a nevýrobné služby a systémy, ktorých nefunkčnosť by mohla vážne ohroziť bezpečnosť štátu, verejnej správy, ekonomiky a zabezpečenie základných potrieb.

Rozlišujeme:

1. **Informational** - túto udalosť je dobre zaznamenať pre ďalšie spracovania, analýzy a monitorovania kapacitných trendov.
2. **Warning** - táto udalosť signalizuje dosiahnutie kritickej hodnoty niektorého z parametrov, napr. CPU, RAM, vďaka čomu je možné predchádzať vzniku incidentov.
3. **Exception** - táto udalosť signalizuje neštandardný stav, ktorý si vyžaduje našu akútnu pozornosť, napr. nedoručený mail, prihlásenie neplatným heslom.

Kybernetický bezpečnostný incident

Kybernetický bezpečnostný incident je narušenie integrity komunikačných sietí, bezpečnosti informačných systémov alebo narušenie bezpečnosti služieb, ako následok vzniku kybernetickej bezpečnostnej udalosti.

Informačný systém chápeme ako systém vzájomne prepojených procesov a informácií, ktoré tieto údaje spracúvajú. Zahrňuje informačné a dátové zdroje, pracovné, programové prostriedky, nosiče, zodpovedajúce technológie, normy a postupy.[4]

2.3 Známe štandardy

Existujú odvetvia, ktoré vyžadujú súlad s medzinárodnou organizáciou pre normalizáciu, ISO. Iné z organizácií sa dobrovoľne usilujú o dosiahnutie súladu s požiadavkami ISO, aby mohli verejne inzerovať v rámci týchto noriem. Ukazovateľom tohto súladu sa všeobecne považuje za ukazovateľ kvality výrobkov a poskytovania služieb. Viaceré s požiadaviek ISO vyžadujú, aby všetky testovacie prístroje boli certifikované podľa NIST na ďalšiu spoluprácu v rámci účelu dokumentácie. Bližšie o organizácii NIST sa budeme zaoberať v ďalších častiach tejto práce, (viď 2.3.1).

Rozlišovanie pojmu štandard a norma

V rôznych odborných textoch v kontexte rodiny ISO/IEC 27000 sa zamieňajú pojmy štandard a norma. Mohlo by skoro zdať by sa zdalo, že pojmy pomenúvajú tú istú vec. V publikácii *Problematika ISMS v manažerské informatice* (viď 2) sú tieto pojmy rozlišované a preto sa bude táto práca podľa tejto publikácie riadiť.

- **Štandard** je možno chápať ako technickú dokumentáciu obsahujúcu jasne stanovené kritériá využívané ako pravidlá, prípadne smernice, resp. ho možno chápať ako súbor charakteristických vlastností, ktorý zabezpečuje, že výrobky, procesy, či materiály sú v podobe, aký bol pôvodný zámer.

- **Norma** je doporučenie pre daný štandard, na základe ktorého sa realizuje požadované kompatibilné riešenie.

2.3.1 Inštitúcie zaoberajúce sa bezpečnosťou

Okrem organizácie ISO existujú aj ďalšie organizácie a inštitúcie, ktoré sa zaoberajú bezpečnosťou a správnym fungovaním ISMS. Každá z týchto organizácií má vlastné postupy a vydáva svoje vlastné vyhlášky a odporúčania. Organizácie sa odlišujú svojím prístupom, niektoré sú úmyselne cielené na konkrétnu oblasť, iné popisujú informačnú bezpečnosť len okrajovo.

Inštitúcie na území Českej republiky:

- MVCR (Ministerstvo vnútra Českej republiky - odbor koncepcie a koordinácie ISVS)
- ÚOOÚ (Úrad na ochranu osobných údajov)
- ÚNMZ (Úrad pre normalizáciu, metrológiu a skúšobníctvo)
- NBÚ (Národný bezpečnostný úrad)

Medzi zahraničné a medzinárodné normalizačné inštitúcie patria:

- NIST (US National Institute of Standards and Technology - Národný inštitút pre normy a technológie v USA) - bol založený v roku 1901. Je jedným z najstarších fyzikálnym laboratórií v krajine. Je neregulačnou federálnou agentúrou spadajúcou pod ministerstvo obchodu. NIST vyvíja a podporuje merania, normy a technológie na zvýšenie produktivity, uľahčenie obchodu a zlepšenie kvality života.

- ISACA (Information Systems Audit and Control Association - Medzinárodná profesná asociácia zameraná na oblasť auditu, riadenia, kontroly a bezpečnosti informačných systémov)

- OECD (Organization for Economic and Cultural Development - Organizácia pre hospodársku spoluprácu a rozvoj)

- BSI (British Standards Institute - Britský normalizačný inštitút)

- ANSI (American National Standards Institute - Americký národný normalizačný inštitút) [11]

2.3.2 ISO/IEC 27000-rodina známych štandardov

V tejto kapitole budú popísané niektoré z noriem rady ISO/IEC 27000, ktorých súčasťou je odporučenie pre zavedenie systému riadenia bezpečnosti informácií. Rada noriem ISO/IEC 27000, inak nazývaná ako systém riadenia informácií spadá do oblasti bezpečnosti informácií. Základom noriem rodiny ISO je ISO/IEC 27001, ktorá v základe definuje požiadavky na organizáciu ako celok pri práce s informáciami. Podľa základného štandardu ISO Guide 83 publikovaného v apríli 2012, majú všetky

dokumenty rodiny ISO 27K jasne definovanú štruktúru, postup a pravidlá začlenenia jednotlivých špecifických požiadaviek.[2][5]

2.3.3 Predstavenie konceptu ISO/IEC 27001

ISO/IEC 27001 je označenie štandardu, ktorá špecifikuje osvedčený postup ISMS a zahrňuje požiadavky na dodržiavanie predpisov. Patrí do rodiny ISO/IEC 27000, ktorú vydáva medzinárodná organizácia ISO. ISO/IEC 27001 poskytuje komplexný prístup pre systémy pri riadení informačných systémov, od aktív, dát, cez papierovú dokumentáciu a komunikačné technológie.

Tento štandard sa zavádza vo firmách ako certifikácie pre posúdenie schopnosti organizácie vytvoriť a udržať komplexný systém informačnej bezpečnosti. Možno povedať, že podľa ISO/IEC 27001 je organizácia certifikovaná, a teda spresňuje, s podrobným postupom ako by malo byť ISMS navrhnuté.

ISO/IEC 27001 je štruktúrovaný spôsobom, že je úzko prepojený na štandard ISO/IEC 9001, ktorý sa zaoberá štandardom kvality podnikateľských procesov organizácie.

V druhej polovici dokumentu sa nachádza príloha A, v ktorá obsahuje ciele opatrení, ktoré sú detailne rozpracované ako súčasť štandardu ISO/IEC 27002. Tieto ciele stanovujú, čo má byť dosiahnuté a opatrenia špecifikujú ako by sa týchto cieľov malo dosiahnuť.

Štandard ISO/IEC 27001 špecifikuje:

1. Procesy ustanovenia a riadenia ISMS
2. Procesy zavedenia a správy ISMS
3. Procesy monitorovania a analýza efektivity ISMS
4. Procesy údržby a zlepšovania ISMS
5. Procesy správy dokumentovej základne ISMS
6. Zodpovednosť vedenia organizácie za projekt ISMS
7. Ciele a princípy vybraných bezpečnostných opatrení
8. Procesy preskúmania ISMS treťou stranou, audit
9. Procesy aktualizácie ISMS

Štruktúra dokumentu:

Dokument má 10 krátky doložiek s prílohou A, ktorá obsahuje zoznam opatrení a cieľov, rady ako ich dosiahnuť a dôvod pre výber pri dosiahnutí týchto cieľov. Ciele definovaných normou ISO/IEC 27001:2013 sú bližšie popísané v kapitolách normy ISO/IEC 27002. [1] [6]

2.3.4 Predstavenie konceptu ISO/IEC 27002

Okrem ISO/IEC 27002 existuje v rodine ISO rada ďalších štandardov, ktoré poskytujú pokyny na implementáciu ISO/IEC 27001. Najznámejšia je ale práve ISO/IEC 27002, slúži organizácii na zváženie, čo všetko potrebuje na splnenie požiadaviek ISO/IEC 27001. Zatiaľ čo ISO/IEC 27001 poskytuje špecifikáciu, ISO/IEC 27002 ponúka manuál, smerovanie a odporúčané osvedčené postupy, ktoré sa môžu použiť na presadzovanie ISO/IEC 27001 špecifikácii.

Podľa ISO/IEC 27002 sa ISMS zavádza v podniku. Môžeme konštatovať, že je kódexom praktík, ktorá zaisťuje bezpečnosť informácií dotvárajúcich detaily postupov organizácie riadenia podľa ISO/IEC 27001. Vyberá opatrenia, ktoré by mal systém obsahovať.

Štruktúra dokumentu:

Tento štandard sa skladá zo 14 hlavných kapitol. Každá z týchto kapitol obsahuje bezpečnostné opatrenia a ciele, ktoré sa majú dosiahnuť a spôsob akým sa tieto ciele majú dosiahnuť po zavedení jednotlivých bezpečnostných opatrení.[7]

2.3.5 Predstavenie konceptu ISO/IEC 27003

Medzinárodná norma ISO/IEC 27003 vznikla v roku 2010. Norma obsahuje postup plánovania procesu implementácie ISMS na konci ktorého je vypracovaný plán, ktorý je podkladom pre realizovanie implementácie ISMS. V tomto dokumente sa nachádza odporúčanie pre návrh zavedenie ISMS v súlade s požiadavkami normy ISO/IEC 27001. Proces implementácie štandardu je rozdelený do piatich fáz:

- získanie súhlasu so začatím projektu od vedenia organizácie

- upresnenie hraníc, bezpečnostnej politiky a rozsahu
- vypracovanie analýzy požiadavkou bezpečnosti informácií
- vytvorenie zvládnutia a hodnotenia rizík
- realizácia systému riadenia bezpečnosti informácií

Finálnou fázou a zároveň výstupom je súhrn bezpečnostných opatrení s plánom implementácie v súlade s normou ISO/IEC 27001.

2.3.6 Predstavenie konceptu ISO/IEC 27004

Medzinárodná norma ISO/IEC 27004 bola vydaná v roku 2009. Aby bolo možné vyhodnocovať účinnosť zavedených opatrení v rámci ISMS je nutné mať nastavený systém metrík. Obsah tejto normy je zameraný na rozvoj metrík bezpečnosti informácií, analýzu dát a správu výsledkov meraní, preto je implementácia tohto štandardu odporučením.

2.3.7 Predstavenie konceptu ISO/IEC 27005

Táto medzinárodná norma je platná od roku 2011. Je určená najmä pre členov a pracovníkov organizácie, ktorí zastávajú manažérske pozície a zaoberá sa riadením rizík v oblasti bezpečnosti informácií. Norma je štruktúrovaná tak, že sa riadi konceptom štandardu ISO/IEC 27001 a podporuje tak implementáciu informačnej bezpečnosti do systému. Neobsahuje konkrétne metodiky, preto je na každej z organizácií, aký zvolí postup implementácie.

2.3.8 Predstavenie konceptu ISO/IEC 27006

Norma ISO/IEC 27006 je platná od roku 2011. V tejto norme sa nachádzajú požiadavky pre orgány, ktoré sprostredkúvajú audit a certifikácie ISMS. Norma tieto procesy akreditácie aktívne podporuje svojimi odporúčaniami.

2.3.9 Predstavenie konceptu ISO/IEC 27007

Medzinárodná norma ISO/IEC 27007 vznikla vo svojej platnej verzii v roku 2011. V tejto norme sa nachádzajú odporúčania pre odbornú spôsobilosť audítorov ISMS,

riadenia jednotlivých programov auditov ISMS podľa normy ISO/IEC 27001. Väčšinu informácií norma čerpá z normy ČSN EN ISO/IEC 19011 Smernica pre audit systému manažmentu akosti alebo systému environmentálneho manažmentu. [5]

2.3.10 Predstavenie konceptu ISO/IEC 27701

Predstavenie konceptu ISO/IEC 27701 je jedným z dôležitých bodov, na ktorý sa zameriava táto práca. Po predstavení jeho konceptu a štruktúr sa v ďalších fázach pristupuje k samotnej implementácii. Tento krok je zároveň aj cieľom a hlavnou náplňou diplomovej práce.

Štandard ISO/IEC 27701 predstavuje rozšírenie medzinárodného štandardu ISO-/IEC 27001 riadenia bezpečnosti informácií a prehlbuje oblasť ochrany súkromia a bezpečnosti informácií.

Norma ISO/IEC 27701:2019 vznikla za účelom, aby zainteresovaným stranám ponúkla manuál, akým spôsobom majú zavádzať opatrenia špecifikované v smerniciach EU GDPR zaručujúce ochranu osobným údajov. Bližšie sa GDPR budeme venovať v ďalších častiach tejto práce (viď 2.5.1).

Štandard ISO/IEC 27701 poskytuje rámec, ktorý pomáha organizáciám implementovať, udržiavať a neustále zlepšovať systém správy osobných údajov tzv. PIMS. Rozšírením požiadaviek a usmernení sa implementuje ustanovenie PIMS pomocou jej odporúčaných kontrol a opatrení zo zavedenej normy ISO/IEC 27001.

Taktiež sa v ňom stanovujú požiadavky na rozšírenie systémov riadenia informačnej bezpečnosti ISMS pre zlepšenie ochrany súkromia.

Štruktúra dokumentu:

- V paragrafe 5 sú stanovené požiadavky PIMS, vzťahujúce sa k bezpečnosti informácií štandardu ISO/IEC 27001 v rámci organizácie vystupujúci ako správca alebo spracovateľ osobných údajov. Príkladom môže byť odvolanie sa na jasné určenie, kedy právnická alebo fyzická osoba je v roli spracovateľa osobných údajov a kedy sa jedná o spracovávateľa (viď 2.5.1) alebo určenie interných a externých faktorov, ktorá môžu mať vplyv na stanovený cieľ v rámci PIMS. Jedná sa o aplikovateľné regulácie, platné legislatívy, súdne rozhodnutia (viď 2.5.3)

- V paragrafe 6 sa nachádzajú požiadavky vzťahujúce sa k opatreniam bezpečnosti informácií štandardu ISO/IEC 27002 vystupujúci ako správca alebo spracovateľ osobných údajov.
- Paragraf 7 obsahuje dodatočné rady štandardu ISO/IEC 27002 pre správcov osobných údajov.
- Paragraf 8 obsahuje rady štandardu ISO/IEC 27002 pre spracovateľa osobných údajov.

V druhej polovici normy ISO/IEC 27701:2019 sa nachádzajú prílohy A až F:

- príloha A obsahuje všetky aplikovateľné opatrenia pre organizáciu v pozícii správcu.
- príloha B obsahuje všetky aplikovateľné opatrenia pre organizáciu v pozícii spracovateľa

Prílohy C D a E mapujú ustanovenia voči iným štandardom a normám zaoberajúcim sa bezpečnosťou informácií:

- príloha C voči štandardu ISO/IEC 29100.
- príloha D voči celoeurópskemu zákonu zaoberajúcim sa bezpečnosťou informácií GDPR.
- príloha E voči štandardu ISO/IEC 29151 a ISO/IEC 27018.
- príloha F je špeciálnym návodom pre aplikovanie rozšírenia voči štandardom ISO/IEC 27001 a ISO/IEC 27002 pre ochranu súkromia pri spracovávaní osobných údajov. [8]

2.4 Implementácia nadväzujúceho štandardu ISO/IEC 27701

V tejto kapitole, sú popísané kroky nevyhnutné k procesu implementácie nadväzujúceho štandardu ISO/IEC 27701 na už zavedený štandard ISO/IEC 27001. Zavedenie predstavuje určitý zásah do procesu vykonávania činnosti organizácie a preto je dôležitá aktivita organizácie a záujem tento štandard aktívne zaviesť do praxe. V prípade, že sa Firma XY rozhodne certifikovať podľa tohto štandardu je nutné procesy riadne zdokumentovať a následne systém udržovať, vyhodnocovať a neustále zlepovať.

2.4.1 Príloha F-Nadväznosť štandardu ISO/IEC 27701 na ISO-/IEC 27001

ISO/IEC 27701 v nadväznosti na štandard ISO/IEC 27001 ponúka obdobné komplexné riešenie pri stanovenej problematike. ISO/IEC 27001 je navrhnutá tak, aby pomohla organizáciám riadiť ich procesy informačnej bezpečnosti v súlade s najlepšími medzinárodnými postupmi pri optimalizácii nákladov.

Poskytuje špecifické kroky pre správu informačnej bezpečnosti prostredníctvom pracovných politík, postupov a iných kontrol, do ktorých sú zapojení ľudia, procesy a technológie, aby pomohla jednotlivým organizáciám chrániť a spravovať všetky svoje údaje.

V kombinácii s ISO/IEC 27001 môže ISO/IEC 27701 pomôcť organizáciám demonštrovať, ako ich mechanizmy riadenia podporujú súlad s kľúčovými zákonmi o ochrane súkromia. Tento krok je rozhodujúcim prínosom v prípade, že dozorný orgán po porušení pravidiel požiada dôkaz o spoľahlivých postupoch v oblasti ochrany osobných údajov. Ako príklad je možné uviesť prílohu ISO/IEC 27701 *Bezpečnostné techniky* štandardu ISO/IEC 27701 rozširujúcu ISO/IEC 27001 a ISO/IEC 27002 *Správu informácií o súkromí požiadavky a usmernenia.*

Ak organizácia zaviedla normu ISO/IEC 27001, môže pomocou normy ISO/IEC 27701 rozšíriť svoje bezpečnostné opatrenia tak, aby pokrylo požiadavky na ochranu súkromia. Organizácie, ktoré nezaviedli ISMS, môžu implementovať normy ISO/IEC 27001 a ISO/IEC 27701 spoločne ako jeden projekt implementácie.

Normu ISO/IEC 27701 však nemožno implementovať ako samostatný štandard. Dôvodom je to, že ISMS vyhovujúci norme ISO/IEC 27001 je jadro, na základe ktorého dodatky ISO/IEC 27701 doplňujú opatrenia pre zachovanie súkromia a ochrany informácií. Rozšírenie ISMS v súlade s normou ISO/IEC 27001 a ISO/IEC 27701

môže poskytnúť dôkaz o tom, že organizácia podnikla kroky na implementáciu vhodných technických a organizačných opatrení na zníženie rizík a ochranu osobných údajov, tak ako to vyžaduje rastúca škála zákonov o ochrane súkromia na celom svete.[9]

2.4.2 Príloha F-aplikovanie PIMS

Vo väčšine prípadov pri už zavedenom štandarde ISO/IEC 27001 by mala organizácia začať pri prílohe F, ktorá hovorí o tom, akým spôsobom sa aplikuje PIMS do štruktúr tohto štandardu. Existujú tri možnosti:

1. zavedenie bezpečnostných štandardov, v podobe akej sú.
2. zavedenie dodatkov k bezpečnostným normám: Štandard bude zavedený s dodatočnými požiadavkami týkajúcej sa ochrany osobných údajov.
3. spresnenie bezpečnostných štandardov: Uvedené normy sú spresnené požiadavkami na ochranu osobných údajov.

Rozdiel v terminológii bezpečnosti informácii	
ISO/IEC 27001	Rozšírenie ISO/IEC 27701
Bezpečnosť informácii	Bezpečnosť informácii a súkromie
Politika v oblasti bezpečnosti informácii	Politika v oblasti bezpečnosti informácii a ochrany súkromia
Systém riadenia bezpečnosti informácii/**ISMS**	System riadenia osobným údajov/**PIMS**
Ciele bezpečnosti informácii	Ciele bezpečnosti informácii a súkromia
Úroveň bezpečnosti informácii	Úroveň bezpečnosti informácii a súkromia
Požiadavky informačnej bezpečnosti	Požiadavky informačnej bezpečnosti a súkromia
Riziko ohrozenia bezpečnosti informácii	Riziko ohrozenia bezpečnosti informácii a súkromia
Posúdenie rizika ohrozenia bezpečnosti informácii	Posúdenie rizika ohrozenia bezpečnosti informácii a súkromia
Plány riešenia pri riziku ohrozenia bezpečnosti informácii	Plány riešenia pri riziku ohrozenia bezpečnosti informácii a súkromia

Obr. 2.2: Porovnanie rozdielu v terminológii jednotlivých štandardov. zdroj: autor textu

To znamená, že sa mierne mení terminológia a to tak, že napr. informačná bez-

pečnosť sa mení na informačnú bezpečnosť a súkromie, alebo politika v oblasti bezpečnosti informácií na politiku v oblasti bezpečnosti informácií a ochranu súkromia. [9] [10]

2.4.3 Prehlásenie o aplikovateľnosti

V postupných krokoch sa opatrenia stanovené v ISO/IEC 27001:2013 porovnajú s opatreniami uvedenými v prílohe A a prílohe B normy ISO/IEC 27701:2019 či nedošlo k vynechaniu niektorých z dôležitých opatrení. Pri posudzovaní splniteľnosti jednotlivých cieľov podľa normy ISO/IEC 27001:2013 a prílohy A normy ISO/IEC 27701:2019 sa opatrenia posudzujú v kontexte rizík v súvislosti s bezpečnosťou informácií, tak ako riziká v súvislosti so spracovaním osobných informácií a riziká spojené so subjektmi údajov.

V tomto bode je vypracovaná súhrná správa, ktorá interpretuje výsledky z vykonanej porovnávacej analýzy. Správa je identifikovaná ako *Prehlásenie o aplikovateľnosti*. Cieľom je rozhodnúť, aký bude následný postup pri výskyte a identifikácii rizík. Vnútri tejto správy je zoznam opatrení, ktoré sú relevantné a aplikovateľné v rámci organizácie, pre ktorú je správa určená.

Dokument *Prehlásenie o aplikovateľnosti* musí obsahovať:

1. vybrané bezpečnostné opatrenia a dôvod ich výberu
2. zdôvodnenie vyradenia opatrení prílohy A v pozícii správcu a prílohy B v pozícii spracovateľa

Nie všetky z opatrení obsiahnuté v prílohách A a B je nutné implementovať. Zdôvodnenie vyradenia opatrení, môže obsahovať prípady, kedy opatrenie nie je v súlade s legislatívou, či nariadeniami, vrátane tých, ktoré sa vzťahujú na subjekty osobných údajov. Z *Prehlásenia o aplikovateľnosti* by malo jasne vyplývať, ako sa bude s konkrétnymi opatreniami pracovať. Všetky z opatrení, ktoré budú implementované by mali mať stanovený spôsob, ako k ich implementáciám dôjde. [8]

2.4.4 Implementovanie opatrení

Najdôležitejšia fáza celého procesu. V tejto fáze sa dokumentujú procesy, produkujú sa nové nariadenia alebo sa upravujú tie neaktuálne. Mnohé z interných činností firmy musia prejsť obmenou, tak isto prístup k nim, aby sa dosiahlo súladu s opatreniami na vrhnutými v štandarde ISO/IEC 27701.

2.4.5 Preverenie nedostatkov

Pri najmenšom podozrení, že opatrenia nie sú zavedené správne, čiže či dochádza k nezhodám je nutné tieto podozrenia preveriť a vyhodnotiť. Je rovnako dôležité dosiahnuť aj presadenie preventívnych opatrení, aby sa prípadným škodám zamedzilo do budúcnosti.

2.5 Európske právne akty zaoberajúce sa bezpečnosťou informácií

Táto sekcia rozoberá základné z Európskych právnych aktov vzťahujúce sa na členské štáty danej organizácie.

2.5.1 EU GDPR

GDPR je celoeurópske ucelené obecné nariadenie zaoberajúce sa ochranou osobných údajov, ktoré nahradilo európsku smernicu DPD a na tejto smernici sú založené ďalšie z právnych predpisov členských štátov vrátane britského DPA 1998. Tento dokument rozširuje práva jednotlivcov a ukladá organizáciám nové povinnosti, ktoré musia integrovať do svojich štruktúr.

Podľa GDPR sa organizácie môžu vyskytnúť v situácii v dvoch postaveniach:

správca osobných údajov

Správca osobných údajov je podľa GDPR, každý zo subjektov, ktorý špecifikuje prostriedky a účel spracovania osobných údajov, pričom nezáleží na právnej norme, pre ktoré sú tieto údaje spracovávané. Údaje sú zhromažďované, spracovávané a ukladané. S ukladaním dát je spojený kladený dôraz na ich dostatočné zabezpečenie.

spracovateľ osobných údajov

Spracovateľ osobných údajov je fyzická alebo právnická osoba, agentúra, orgán verejnej moci alebo iný subjekt, ktorý v mene správcu spracováva osobné údaje. Na rozdiel od správcu, spracovateľ môže vykonávať len tie činnosti, ktorými je spracovateľ správcom poverený. Spracovateľ je v tejto funkcii len vo vzťahu k osobným údajom poskytnutým správcom, na rozdiel od osobných údajov, ktoré sa ho priamo netýkajú.

2.5.2 GDPR obecne

GDPR sa vzťahuje na každého, kto zhromažďuje alebo manipuluje s dátami európskych občanov, v rámci organizácií a firiem, ktoré sa nachádzajú mimo Európskej únie, ale pôsobia na európskom trhu. Toto nariadenie má za cieľ chrániť digitálne práva občanov Európskej únie, takže sa zameriava na subjekty, ktoré spracovávajú osobné údaje, zamestnancov, klientov, zákazníkov, tak ako tých ktorí analyzujú dáta správania sa užívateľov na internete, či pri využívaní rôznych aplikácii.

GDPR je celoeurópsky jednotne zavedené od 25. mája 2018. Zákon o ochrane osobných údajov a právna úprava smernice 95/46/ES, doposiaľ suploval práva a povinnosti vyplývajúce s obecného nariadenia na ochranu osobných údajov.

Význam prijatia GDPR vo forme európskeho nariadenia, je dôležitý najmä z pohľadu jednotnej platnosti vo všetkých štátoch Európskej únie, čo znamená, že národné vlády nemôžu toto nariadenie ohýbať aby vyhoveli záujmom rôznych lobistov. Regulátorom, v sektore ochrany osobných údajov, ktorý plní funkciu začlenenia GDPR do štruktúr národnej právomoci v Českej republike, je Úrad pre ochranu osobných údajov.

Nariadenie so sebou prináša rovnocennú vymáhateľnosť práva v celej Európskej únii, sankcie a spoluprácu spoľahlivého dozorujúceho orgánu. V prípade porušenia, nepripravenosti, či nezavedenia nového nariadenia hrozia subjektom pokuty do výšky až 4% z celkového ročného obratu spoločnosti. Okrem finančných sankcii, môžu byť správcovia alebo spracovatelia osobných údajov vystavení žalobám s nárokom na náhradu škody v prípade hmotnej, či nehmotnej ujmy a to konkrétne:

- § 180 trestného zákonníka - pri neoprávnenom manipulovaní s osobnými údajmi, najmä v sektore verejných inštitúcií.
- pri porušení GDPR, čoho dôsledkom je zodpovednosť za škodu spôsobenú pri výkone verejnej moci rozhodnutím alebo nesprávnym úradným postupom.
- nedodržaní pravidiel stanovených v právnych predpisoch, teda predpisoch týkajúcich sa osobných údajov, kde dôjde súčasne k porušeniu.

Spracovateľ alebo správca osobných údajov podľa GDPR musí preukázateľne doložiť a zdokumentovať, že spracováva len dáta, ktoré sú ku konkrétnemu účelu nevyhnutné a to po celú dobu spracovania. Na rozdiel od nedávnej právnej úprave GDPR taktiež zavádza nové práva tzv. subjektom údajov.

Subjekty údajov musia byť o svojich práva dôkladne informovaní. Jedná sa o právo napr. ohradiť sa voči spracovaniu údajov, po ktorom správca nebude môcť tieto údaje

ďalej spracovávať. Taktiež právo preniesť údaje od jedného správcu k druhému, ak sú údaje spracované automatizovane. Subjekt údajov, by mal mať prístup k údajov, ktoré sú zhromažďované a taktiež má možnosť požiadať o vymazanie údajov, resp. byť "zabudnutý", čo znamená, že údaje subjektu údajov budú bezodkladne vymazané, ak neexistuje dôvod pre ich ďalšie spracovanie. S GDPR sa rozširuje aj definícia termínu "osobný údaj". Po novom sú do tohto termínu začlenený aj e-mail, IP adresa alebo údaje zhromažďované na internete, tzv. cookie. Táto smernica sa stala akýmsi modelom pre mnohé štátne zákony a predpisy krajín mimo Európskej únie, akými sú napr. Chile, Japonsko, Brazília, Južná Kórea, Argentína, Kenya. [12]

2.5.3 České právne akty vzťahujúce sa k bezpečnosti informácií

Táto kapitola sa zaoberá niektorými relevantnými zákonmi týkajúcich sa bezpečnosti informácií. Základným úkonom pri riešeniu otázky bezpečnosti je znalosť a modifikácia už existujúcich právnych predpisov. Legislatíva je nevyhnutný dokument potrebný na zrovnoprávneniu dokumentov a dát uložených v IS/ICT s dátami v klasickej papierovej podobe. Tento legislatívny rámec je základným kameňom pre budovanie informačnej bezpečnosti. Účel novovzniknutých zákonov je taktiež zosúladiť právny rád Českej republiky s právnym nastavením ostatných členských štátov Európskej únie.

- **Zákon č. 110/2019 Z.z. o spracovaní osobných údajov** upravuje povinnosti a práva pri procese spracovania osobných údajov, aby nemohla nastať situácia, že by došlo k náhodnému, či účelovému prístupu k osobným údajom, k ich zničeniu, strate, či úprave, tak ako k prenosom, bez vedomosti vlastníka osobných údajov. Zákon rozlišuje, jednotlivé strany, ktoré sú zapojené do ochrany osobných údajov, t.j. spracovateľ, správca, subjekt údajov a príjemca. Tento zákon taktiež stanovuje podmienky, za ktorých sa uskutočňuje transfer osobných údajov do zahraničia.

- **Zákon č. 412/2005 Z.z. o ochrane utajovaných informácií a o bezpečnostnej spôsobilosti** upravuje podmienky a zásady pre označenie informácie ako utajovaná, prístup k nim a výkon štátnej správy. Taktiež upravuje a vymedzuje činnosť Národného bezpečnostného úradu (NBS). Podľa **vyhlášky č. 412/2005 Sb.**, sú vymedzené druhy zabezpečenia informácií, ktoré sú utajované, zatiaľ čo ich úroveň je sledovaná Národným bezpečnostným úradom.

Jedná sa o:

- Fyzickú bezpečnosť
- Kryptografickú ochranu
- Administratívnu bezpečnosť
- Personálnu bezpečnosť
- Priemyslovú bezpečnosť
- Bezpečnosť komunikačných a informačných systémov [11]

- **Zákon č. 121/2000 Z.z. autorský zákon** integruje predpisy Európskeho spoločenstva do rádu Českej republiky a následne upravuje:

  - Práva upravujúce autorské práva
  - Ochranu práv podľa zákona
  - Práva autora k jeho vlastnému dielu
  - Kolektívnu správu autorských práv

- **Zákon č. 110/2019 Z.z. o spracovaní osobných údajov** a súvisiaci **zákon č. 111/2019 Z.z.** nezavádza prevratné zmeny oproti samotnému GDPR. Jednou zo zmien však je, že boli stanovené nulové sankcie pri porušení GDPR pre orgány verejnej moci a verejné subjekty.
- **Zákon č. 181/2014 Z.z.o ochrane kybernetickej bezpečnosti** modifikuje povinnosti a práva osôb a právomoci orgánov verejnej moci v oblasti kybernetickej bezpečnosti. Ak sú všetky body v tomto zákona obsiahnuté, subjekt by mal by schopnejší odolať prípadným kybernetickým hrozbám. Tento zákon sa však nevzťahuje na rozsah opatrní pre kritické, významné informačné a komunikačné systémy. So **zákonom č. 181/2014 Z.z.** úzko súvisí jemu podobné právne predpisy:

  - **Vyhláška č. 317/2014 Z.z.**, ktorá hovorí o **významných informačných systémoch a určujúcich kritériách**
  - **Nariadenie vlády č. 432/2010 Z.z. o kritériách určenia prvku kritickej infraštruktúry** [14][15]

3 Analýza súčasného stavu

Táto kapitola prináša základné informácie o spoločnosti, do ktorej bude štandard ISO/IEC 27701 implementovaný. Na analýzu firmy poslúži SWOT analýza a následne bude predstavená firma z pozície správcu a spracovateľa. V ďalšej časti sú predstavené nástroje, ktoré boli zvolené na vykonanie navrhovaných zmien. Záverom tejto kapitoly je celkové zhrnutie stavu bezpečnosti informácií vo firme, v ktorej je už zavedený štandard ISO/IEC 27001, a to z pohľadu oblasti konkrétnych opatrení obsiahnutých v štandarde ISO/IEC 27701. Z dôvodu bezpečnosti a rizika vynesenia citlivých dát, spoločnosť bude v rámci tejto práce anonymizovaná a od tejto sekcie označovaná ako Firma XY.

3.1 Predstavenie spoločnosti

Firma XY je česká súkromná firma, ktorá na slovenskom a českom trhu funguje od roku 1990.

Právna forma: Akciová spoločnosť

Zameriava sa hlavne na trh oblasti dodávok produktov, služieb a riešení na poli informačných a komunikačných technológií.

V počiatkoch sa o rýchly rozvoj vlastnej značky osobných počítačov zaslúžilo systematické budovanie rozsiahlej obchodnej a servisnej siete. V druhom desaťročí svojej existencie sa Firme XY podarilo postupne prepracovať medzi vrcholných predstaviteľov v oblasti rozsiahlych a zložitých ICT projektov a to koncentrovaním svojej pozornosti na poskytovanie komplexných IT riešení a služieb pre firemnú klientelu a štátnu správu.

Firma XY je akciová spoločnosť, ktorej hlavné sídlo sa nachádza v Ostrave. Jej predsedom predstavenstva je zároveň jeden z jej zakladateľov. Firma sa delí na 3 základné časti, tzv. business units, ktoré sa odlišujú svojim zameraním a segmentom trhu, ktorý obsluhujú. Jednotlivé časti majú svojich samostatných riaditeľov.

3.1.1 História

Firma XY bola založená v Ostrave v roku 1990, kde má dodnes svoje hlavné centrum. Postupným ustaľovaním sa na trhu sa podarilo rozšíriť pôsobenie v Prahe a Brne

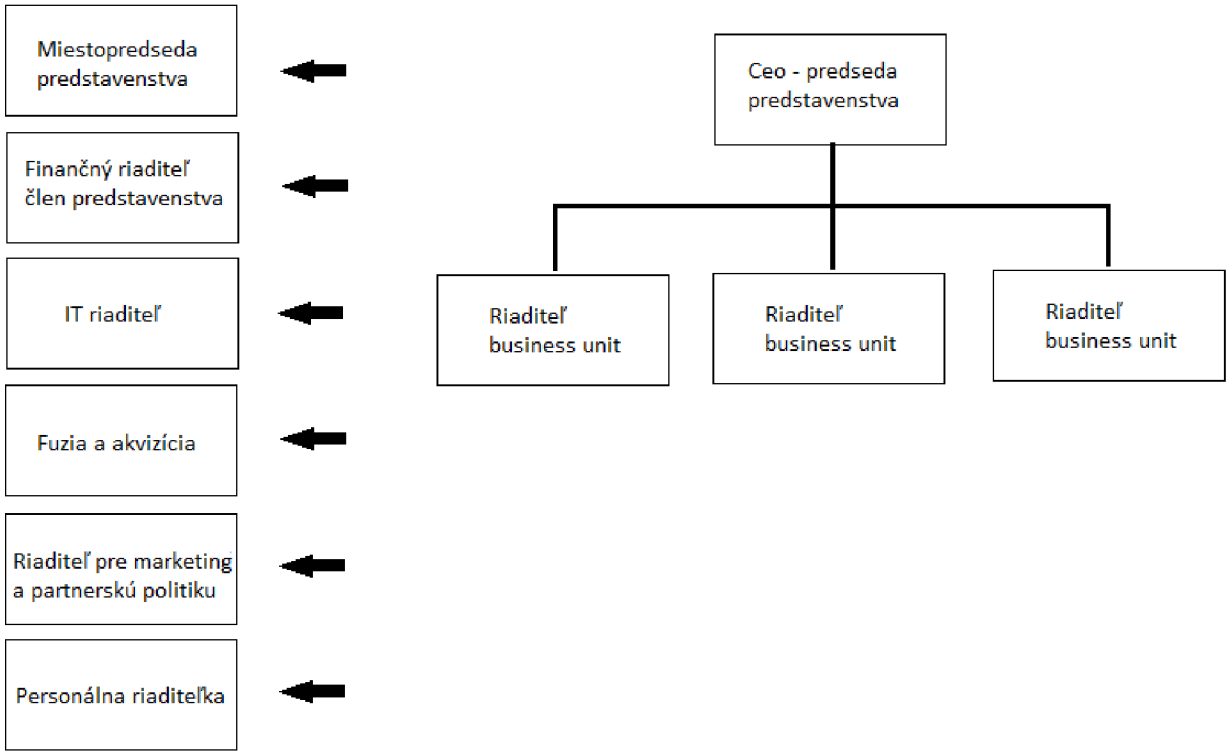
a to v roku 1991. Systematickým budovaním siete zastúpení sa podarilo expandovať a medzi rokmi 1992-1994 sa dostali k zastúpeniu 50 pobočiek po celej českej republike. O rok na to sa spoločnosti podarilo prepracovať na najväčšieho dodávateľa osobných počítačov v krajine. Ďalším krokom pri bolo vytvorenie distribučného oddelenia spoločnosti. ktoré je známe ako Firma XY CZ. V roku 1999 sa firma rozrástla natoľko, že bolo potrebné vytvoriť špeciálne divízie a ERP systémy, DMS systémy a IT infraštruktúru. V nasledujúcich rokoch sa podarilo získať outsourcing kontrakty s viacerými českými spoločnosťami, medzi inými Český Telecom.

Taktiež prebudovať pobočkové siete Firmy XY na regionálne centra. Podarilo sa ukončiť maloobchodný predaj a spoločnosť sa viac začala zameriavať na firemnú klientelu. Expandovaním a rozvojom aktivít na Slovensku sa Firma XY v roku 2012 zaslúžila o vybudovanie pobočky a vzniklo Firma XY SK a.s. V spolupráci s Microsoftom bol vybudovaný vlastný cloud v Českej republike a to v roku 2014. V roku 2017 vstúpil do firmy investor KKCG a.s., ktorý odkúpil 70 % akcii, zvyšok vlastní management spoločnosti.

3.1.2 Organizačná štruktúra

Organizačná štruktúra, je pomerne komplexná. Zobrazená štruktúra ukazuje sa len vrcholovú vetvu. Najvrcholnejším predstaviteľ je CEO-predseda predstavenstva, ktorému prislúcha obchodné vedenie spoločnosti. Riaditeľ business unit je zodpovedný za celý segment jednotlivých častí spoločnosti.

Firma XY je rozdelená v pôsobnosti v oblasti 3 segmentov. Každý z týchto segmentov zameraný na rozdielnu časť zamerania spoločnosti. Podrobná organizačná štruktúra je zachytená na nasledujúcej schéme:



Obr. 3.1: Organizačná štruktúra Firmy XY, spracovanie: autor textu

1. Prvý zo segmentov je zameraný na enterprise projekty pre väčších zákazníkov, segment s mnoho divíziami
2. Druhý segment je zameraný na podnikové aplikácie, implementácia a podpora podnikových informačných systémov Microsoft Dynamics
3. Tretí je obchodný segment, zameraný na stredných a malých zákazníkov, poskytuje IT infraštruktúru, podporu firemných procesov.

3.1.3 SWOT analýza Firmy XY

SWOT analýza predstavuje univerzálnu analytickú techniku zameranú na zhodnotenie vnútorných a vonkajších faktorov ovplyvňujúce úspech konkrétneho cieľa alebo celkovú efektivitu organizácie. Jej podstatou je identifikovať kľúčové silné a slabé stránky, teda v čom organizácia vyniká a v čom zaostáva, tak ako je dôležité poznať aj jej príležitosti a hrozby, ktoré sa nachádzajú v jej vonkajšom okolí. Zdrojom informácií na vypracovanie SWOT analýzy sú z archívne materiály firmy a dotazníku vyplnený manažérom jedného zo segmentov firmy.

Silné stránky

- Finančná stabilita spoločnosti
- Stabilní pozícia na českom ale aj zahraničnom trhu
- Kvalita dodávaných služieb
- Podpora noriem a legislatív
- Variabilita zamerania v podnikovej sfére
- Široký okruh zákazníkov

Slabé stránky

- Pri neočakávanom odchode zamestnanca chýba nejaký portál, wiki, za základe ktorého by účastník pozíciu prebral
- Nepraktický IS, neorganizovaný v rámci bezpečnosti informácií

Príležitosti

- Možnosť väčšieho využitia európskeho trhu
- Spolupráca s novými dodávateľmi

Hrozby

- Chyba prevádzkových zamestnancov
- Použitie softvéru neautorizovanými užívateľmi
- Chyba prenosu
- Infiltrácia komunikácie
- Zlyhanie komunikačných prostriedkov
- Zlyhanie hardvéru
- Zmena legislatívy
- Zneužitie aktíva externým užívateľom

3.2 Analýza konkrétnych oblastí

Na základe revízie GDPR vykonanej sériou rozhovorov s manažérmi jednotlivých sekcii firmy a spracovania týchto výsledkov vznikol dokument, ktorý mapuje činnosti jednotlivých segmentov Firmy XY. V nasledujúcich sekciách sú v skrátenej verzii uvedené tabuľky Firmy XY vystupujúcej v pozícii správcu (3.2) a následne aj spracovateľa (3.3). Plná verzia je obsiahnutá v prílohách (príloha č.A.1).

Zámerom tohto spracovania je analyzovať a identifikovať, za akým účelom Firma XY spracováva, resp. zákonnosť spracovania jednotlivých osobných údajov podľa nariadenia GDPR. Údaje ďalej ukazujú aké kategórie osobných údajov sú zhromažďované, podrobný popis konkrétnych osobných údajov o subjekte a v ktorých segmentoch firmy sú dáta prijímané. Tento dokument, je podľa nariadenia GDPR nutné udržovať a upravovať v aktuálnej forme.

3.2.1 Analýza spoločnosti ako správca osobných údajov

Obr. 3.2: Tabuľka 1: Spracovanie OU v pozícii správcu, zdroj: autor textu

Spracovanie	Oddelenie	Kategória OU
Vyhlásenie poplatníka - mesačné zľavy a ročné zúčtovanie	mzdové oddelenie	Meno, priezvisko, titul, trvalé bydlisko, rodné číslo, mzda, zmena stavu, do toho prikladá poistenie, hypotéky, dary,
Potvrdenie o zdaniteľných príjmoch	mzdové oddelenie	Meno, priezvisko, titul, trvalé bydlisko, rodné číslo, mzda, zmena stavu, do toho prikladá poistenie, hypotéky, dary,
Prihlásenie a odhlásenie zdravotného poistenia	mzdové oddelenie	Meno, priezvisko, trvalé bydlisko, rodné číslo
Prihlásenie a odhlásenie a zmeny sociálneho poistenia	mzdové oddelenie	Meno, priezvisko, trvalé bydlisko, rodné číslo + zmeny stavu, adresy
Evidenčný list dôchodkového poistenia	mzdové oddelenie	Meno, priezvisko, titul, adresa, od kedy pracuje, rodné číslo, mzdové údaje
Prehľad o výške príjmov ako podklad pre výplatu dávok chorobu. poistenie	mzdové oddelenie	Meno, priezvisko, rodné číslo, od kedy nastúpil a zárobok za posledných 12 mesiacov
Odhlásenie a prihlásenie cudzincov	mzdové oddelenie	Meno, priezvisko, miesto narodenia, trvalé bydlisko, miesto pobytu v čr, od kedy pracuje, pozície
Potvrdenie na účely podpory v nezamestnanosti	mzdové oddelenie	Meno, priezvisko, titul, rodné číslo, trvalé bydlisko, zamestnaný od do, dôvod ukončenia, priemerná výška čistého príjmu
zápočtový list	mzdové oddelenie	Meno, priezvisko, titul, trvalé bydlisko, vzdelanie, pozícia, od kedy do kedy, dátum narodenia
Hlásenie o pracovnom úraze	mzdové oddelenie	Meno, priezvisko, rodné číslo, telefón, adresa, údaje o úraze a prikladá sa záznam o pracovnom úraze
Vyčíslenie náhrady za stratu na zárobku	mzdové oddelenie	Meno, priezvisko, mzdové údaje
Ohlásenie pracovného úrazu na Inšpektorát bezpečnosti práce	mzdové oddelenie	Meno, priezvisko, rodné číslo, popis úrazu
Exekútorské úrady - súčinnosť k exekútorskému príkazu	mzdové oddelenie	Meno, priezvisko, rodné číslo, trvalé bydlisko, či už sú exekučné príkazy (iba áno / nie), budem / nebudem vykonávať zrážky, bankový ústav, počet vyživovaných osôb
Otázky od verejnej inštitúcie (súdy, polícia)	mzdové oddelenie	Meno, priezvisko, mzdové údaje, pracovné hodnotenie (záleží na tom, čo je vyšetrovaných)

Podklady pre mzdy - zrážky na základe dohody so zamestnávateľom	mzdové oddelenie	Adresa bydliska, dátum narodenia, E-mail, Meno a priezvisko, Osobné číslo, Rodné číslo, Telefón, vlastnoručne podpis
Podklady pre mzdy - zrážky pre exekúcie, insolvencie, výživné	mzdové oddelenie	Adresa bydliska, Celkový dlh, Čiastka zrážky dlhu (exekúcie, insolvencie), Čiastka zrážky výživného, Dátum narodenia, Meno a priezvisko, Priemerná mzda, Rodné číslo, Rodné priezvisko, Súdny výkon rozhodnutia, Účet splácanie dlhu (exekúcie, insolvencie), Účet splácanie výživného
Podklady pre mzdy - údaje o dochádzke	mzdové oddelenie	Meno a priezvisko, Neprítomnosť, Odpracovaný čas, Osobné číslo
Podklady pre mzdy - údaje o mzde, prémiách a odmenách	mzdové oddelenie	Čistá mzda, Meno a priezvisko, Mzda k výplate, Odmeny ku mzde, Osobné číslo, Zdôvodnení odmeny ku mzde
štatistické šetrenie	mzdové oddelenie	narodenia, pozície, osobné číslo, mzdové údaje, najvyššie vzdelanie, zamestnaný od do, koľko odpracoval hodín, aké mal prémie, príplatky, bonusy ...
Výplatná páska - elektronická	mzdové oddelenie	Meno a priezvisko, Adresa, osobné číslo, mzdové údaje, zdravotná poisťovňa
Výplatná páska - papierová	mzdové oddelenie	Meno, priezvisko, osobné číslo, mzdové údaje, zdravotná poisťovňa
prezenčná listina	oddelenie vzdelávania	Meno, priezvisko, názov firmy, podpis, deň účasti
preberací protokol	Účtovné oddelenie	Meno, adresa, rodné číslo alebo OP, adresa, telefón, e-mail, číslo účtu
stravné lístky	Účtovné oddelenie	Osobné číslo, meno, priezvisko, počet stravných lístkov
cestovný príkaz	Účtovné oddelenie	Meno, adresa, zaradenie, údaje o ceste
inventúra majetku	Účtovné oddelenie	Meno, priezvisko, lokalita, jednotlivé majetky
inventúra tovaru	Účtovné oddelenie	Meno a priezvisko, lokalita, súpis tovar, podpis člena inventárne komisie (3)

3.2.2 Analýza spoločnosti ako spracovateľ osobných údajov

Obr. 3.3: Tabuľka 2: Spracovanie OU v pozícii spracovateľa, zdroj: autor textu

Spracovanie	Oddelenie	Kategória OU
Objednávka školenia z webu	oddelenie vzdelávania	Meno, priezvisko, email, telefón, údaje zamestnávateľa, termín školenia, miesto, mená účastníkov, príp. titul a emailová adresa účastníka, cena
Registrácia na portále školiaceho strediska	oddelenie vzdelávania	Meno, priezvisko, email, telefón
subdodávateľ školenie	oddelenie vzdelávania	meno, priezvisko, email, firma
Osvedčenie o absolvovanom školenia alebo certifikát zo školenia	oddelenie vzdelávania	Meno, priezvisko, názov kurzu, termín, rozsah v hodinách
Person VUE	oddelenie vzdelávania	Meno, priezvisko, email, fotografie, preukázanie totožnosti OP alebo pasom + ďalším dokladom
Súhlas s pravidlami testovania + prezenčná listina	oddelenie vzdelávania	Meno, priezvisko, podpis
Záverečná správa k ESF (školenie)	oddelenie vzdelávania	Meno a priezvisko, názov firmy
AKRO	oddelenie vzdelávania	Meno a priezvisko, email, telefón, prihlasovacie údaje
IS pre podporu zákazníka ITSM	Oddelenie IT interné	Meno a priezvisko, pozícia, e-mail, telefón, názov, adresa
projektový server	Oddelenie IT interné	Meno a priezvisko, pozícia, e-mail, telefón, názov, adresa
O2	oddelenie prevádzky	Meno a priezvisko, Adresa, e-mail, telefón, číslo účtu, podpis
Súťažné podklady	Obchodné oddelenie 1	z Axapta ↑ + súťažných podkladov (kontaktnej osoby, email, telefón, meno a priezvisko)
Zmluva	Obchodné oddelenie 1	meno a priezvisko, email, telefón, pozície, podpis
servisná zmluva	Obchodné oddelenie 1	Meno a priezvisko, e-mail, telefón
archivácia zmluvy	Obchodné oddelenie 1	Meno a priezvisko, telefón, email
Customer service MS Dynamics 365	Obchodné oddelenie 1	Názov, meno a priezvisko, IČO / DIČ, e-mail, telefón, adresa
projektová dokumentácia	Obchodné oddelenie 1	kontakty naše + zákazníci, dovolenky
Projekty migrácie dát	Obchodné oddelenie 1	dáta zákazníkov dostaneme v určitej štruktúre a chceme ich do inej štruktúry
Directemailing	marketingové oddelenie	Meno a priezvisko, e-mail
Digitálne agentúra AETNA	marketingové oddelenie	Meno a priezvisko, firemné adresa
archivácia zmlúv	Back-office	Meno a priezvisko, adresa, názov, IČO / DIČ, podpis, telefón, e-mail, plná moc, ...
Microsoft licencie	Back-office	názov školy, IČO, adresa, objednávateľ

HP licencie	Back-office	názov firmy, adresa, IČO, DIČ, objednávateľ
dátová schránka	Back-office	Názov, IČO, adresa, príslušným úradom zasielaný na štatutárny orgán zapísaný v ROS na adresu pobytu podľa ROS / ROB, príp. doručovaciu adresu zapísanú v ROB.
Odoslanie zmluvy na realizáciu	Obchodné oddelenie 2	Meno a priezvisko (obchodníci a realizácia), telefón, email
Spolupráca so zahraničnou firmou	Obchodné oddelenie 2	Meno a priezvisko, email, telefón, (manažér IT)

3.2.3 Podmienky zhromažďovania a spracovania osobných údajov

Súbor politík pre bezpečnosť informácií je schválený, definovaný a publikovaný vedením Firmy XY. Je dôležité, aby zamestnanci a relevantné externé strany boli s jeho obsahom dobre oboznámení. Súbor základných bezpečnostných praktík tzv. bezpečnostné desatoro je povinný dokument na preštudovanie po úspešnom absolvovaní pohovoru a prijatí do spoločnosti. Bezpečnostná politika je v pravidelných intervaloch analyzovaná a upravená na pravidelných poradách vedenia zakaždým, kedy dôjdem k značnej zmene v interných štruktúrach firmy pre zaistenie jej efektivity. Súčasťou bezpečnostnej politiky je množstvo regulácii pri zhromažďovaní a spracovaní osobných údajov.

3.2.4 Povinné úkony voči subjektu údajov

Podľa normy ISO/IEC 27001 sú vo Firme XY informácie klasifikované z hľadiska hodnoty, zákonných požiadaviek, citlivosti voči neoprávnenému prezradeniu, či modifikácii v súlade s legislatívou. Sú zavedené postupy pre označovanie informácií v súlade s klasifikačnou schémou informácií. Aby sa zabránilo zneužitiu informácií a neautorizovanému prístupu sú implementované postupy pre ukladanie a úpravu dát.

3.2.5 Pôvodné znenie a úprava ochrany súkromia a osobných údajov

Firma XY má integrované politiky pri použití mobilných zariadení. V rámci zavedenia bezpečnostnej politiky sú prijaté opatrenia, ktoré môžu vzniknúť pri používaní mobilných zariadení. Taktiež sú vytvorené a aplikované zásady, politika a opatrenia na ochranu informácií, ktoré sú prístupné spracovávané a ukladané pri práci na diaľku. Firma má implementované a popísané postupy pre správu výmenných počítačových médií, ktoré obsahujú dáta s citlivým obsahom. Tieto postupy popisujú aj bezpečnú likvidáciu médií v súlade s formalizovanými krokmi a bezpečnostné metódy, ktoré musia byť dodržané behom prepravy médií, aby nedošlo k ich narušeniu, zneužitiu, či neoprávnenému prístupu k nim .

3.2.6 Prenos a zdieľanie osobných údajov

Vo Firme XY sú zavedené formalizované politiky, opatrenia a postupy aby prenos informácií bol dostatočne zabezpečený a to pri použitý rôznorodého typu komunikačného vybavenia. Elektrické predávanie správ je dostatočné chránené. Požiadavky na dohody o utajovaní a dohody o mlčanlivosti reflektujúce potreby organizácie chrániť informácie sú pravidelné monitorované a dokumentované a to podľa normy ISO/IEC 27001.

3.3 Nástroje využité na riadenie zmien

V tejto sekcii budú predstavené nástroje, ktoré boli zvolené na vykonanie navrhovaných zmien v podobe implementovania opatrení zo štandardu ISO/IEC 27701.

3.3.1 Gap analýza

Gap analýza, nazývaná aj rozdielová analýza je praktický manažérsky kontrolný nástroj vnútorného prostredia, ktorý by mal byť využívaný najmä vo vrcholovom manažmente, pri manažérskych rozhodnutiach, zostavovaním rozpočtu, organizáciami na zvýšenie pracovnej morálky a výkonnosti. Účelom je nájsť jednotlivé rozdiely medzi súčasným a referenčným, teda požadovaným stavom. V tejto práci je referenčným stavom myslené vyhovenie požiadavkom, ktoré sú rozpracované v norme ISO/IEC 27701:2019. Analýza môže byť využitá na organizačnej úrovni pri rôznych druhoch projektového riadenia, akou je napríklad rozvoj firemnej stratégie.

Pri využívaní tohto nástroja musíme prejsť niekoľkými dôležitými krokmi, aby sme dosiahli požadovaný cieľ alebo sa k nemu aspoň priblížiť. Pre tento účel sa vypracuje akčný plán, ktorý načrtne jednotlivé kroky na prekonanie medzery medzi aktuálnym stavom a ideálnym výsledkom. Medzery medzi požadovaným a súčasným stavom sa vo väčšine prípadov opakovane vyskytujú v jednotlivých kľúčových oblastiach. Gap analýza sa zameriava na jeden alebo viac z týchto kľúčových bodov:

1. Organizácia – ktoré zo zručností, znalosti či skúsenosti zamestnancom v organizácii chýbajú, musia byť preto viac trénovaní a školení
2. Smerovanie organizácie – medzery v obchodnom smerovaní, na trhu
3. Procesy – zlepšenie procesov, aby dosiahli väčšiu efektivitu
4. Technológie – nedostatok funkčných systémov, prípadne nekompatibility medzi nimi

[13]

3.3.2 Analýza dopadu

Metóda analýzy dopadu, sa zdá byť vhodným nástrojom, ktorý je možno využiť pri riadení zmien a riadení projektov, tak ako v oblasti strategického riadenia. Tento

nástroj má využitie pri zhodnotení plánovaných dopadov, prípadne predpokladov v projekte alebo činnosti plánujúce určitú zmenu.

Preto sa zdá byť vhodným riešením aj vrámci tejto práce. Znázorňuje rozpätie, v akom môžu jednotlivé riziká vplývať na Firmu XY. Dopady na organizáciu sa líšia svojou závažnosťou. Tie sú rozlišované na základe určitých kritérií, resp. následkov, ktoré postihujú. Na základe toho rozlišujeme dopad v podobe finančnej straty, dopad na dodávku služieb, poškodenie alebo strata povesti a nesplnenie zákonných alebo regulačných povinností. Pri procesoch rozhodovania si spoločnosť kladie určité priority, rozhoduje sa na základe stanovených kritérií. [16]

4 Vlastné návrhy riešenia

Nasledujúca kapitola obsahuje výstupy dosiahnutých využitím Gap analýzy a Analýzy dopadu. Tieto výstupy sú v podobe opatrení, ktoré sú reakciou na vzniknuté rizika identifikované definovaním kritérií dopadu.

4.1 Fáza príprav pred Gap analýzou

V tej sekcii sú špecifikované ciele a zameranie projektu. Pred samotným započatím Gap analýzy sú ujasnené zámery a očakávané výstupy implementácie a celého projektu. Na základe využitia citlivých dát a zasiahnutia do prvkov bezpečnostnej architektúry sú prípadné nejasnosti a potrebné modifikácie štruktúr konzultované s generálnym riaditeľstvom.

4.1.1 Ciele a výstupy

Napriek rozsiahlosti skúmanej Firme XY sa bude vzhľadom k opatreniam zameriavať analýza ako celok. Cieľom je vytvoriť hodnoverný obraz o súčasnom stave spoločnosti v rolách, kedy vystupuje ako správca a kedy ako spracovateľ osobných údajov a porovnať tento výstup s referenčným stavom. Podľa normy ISO/IEC 27701:2019 budú navrhnuté opatrenia, akým spôsobom objavené nedostatky znížiť na minimum alebo v ideálnom prípade kompletne eliminovať.

4.2 Vypracovanie Gap analýzy

Pre vypracovanie Gap analýzy je nutné zamyslieť sa nad procesom skúmania a ako k jeho výsledku dospejeme. Firma ma ambície zlepšiť svoju situáciu na trhu a teda sa snaží nájsť odpovede na to ako toto zlepšenie dosiahnuť. Tento proces je realizovaný za pomoci nasledovania niekoľkých krokov.

1. Dospieť k záveru ako vyhovieť požiadavkám rozširujúceho štandardu ISO/IEC 27701, dokumentovať jednotlivé kroky a následne sa nimi aj riadiť
2. Analýza dopadu, teda vyhotovenie zoznamu dôsledkov, ktoré spoločnosť môžu ovplyvniť, ak by sa rozhodla štandard neaplikovať

4.2.1 Forma spracovania

Záznam opatrení aplikovaných v rámci tejto práce je spracovávaný vo forme štrukturovaných tabuliek. Každá z oblastí, do ktorej opatrenia pochádzajúce z normy ISO/IEC 27701:2019 patria je spracovaná do osobitnej tabuľky. Firma XY berie do úvahy a systematicky analyzuje štandard v plnom rozsahu, teda každé jedno z kontrol, ktoré je súčasťou normy ISO/IEC 27701:2019 tak, aby bola zaručený plynulý priebeh implementácie.

Názov kapitoly		**Vyhovenie požiadavkám**		**Analýza dopadu**		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
Označenie poradia prvku	Znenie opatrenia					

Obr. 4.1: Štruktúra tabuliek, zdroj: autor textu

Štruktúra tabuliek opatrení z odporúčaní štandardu ISO/IEC 27701, ktoré spadajú do jednotlivých oblastí je rovnaká, tak ako je to možné vidieť na v tabuľke (4.2.1). V prvom kroku je postupne zvolené opatrenie v súlade s normou ISO/IEC 27701:2019, porovnávané so stavom, ktorý je požadované dosiahnuť. Následne je vyhodnotený dopad, ktorý je rozsiahly v závislosti od závažnosti nezavedeného opatrenia.

Podrobné objasnenie použitých skratiek v tabuľke (4.2.1) je umiestnené v tabuľke (4.2.1). Hodnota „Dopad“ je hodnota miery závažnosti, ktorá môže hroziť v prípade ignorovania opatrenia a vzniku incidentu. Kritériám hodnotenia dopadu sa budem venovať v ďalšej časti tejto práce. Tak isto je význam hodnoty „P(A)“ teda pravdepodobnosti, percentuálna hodnota s akou môže dôjsť k incidentu v prípade ignorovania odporúčaného opatrenia.

Schéma tabuľky v časti „Analýzy dopadu“ obsahuje bunku s názvom „Hodnota“.

Túto hodnotu vypočítame aplikovaním nasledujúceho vzorca:

$$\textbf{Hodnota} = \textbf{Dopad} * \textbf{P(A)}$$

Obr. 4.2: Výpočet výslednej hodnoty analýzy dopadu

Výsledok vedie k výpočtu celkovej hodnoty dopadu. Na základe veľkosti číselnej hodnoty výstupu posudzujeme výšku úrovne rizika a to je kategorizované podľa nasledujúcej tabuľky:

Úroveň rizika	Hodnotenie	Popis
Nezávažné riziko	1 - 3	Nevyžaduje sa žiadna akcia, riziko s nízkym dopadom
Tolerovateľné	4 - 7	Riziko je možno tolerovať, ak náklady na zriadenie opatrenia presahujú náklady spôsobené danou hrozbou využitím zranitelnosti
Závažné	7 a viac	Je potrebné vytvoriť akčný plán na zvládnutie rizika a implementovat relevantné opatrenie.

Obr. 4.3: Hodnotenie výsledku rizikovosti, zdroj: autor textu

Na základe dohody s predstaviteľmi Firmy XY boli stanovené kritéria dopadu. Tieto kritéria boli vytvorené na základe preskúmaní prioritných oblasti záujmu Firmy XY. (viď 4.2.1). Napriek tomu, že niektoré z incidentov sa môžu zdať nepravdepodobné, je dôležité o nich udržiavať prehľad. Analýza dopadu sleduje tie najzávažnejšie oblasti s najväčšími likvidačnými škodami, preto budú sledované najmä výstupy s hodnotou vyššou ako 7, podľa tabuľky 4.2.1.

	Riziko dopadu	1	2	3	4	5
		Nízke	Mierne	Stredné	Kritické	Fatálne
Bezpečnosť	**Ohrozenie aktív**	Poškodenie ICT, no škody sú nevýznamné	ICT je poškodené, obnova jeho funkcionality a spôsobené škody sú rádovo v desiatkach tisícov korún	ICT je poškodené, obnova jeho funkcionality a spôsobené škody sú v rádoch stoviek tisícov korún	ICT je vážne poškodené, obnova funkcionality je spojená s veľkými finančnými prostriedkami, spôsobené škody sú v rádoch miliónov korún	ICT je úplne zničené, pre obnovu jeho funkcionality je potrebé opätovné vybudovanie.
Ľudské zdroje	**Prekročenie právomocí**	Zapojenie výlučne koncových pracovníkov do procesu	Krátkodobé zapojenie vedúcich pracovníkov do procesu	Dlhodobé zapojenie vedúcich pracovníkov do procesu	Krátkodobé zapojenie vrchného vedenia do procesu	Dlhodobé zapojenie vrchného vedenia do procesu
Zákazníci	**Stráta dôvery zákazníkov**	Menšia strata zákazníkov bez významného dopadu	Väčšia strata zákazníkov s výraznejším stratom zákaziek	10% strata zákazníkov spôsobená stratou dôvery	20% strata zákazníkov spôsobená stratou dôvery	Likvidačné percento straty zákazníkov
Legislatíva	**Porušenie legislatívy**	Jednorázová pokuta vo výškach tisícky korún	Opakovaný delikt s pokutou do výšky desiatkach tisíc korún	Opakovaný delikt s pokutou do výšky stoviek tisíc korún	Opakovaný delikt s pokutou do výšky milión korún	Prehraný súdny spor s nutnosťou zaplatiť likvidačnú čiatku
Financie	**Finančná škoda na strane spoločnosti**	Finančná škoda, no relatívne nevýznamná	Finančné škody sú rádovo v desiatkach tisícov korún	Finančné škody sú rádovo v stovkách tisíc korún	Finančné škody sú rádovo v miliónov korún	Likvidačná škoda

Obr. 4.4: Kritéria dopadu, zdroj: autor textu

Pravdepodobnosť	Hodnota
Malá	1
Stredná	2
Vysoká	3

Obr. 4.5: Pravdepodobnosť kritérií dopadu, zdroj: autor textu

Nasleduje vysvetlenie skratiek, ktoré sú využívané v tabuľkách na kategorizovanie opatrení:

Skratky a vysvetlivky		
Skratky		
1)	**A/N**	Bude aplikované/nebude aplikované dané opatrenie
2)	**D/K**	Je dokumentované/nie jenedokumentované dané opatrenie
Dokumentovanie opatrenia-vysvetlivky		
1)	D	Opatrenie je dokumentované
2)	/	Opatrenie je zčasti dokumentované, je potrebná úprava
3)	N	Opatrenie nie je dokumentované
Aplikovanie opatrenia-vysvetlivky		
1)	OK	Opatrenie je aplikované
2)	MU	Menšia úprava opatrenia
3)	VU	Vačšia úprava opatrenia
4)	PZ	Aktuálne nezavedené opatrenie, potrebné zaviesť
5)	NZ	Nebude aplikované

Obr. 4.6: Vysvetlenie skratiek využitých v tabuľkách, zdroj: autor textu

Ako uvádza aj tabuľka vysvetliviek a skratiek, vyhodnocovanie jednotlivých opatrení a ich aplikovanie bude posudzované z dvoch hľadísk:

1. Či je opatrenie je už zavedené alebo v nejakej forme zaužívané a následne je vyhodnotená relevantnosť a benefity zo zavedenia daného požiadavku
2. Vyhodnotenie, či o zavedení opatrenia existuje dôkaz, resp. či je tento proces zdokumentovaný (kontrola smerníc, zmlúv, bezpečnostných politík, príručiek, manuálov)

4.3 Výstupy Gap analýzy

V aktuálnej situácii je Firma XY v súlade s predpísanými požiadavkami štandardu ISO/IEC 27001:2013. Nespĺňa však prvky, ktoré sú špecifikované v štandarde ISO-/IEC 27701:2019. Táto kapitola má za úlohu predstaviť opatrenia, ktoré Firme XY pomôžu dosiahnuť súlad s týmto štandardom a ošetriť bezpečnostné riziká, ktoré pri nezavedení tohto štandardu môžu nastať.

4.3.1 Opatrenia a kontroly správcov údajov, príloha A

Podmienky pre hromadenie a spracovanie dát

Podmienky pre hromadenie a spracovanie dát		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
A.7.2.1	**Identifikovať zámer dokumentu**	MU	D	1	1	1
A.7.2.2	**Definícia právneho základu**	MU	D	1	2	2
A.7.2.3	**Určiť kedy a ako je získaný súhlas**	OK	D	2	3	6
A.7.2.4	**Získanie súhlasu pre uchovanie údajov**	OK	D	2	3	6
A.7.2.5	**Hodnotenie vplyvu na súkromie**	MU	N	1	3	3
A.7.2.6	**Zmluvy so spracovateľmi osobných údajov**	MU	D	1	2	2
A.7.2.7	**Viac spracovateľov osobných údajov**	OK	N	2	2	4
A.7.2.8	**Záznamy spojené so spracovaním osobných údajov**	OK	D	2	4	8

Obr. 4.7: Podmienky pre hromadenie a spracovanie dát, zdroj: autor textu

Zistenie:

Tým, že má Firma XY zavedený štandard ISO/IEC 27001 a teda vypracovanú štrukturovanú bezpečnostnú politiku, má okrem toho k dispozícii bezpečnostné manuály, príručky a smernice, ktoré sú udržiavané na nepravidelnej báze. Preto nedávno došlo k menšej úprave a zjednoteniu týchto dokumentov do prehľadnejšej formy.

V písomných zmluvách so spracovateľmi osobných údajov Firma XY zlyháva pri vykonávaní niektorých príslušných kontrol v prílohe B, preto je nutná úprava, ktorá zabezpečí ich dodržiavanie.

Opatreniu, A.7.2.5 podľa ktorého organizácia vykoná posúdenie vplyvu na súkromie a A.7.2.7 podľa, ktorého organizácia určí príslušné úlohy a zodpovednosti za spracovanie osobných údajov vrátane požiadaviek na ochranu a bezpečnosť osobných údajov chýba dokumentácia.

Odporúčanie:

Podľa odporúčaní štandardu ISO/IEC 27701:2019 je nutné bezpečnostnú politiku a ostatné komplexné dokumenty týkajú sa bezpečnosti informácií dopĺňať a aktualizovať na pravidelnej báze, aby bola zaručená ich účinnosť a vhodnosť.

Pri opatrení A.7.2.1 a A.7.2.2 je nutné poopraviť formuláciu znení s dôrazom na súkromie subjektov údajov z prílohy F, (viď 2.4.2), v súlade podľa odporúčaní štandardu ISO/IEC 27701.

Opatrenie A.7.2.5 a A.7.2.7 Firma XY aktívne vykonáva, ale je potrebné doplniť jej príslušnú štrukturovanú dokumentáciu.

Povinné úkony voči subjektu údajov

Povinné úkony voči subjektu údajov		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
A.7.3.1	**Stanovenie a plnenie záväzkov voči subjektom údajov**	MU	/	1	1	1
A.7.3.2	**Určenie informácií pre subjekty údajov**	OK	D	2	2	4
A.7.3.3	**Poskytovanie informácií subjektom údajov**	OK	D	2	2	4
A.7.3.4	**Mechanizmu na zmenu alebo odvolanie súhlasu**	OK	D	2	3	6
A.7.3.5	**Mechanizmus na námietky proti spracovaniu osobných údjaov**	OK	D	2	2	4
A.7.3.6	**Oprava a vymazanie prístupu**	PZ	N	2	4	8
A.7.3.7	**Povinnosti spracovateľov osobných údajov informovať tretie strany**	OK	D	2	4	8
A.7.3.8	**Poskytnutie kópie spracovaných osobných údajov**	OK	N	1	2	2
A.7.3.9	**Spracovanie žiadosti**	OK	N	2	4	8
A.7.3.10	**Automatizované rozhodovanie**	OK	N	2	1	2

Obr. 4.8: Povinné úkony voči subjektu údajov, zdroj: autor textu

Zistenie:

Opatrenie A.7.3.1 podľa ktorého organizácia určí a zdokumentuje svoje právne, regulačné a obchodné povinnosti v súlade so zásadami subjektom osobných údajov súvisiacimi so spracovaním ich osobných údajov je dokumentované čiastočne, chýba jednotná dokumentácia v zmysle zjednotenia do jedného dokumentu.

Opatrenie A.7.3.6 podľa ktorého organizácia implementuje postupy a mechanizmy na splnenie svojich záväzkov voči subjektom údajov pri prístupe k úprave a vymazaniu ich osobných údajov nie je zavedené a dokumentované.

Pre opatrenie A.7.3.8, podľa ktorého organizácia musí byť schopná poskytnúť kópiu osobných údajov subjektom osobných údajov, A.7.3.9, podľa ktorého organizácia musí definovať a zdokumentovať politiky a postupy pre vybavovanie a reagovanie na legitímne žiadosti subjektov osobných údajov a A.7.3.10 podľa ktorého organizácia určí a adresuje povinnosti vrátane právnych záväzkov voči príkazcom subjektom osobných údajov chýba dokumentácia.

Odporúčanie:

Pre súlad s opatrením A.7.3.1 je potrebné zlúčiť čiastkové informácie týkajúceho sa tohto opatrenia (školenie (obchod + zmluva o spracovaní, HR, Marketing) do jedného komplexného dokumentu.

Pre opatrenie A.7.3.6 je potrebné vypracovať dokumentáciu s postupom na splnenie svojich záväzkov voči subjektom údajov k úprave a vymazaniu ich osobných údajov.

Opatrenie A.7.3.8, A.7.3.9 a A.7.3.10 Firma XY aktívne vykonáva, ale je potrebné doplniť jej príslušnú štrukturovanú dokumentáciu.

Pôvodné znenie a úprava ochrany súkromia

Pôvodné znenie a úprava ochrany súkromia		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
A.7.4.1	**Limitovanie zhromaždovania osobných údajov**	OK	N	2	4	8
A.7.4.2	**Obmedzenie spracovania**	MU	/	2	4	8
A.7.4.3	**Presnosť a kvalita**	MU	D	2	4	8
A.7.4.4	**Ciele minimalizacie osobných údajov**	PZ	N	2	3	6
A.7.4.5	**Vymazanie osobných údajov ku konci spracovania**	OK	D	2	2	4
A.7.4.6	**Dočasné záznamy**	MU	D	1	3	3
A.7.4.7	**Doba uchovania osobných údajov**	MU	D	1	3	3
A.7.4.8	**Likvidácia osobných údajov**	OK	D	1	3	3
A.7.4.9	**Prenos osobných údajov**	OK	D	2	4	8

Obr. 4.9: Pôvodné znenie a úprava ochrany súkromia, zdroj: autor textu

Zistenie:

Pre opatrenie A.7.4.1, podľa ktorého organizácia obmedzí hromadenie osobných údajov na minimum a A.7.4.4, podľa ktorého organizácia musí definovať a dokumentovať ciele minimalizácie údajov a aké mechanizmy sa používajú na dosiahnutie týchto cieľov chýba dokumentácia.

Opatrenie A.7.4.2, organizácia obmedzí spracovanie osobných údajov na spracovanie, ktoré je primerané a potrebné na identifikované účely je dokumentované len čiastočne a to v smernici osobných údajov.

Odporúčanie:

Opatrenie A.7.4.1 Firma XY aktívne vykonáva, ale je potrebné doplniť jej príslušnú štrukturovanú dokumentáciu. Opatrenie A.7.4.2 je potrebné dokumentovať a upraviť do formy plného znenia v súlade s odporúčaním štandardu ISO/IEC 27701.

Opatrenie A.7.4.3, podľa ktorého organizácia zabezpečí a zdokumentuje, že osobné údaje sú úplné a aktuálne, ako je potrebné na účely, na ktoré sa spracovávajú, A.7.4.6, podľa ktorého organizácia zabezpečí, aby dočasné súbory vytvorené v dôsledku spracovania osobných údajov boli zneškodnené podľa zdokumentovaných postupov v stanovenom zdokumentovanom období a A.7.4.7, podľa ktorého organizácia neuchováva osobné údaje dlhšie, ako je potrebné na účely, na ktoré sa spracúvajú osobné údaje je potrebné upraviť do formy plného znenia v súlade s odporúčaním štandardu ISO/IEC 27701.

Opatrenie A.7.4.4 Firma XY nemá zavedené, je potrebné doplniť jej príslušnú štrukturovanú dokumentáciu a zaviesť opatrenie do praxe.

Prenos a zdieľanie osobných údajov

Prenos a zdielanie osobných údajov		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
A.7.5.1	**Identifikovať základ pre prenos osobných údajov medzi jurisdikciami**	PZ	N	1	3	3
A.7.5.2	**Krajiny a medzinárodné organizácie, do ktorých je možný prenos osobných údajov**	PZ	N	2	2	4
A.7.5.3	**Zaznamy na prenos osobných údajov**	PZ	N	3	3	9
A.7.5.4	**Záznamy o sprístupnení osobných údajov tretím stranám**	PZ	N	3	4	12

Obr. 4.10: Prenos a zdieľanie osobných údajov, zdroj: autor textu

Zistenie:

Pre opatrenie A.7.5.1, podľa ktorého organizácia musí identifikovať a zdokumentovať relevantný základ pre prevody osobných údajov medzi jurisdikciami, A.7.5.2, podľa ktorého, organizácia špecifikuje a zdokumentuje krajiny a medzinárodné organizácie, do ktorých je možno osobné údaje v prípadne potreby prenášať, A.7.5.3, podľa ktorého organizácia zaznamenáva prevody osobných údajov tretím stranám alebo smerom od tretích strán týkajúcich sa subjektov osobných údajov a A.7.5.4,

podľa ktorého organizácia zaznamená zverejňovanie informácií osobných údajov tretím stranám chýba dokumentácia.

Odporúčanie:

Opatrenie A.7.5.1, A.7.5.2, A.7.5.3 a A.7.5.4 Firma XY nemá zavedené, je potrebné doplniť jej príslušnú štrukturovanú dokumentáciu a zaviesť opatrenia do praxe.

4.3.2 Opatrenia a kontroly spracovateľov údajov, príloha B

Podmienky pre hromadenie a spracovanie dát

Podmienky pre hromadenie a spracovanie dát		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
B.8.2.1	**Dohoda so zákazníkom**	OK	D	2	3	6
B.8.2.2	**Ciele organizácie**	OK	D	2	4	8
B.8.2.3	**Využitie marketingu a reklamy**	OK	D	1	4	4
B.8.2.4	**Porušenie postupov**	OK	D	1	3	3
B.8.2.5	**Povidnnosti zákazníka**	OK	D	2	3	6
B.8.2.6	**Záznamy týkajúce sa spracovania osobných údajov**	OK	D	2	4	8

Obr. 4.11: Podmienky pre hromadenie a spracovanie dát, zdroj: autor textu

Zistenie:

V tejto oblasti opatrení nebol nájdený nesúlad s opatreniami zo štandardu ISO-/IEC 27701.

Povinné úkony voči subjektu údajov

Povinné úkony voči subjektu údajov		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
B.8.3.1	Povinnosti subjektov údajov	OK	N	1	3	3

Obr. 4.12: Povinné úkony voči subjektu údajov, zdroj: autor textu

Zistenie:

Pre opatrenie B.8.3.1, podľa ktorého organizácia musí poskytnúť zákazníkovi prostriedky na splnenie jeho záväzkov týkajúcich sa subjektu údajov chýba dokumentácia.

Odporúčanie:

Opatrenie B.8.3.1 Firma XY aktívne vykonáva, ale je potrebné doplniť jej príslušnú štruktúrovanú dokumentáciu.

Pôvodné znenie a úprava ochrany súkromia

Pôvodné znenie a úprava ochrany súkromia		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
B.8.4.1	**Dočasné súbory**	OK	D	2	2	4
B.8.4.2	**Vrátenie, prevod alebo likvidácia osobných údajov**	VU	D	2	4	8
B.8.4.3	**Opatrenia pri prenose osobných údajov**	OK	D	3	4	12

Obr. 4.13: Pôvodné znenie a úprava ochrany súkromia, zdroj: autor textu

Zistenie:

Kontext opatrenia B.8.4.2, podľa ktorého organizácia musí zabezpečiť schopnosť návratu, prenosu alebo likvidácie osobných údajov bezpečným spôsobom, je okrajovo spomenutý v bezpečnostnej politike Firmy XY, no nezdá sa byť v plnej zhode.

Odporúčanie:

B.8.4.2 je potrebné upraviť do formy plného znenia v súlade s odporúčaním štandardu ISO/IEC 27701.

Prenos a zdieľanie osobných údajov

Prenos a zdielanie osobných údajov		Vyhovenie požiadavkám		Analýza dopadu		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
B.8.5.1	**Základ pre prenos osobných údajov medzi jurisdikciami**	PZ	N	3	3	9
B.8.5.2	**Krajiny a medzinárodné organizácie, do ktorých je možný prenos osobných údajov**	PZ	N	1	1	1
B.8.5.3	**Záznamy o sprístupnení osobných údajov tretím stranám**	PZ	N	2	3	6
B.8.5.4	**Oznámenie žiadosti o zverejnení osobných údajov**	PZ	N	1	3	3
B.8.5.5	**Právne záväzné zverejnenie osobných údajov**	PZ	N	2	4	8
B.8.5.6	**Zverejnenie subdodávateľov použitých na spracovanie osobných údajov**	PZ	N	1	1	1
B.8.5.7	**Zapojenie subdodávateľa do spracovania osobných údajov**	PZ	N	2	2	4
B.8.5.8	**Zmena subdodávateľa pre spracovanie osobných údajov**	PZ	N	2	4	8

Obr. 4.14: Prenos a zdieľanie osobných údajov, zdroj: autor textu

Zistenie:

Pre opatrenie B.8.5.1, podľa ktorého organizácia musí včas informovať zákazníka o podrobnostiach prevodov osobných údajov medzi jurisdikciami a o akýchkoľvek zamýšľaných zmenách v tomto ohľade, B.8.5.2, podľa ktorého organizácia musí špecifikovať a zdokumentovať krajiny a medzinárodné organizácie, do ktorých je možno

osobné údaje v prípadne potreby previesť, B.8.5.3, podľa ktorého organizácia musí zaznamenať zverejnenie informácií osobných údajov tretím stranám vrátane informácií o tom, ktoré z informácií boli zverejnené, komu a v akom čase, B.8.5.4, podľa ktorého organizácia oznámi zákazníkovi všetky právne záväzné žiadosti o zverejnenie osobných údajov, B.8.5.5 podľa ktorého organizácia odmietne akékoľvek požiadavky na zverejnenie osobných údajov, ktoré nie sú právne záväzné, B.8.5.6, podľa ktorého organizácia musí informovať zákazníka vopred, ak chce využiť služby subdodávateľa na spracovanie zákazníkových osobných údajov, B.8.5.7, podľa ktorého organizácia využije služby subdodávateľov iba v prípade, že je to v zmluve so zákazníkom a B.8.5.8, podľa ktorého sa od organizácie vyžaduje povolenie zákazníka písomnou formou, ak chce vykonávať zmeny týkajúce sa pridania alebo nahradenia subdodávateľov na účely spracovania osobných chýba dokumentácia.

Odporúčanie:

Opatrenie B.8.5.1, B.8.5.2, B.8.5.3, B.8.5.4, B.8.5.5, B.8.5.6, B.8.5.7 a B.8.5.8 Firma XY nemá zavedené, je potrebné doplniť jej príslušnú štrukturovanú dokumentáciu a zaviesť opatrenia do praxe.

4.4 Hodnotenie výstupu

V závere fáze tejto práce je potrebné dodať, že je na vrchnom vedení Firmy XY ako sa rozhodne využiť výstupy z dosiahnutých výsledkov. Ak sa spoločnosť rozhodne, že certifikácia podľa štandardu ISO/IEC 27701 je tou správnou voľbou a prinesie požadované benefity, je nutnou súčasťou ošetriť odhalené nedostatky v časti „Vyhovenie požiadavkám“, (viď 4.2.1). Ak sa na druhej strane nerozhodne certifikovať podľa tohto štandardu, dáta výstupu môže stále využiť v svoj prospech na skvalitnenie procesov a to s prihliadnutím na nasledujúce výstupy:

1. Pri skvalitnení procesov sa zamerať na segmenty s najvyššou vypočítanou celkovou hodnotou dopadu, teda najrizikovejšie bezpečnostné oblasti, ktoré dosiahli podľa kritérií dopadu hodnotu vyššiu ako úroveň hodnoty 7.
2. Zamerať sa taktiež na segmenty, ktoré dosiahli hodnotu dopadu rovnú 4, teda podľa kritérií dopadu hodnotu kritickú na bezpečnosť spoločnosti.

Z výstupu Gap analýzy je viditeľné, ktoré z kontrol a opatrení sú a nie sú ak-

tívne vykonávané, tak ako ktoré majú a ktoré nemajú vedený potrebný záznam a dokumentáciu. Ako možno vidieť z tabuliek jednotlivých oblastí, Firma XY má signifikantnú časť v plnej alebo čiastkovej forme už zavedenú, a teda je možné konštatovať, že má pevne vybudovaný segment informačnej bezpečnosti.

Na nasledujúcom obrázku je výber niekoľkých opatrení, ktoré sa podľa analýzy dopadu zdajú najrizikovejšie:

Výber najkritickejších opatrení		**Vyhovenie požiadavkám**		**Analýza dopadu**		
Prvok normy - číslo	Prvok normy - text	A/N	D/N	Hodnotenie opatrenia		
				P(A)	Dopad	Hodnota
A.7.3.6	**Oprava a vymazanie prístupu**	PZ	N	2	4	8
A.7.4.2	**Obmedzenie spracovania**	MU	/	2	4	8
A.7.5.3	**Zaznamy na prenos osobných údajov**	PZ	N	3	3	9
A.7.5.4	**Záznamy o sprístupnení osobných údajov tretím stranám**	PZ	N	3	4	12
B.8.5.1	**Základ pre prenos osobných údajov medzi jurisdikciami**	PZ	N	3	3	9
B.8.5.5	**Právne záväzné zverejnenie osobných údajov**	PZ	N	2	4	8
B.8.5.8	**Zmena subdodávateľa pre spracovanie osobných údajov**	PZ	N	2	4	8

Obr. 4.15: Výber najkritickejších opatrení, zdroj: autor textu

Výber najkritickejších opatrení je vykonaný na základe výpočtu celkovej hodnoty

dopadu, v tabuľke nazvaná ako „Hodnota“, ktorá je nad hranicou závažnej úrovne rizika, čo znamená, že je potrebné implementovať relevantné opatrenie na zvládnutie vzniknutého rizika (viď 4.2.1). Väčšina z týchto opatrení nie je náročne implementovateľná a Firme XY má možnosť priniesť výrazne zlepšenie v oblasti bezpečnosti informácií.

Záver

Hlavnou náplňou a cieľom tejto práce bolo analyzovať súčasný stav systému riadenia bezpečnosti informácii pre implementovanie rozširujúceho štandardu ISO/IEC 27701: 2019 v zvolenej konkrétnej spoločnosti, pre účel tejto práce z dôvodu rizika úniku citlivých dát anonymizovanej a nazvanej Firma XY. Táto norma zasahuje do viacerých významných oblastí spoločnosti. Na to aby stanovený cieľ mohol by dosiahnutý bolo vykonaných niekoľko krokov, ktoré boli podkladom pre vytvorenie návrhu riešenia a následne vypracovanie postupu implementácie tohto štandardu.

Prvý krok spočíval v preskúmaní a naštudovaní materiálov z oblasti problematiky bezpečnosti informácii. Boli vybrané a objasnené najrelevantnejšie technické termíny, koncepty, inštitúcie pôsobiace v tejto oblasti, štandardy, smernice, normy, nariadenia, ktoré sa týkajú bezpečnosti informácii. Dôraz pri objasnení pojmov bol kladený najmä na systém riadenia bezpečnosti informácii, známy ako ISMS. Tento riadiaci systém bolo dôležité spomenúť, keďže sa jedná o systematický postup pozostávajúci z procesov, technológií a nástrojov, ktorý slúži ako základ pre ochranu firemných dát a informácií za aktívnej asistencie efektívneho risk manažmentu. Bez prítomnosti tohto systému nebolo možné nastaviť rámec a nevyhnutné kontroly nad spracovaním osobným údajov z pozície správcu a spracovateľa, ktoré sú obsahom štandardu ISO/IEC 27001. V práci boli uvedené najznámejšie inštitúcie zaoberajúce sa bezpečnosťou informácií v Českej republike, ale aj v zahraničí.

Pri štandardoch bol kladený dôraz najmä na Medzinárodnú organizáciu pre normalizáciu, rodinu noriem ISO/IEC 27000, s menovaním najznámejších štandardov z tejto rady. Organizácia poskytuje a štandardizuje široký rozsah normalizácii. Množstvo ISO noriem je možne integrovať do jednotného systému riadenia. Medzi radou viacerých štandardov od organizácie ISO, ktoré má Firma XY zavedené, je spomenutý štandard ISO/IEC 27001, na ktorý štandard ISO/IEC 27701 nadväzuje svojimi rozširujúcimi opatreniami. Boli preskúmané a spomenuté aj zákony a legislatíva vzťahujúca sa k tejto téme, a to z pohľadu európskych a českých právnych aktov. Z európskych aktov bol spomenuté celoeurópske ucelené obecné nariadenie zaoberajúce sa ochranou osobných údajov nazývané GDPR.

V praktickej časti bola v prvom rade prezentovaná spoločnosť, ktorej sa táto riadiaca zmena týka. Boli spomenuté základné údaje o Firme XY, história spoločnosti, jej organizačná štruktúra, jej silné, slabé stránky, hrozby a príležitosti za pomoci SWOT analýzy a taktiež bola firma predstavená z revízie záznamov v pozícii správcu a spracovateľa.

Preto aby sa úspešne odhalili všetky riziká a oblasti bezpečnosti v ktorých sa Firma XY má medzery a priestor zlepšiť sa, bola využitá Gap analýza. Metóda bola využitá na porovnanie súčasne fungujúceho stavu a stavu, ktorého je požadované dosiahnuť. Ako referenčný model, teda požadovaný stav bol zvolený štandard ISO/IEC 27701:2019. Vyhodnocovanie jednotlivých opatrení a ich aplikovanie bolo posudzované z dvoch hľadísk, v prvom rade bolo posudzované, či opatrenie je už zavedené alebo v nejakej forme zaužívané a následne bola vyhodnotená relevantnosť a benefity zo zavedenia daného požiadavku. Následne bolo kontrolované, či o zavedení opatrenia existuje dôkaz, resp. či je tento proces zdokumentovaný.

Pre účely tejto práce boli vytvorené kritéria dopadu a hodnota dopadu bezpečnosti incidentu na podnik, v prípade, že by sa firma rozhodla ignorovať riziká a doporučené opatrenia. Za pomoci vyčíslenej pravdepodobnosti bola vypočítaná celková hodnota dopadu, ktorá bola následne porovnaná s vytvorenou stupnicou na meranie úrovne rizika.

Z hodnotenia vyhotovených analýz je možno pozorovať viaceré poznatky. Z tabuliek jednotlivých oblastí je možno vidieť, že niektoré z nedokumentovaných kontrol a opatrení je v skutočnosti vykonávaných a začlenených v každodenných procesoch. Aby bol proces úplný je potrebné o týchto procesoch viesť riadne záznamy a dokumentáciu. Ak k týmto dokumentáciám nedôjde, môže sa stať, že tieto procesy budú prebiehať nekontrolované a chaoticky. Jedným z ďalších pádnych dôvodov dokumentácie je neexistujúci záznam vykonávaných činnosti pre certifikačného audítora, ak by sa Firma XY rozhodla pre certifikáciu štandardu ISO/IEC 27701:2019. Ciele práce boli naplnené, bola vytvorená metodika s doporučením opatrení pre zlepšenie efektivity a úrovne v oblasti bezpečnosti informácii.

Literatúra

[1] STAUDEK, Jan. Bezpečnost IT. *Fi.muni* [online]. 2019 [cit. 2020-04-17]. Dostupné z: https://www.fi.muni.cz/usr/staudek/vyuka/security/PV017.xhtml

[2] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013, 377 s. : il, grafy, tab. ISBN 978-80-7204-872-4.

[3] ZLEPŠOVANIE NA ŠTYRI PÍSMENÁ? PDCA. *QUALITY FOR EVERYONE* [online]. 2019, 2012 [cit. 2020-04-17]. Dostupné z: https://q4e1.blogspot.com/2012/03/zlepsovanie-na-styri-pismena-pdca.html

[4] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník Kybernetické bezpečnosti. *Národní centrum kybernetické bezpečnosti* [online]. Praha, 2015 [cit. 2020-04-17]. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

[5] Řada norem ISO/IEC 27000. *RiskAnalysisConsultans* [online]. [cit. 2020-02-16]. Dostupné z: https://www.iso27000.cz/rac/homepage.nsf/CZ/ISO27000

[6] ISO/IEC, 2013a. Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky [online] [vid. 1. únor 2016]. Dostupné z: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[7] What is the difference between ISO 27001 and ISO 27002? *Dionach* [online]. 2018 [cit. 2020-04-17]. Dostupné z: https://www.dionach.com/blog/what-is-the-difference-between-iso-27001-and-iso-27002

[8] ISO 27701 The international standard for privacy information management. *IT Governance solutions* [online]. [cit. 2020-04-17]. Dostupné z: https://www.itgovernance.co.uk/iso-27701

[9] *International Standard ISO/IEC 27701: Security techniques-Extension to ISO-/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines*. Switzerland: ISO, 2019.

[10] ISO 27701: the new international privacy standard. *Bobsguide* [online]. [cit. 2020-04-17]. Dostupné z: https://www.bobsguide.com/guide/news/2019/Nov/12/iso-27701-the-new-international-privacy-standard/

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

[12] ŠKORNIČKOVÁ, Mgr. Eva. GDPR. *Obecné nařízení o ochraně osobních údajů* [online]. [cit. 2020-02-16]. Dostupné z: http://gdpr.cz

[13] Gap analysis. *Expertprogrammanagement* [online]. [cit. 2020-03-29]. Dostupné z: https://expertprogrammanagement.com/2017/09/gap-analysis/

[14] *Zákony pro lidi* [online]. [cit. 2020-04-17]. Dostupné z: https://www.zakonyprolidi.cz/

[15] Legislativa. *Acsoffice* [online]. Praha, 2020 [cit. 2020-04-17]. Dostupné z: https://acsoffice.cz/kyberneticka-bezpecnost/legislativa/

[16] *Dopadové analýzy* [online]. 2011 [cit. 2020-04-19]. Dostupné z: https://managementmania.com/cs/dopadove-analyzy

Zoznam symbolov, veličín a skratiek

DMS	Distribution Management System
DPD	Data Protection Directive
ERP	Enterprise Resource Planning
ICT	Information and Communication Technologies
ISMS	Information security management system
ISO	International Organization for Standardization
PIMS	Privacy Information Management System

Zoznam príloh

A Prílohy

A.1 Kompletná tabuľka firmy XY v pozícii správcu

,

Spracovanie	Oddelenie	Kategória OU
Vyhlásenie poplatníka - mesačné zľavy a ročné zúčtovanie	mzdové oddelenie	Meno, priezvisko, titul, trvalé bydlisko, rodné číslo, mzda, zmena stavu, do toho prikladá poistenie, hypotéky, dary, školkovné a manželka
Potvrdenie o zdaniteľných príjmoch	mzdové oddelenie	Meno, priezvisko, titul, trvalé bydlisko, rodné číslo, mzda, zmena stavu, do toho prikladá poistenie, hypotéky, dary, školkovné a manželka
Prihlásenie a odhlásenie zdravotného poistenia	mzdové oddelenie	Meno, priezvisko, trvalé bydlisko, rodné číslo
Prihlásenie a odhlásenie a zmeny sociálneho poistenia	mzdové oddelenie	Meno, priezvisko, trvalé bydlisko, rodné číslo + zmeny stavu, adresy
Evidenčný list dôchodkového poistenia	mzdové oddelenie	Meno, priezvisko, titul, adresa, od kedy pracuje, rodné číslo, mzdové údaje
Prehľad o výške príjmov ako podklad pre výlatu dávok chorobu. poistenie	mzdové oddelenie	Meno, priezvisko, rodné číslo, od kedy nastúpil a zárobok za posledných 12 mesiacov
Odhlásenie a prihlásenie cudzincov	mzdové oddelenie	Meno, priezvisko, miesto narozneí, trvalé bydlisko, miesto pobytu v čr, od kedy pracuje, pozície
Potvrdenie na účely podpory v nezamestnanosti	mzdové oddelenie	Meno, priezvisko, titul, rodné číslo, trvalé bydlisko, zamestnaný od do, dôvod ukončenia, priemerná výška čistého príjmu
zápočtový list	mzdové oddelenie	Meno, priezvisko, titul, trvalé bydlisko, vzdelanie, pozícia, od kedy do kedy, dátum narodenia
Hlásenie o pracovnom úraze	mzdové oddelenie	Meno, priezvisko, rodné číslo, telefón, adresa, údaje o úraze a prikladá sa záznam o pracovnom úraze
Vyčíslenie náhrady za stratu na zárobku	mzdové oddelenie	Meno, priezvisko, mzdové údaje
Ohlásenie pracovného úrazu na Inšpektorát bezpečnosti práce	mzdové oddelenie	Meno, priezvisko, rodné číslo, popis úrazu
Exekútorské úrady - súčinnosť k exekutorskému príkazu	mzdové oddelenie	Meno, priezvisko, rodné číslo, trvalé bydlisko, či už sú exekučné príkazy (iba áno / nie), budem / nebudem vykonávať zrážky, bankový ústav, počet vyživovaných osôb

Otázky od verejnej inštitúcie (súdy, polícia)	mzdové oddelenie	Meno, priezvisko, mzdové údaje, pracovné hodnotenie (záleží na tom, čo je vyšetrovaných)
Podklady pre mzdy - zrážky na základe dohody so zamestnávateľom	mzdové oddelenie	Adresa bydliska, dátum narodenia, E-mail, Meno a priezvisko, Osobné číslo, Rodné číslo, Telefón, vlastnoručne podpis
Podklady pre mzdy - zrážky pre exekúcie, insolvencie, výživné	mzdové oddelenie	Adresa bydliska, Celkový dlh, Čiastka zrážky dlhu (exekúcie, insolvencie), Čiastka zrážky výživného, Dátum narodenia, Meno a priezvisko, Priemerná mzda, Rodné číslo, Rodné priezvisko, Súdny výkon rozhodnutia, Účet splácanie dlhu (exekúcie, insolvencie), Účet splácanie výživného
Podklady pre mzdy - údaje o dochádzke	mzdové oddelenie	Meno a priezvisko, Neprítomnosť, Odpracovaný čas, Osobné číslo
Podklady pre mzdy - údaje o mzde, prémiách a odmenách	mzdové oddelenie	Čistá mzda, Meno a priezvisko, Mzda k výplate, Odmeny ku mzde, Osobné číslo, Zduvodneni odmeny ku mzde
štatistické šetrenie	mzdové oddelenie	narodenia, pozície, osobné číslo, mzdové údaje, najvyššie vzdelanie, zamestnaný od do, koľko odpracoval hodín, aké mal prémie, príplatky, bonusy ...
Výplatná páska - elektronická	mzdové oddelenie	Meno a priezvisko, Adresa, osobné číslo, mzdové údaje, zdravotná poisťovňa
Výplatná páska - papierová	mzdové oddelenie	Meno, priezvisko, osobné číslo, mzdové údaje, zdravotná poisťovňa
prezenčná listina	oddelenie vzdelávania	Meno, priezvisko, názov firmy, podpis, deň účasti
preberací protokol	Účtovné oddelenie	Meno, adresa, rodné číslo alebo OP, adresa, telefón, e-mail, číslo účtu
stravné lístky	Účtovné oddelenie	Osobné číslo, meno, priezvisko, počet stravných lístkov
cestovný príkaz	Účtovné oddelenie	Meno, adresa, zaradenie, údaje o ceste
inventúra majetku	Účtovné oddelenie	Meno, priezvisko, lokalita, jednotlivé majetky
inventúra tovaru	Účtovné oddelenie	Meno a priezvisko, lokalita, súpis tovar, podpis člena inventárne komisie (3)

inventúra pokladní	Účtovné oddelenie	Meno a priezvisko, lokalita, súpis tovar, podpis člena inventárne komisie (2)
Zaúčtovanie miezd do účtovníctva	Účtovné oddelenie	Meno, priezvisko, osobné číslo, mzdové údaje vr. Exekúcií, sporenie atď.
Riadenie zásob Axapta	Účtovné oddelenie	Meno a priezvisko, Názov
Pokladničné evidencia	Účtovné oddelenie	Meno, priezvisko, suma
service desk	Oddelenie IT interné	Meno a priezvisko (manažér projektu, nadriadený, pracovník, vlastník, kontakt, kontakt zákaznícky), e-mail, telefón, názov spoločnosti, funkcie, role kontaktu, úplná adresa
Axapta	Oddelenie IT interné	Meno a priezvisko (zamestnanec, nadriadený, mzdy zadal / schválil), dátum narodenia, osobné číslo, telefón, e-mail
Axapta CRM	Oddelenie IT interné	ID kontaktu, názov spoločnosti, meno a priezvisko, telefón, email, hlavný kontakt, funkcia
SharePoint portal server	Oddelenie IT interné	Všetky osobné údaje zamestnanci, zákazníci, metadáta
DC	Oddelenie IT interné	meno a priezvisko, osobné číslo, mzda, číslo účtu, e-mail, telefón, adresa, dátum narodenia, rodné číslo, číslo OP
ServiceNOW	Oddelenie IT interné	Meno, priezvisko, telefón, email
magma	Oddelenie IT interné	všetky údaje potrebné pre mzdové vyúčtovanie
magma nadstavba	Oddelenie IT interné	meno a priezvisko, osobné číslo, dochádzka
AD	Oddelenie IT interné	meno, priezvisko, email, telefón, organizačné začlenenie (pozícia), osobné číslo, fotografie,
certifikačná autorita	Oddelenie IT interné	názov, meno a priezvisko, e-mail
Office 365	Oddelenie IT interné	Údaje z AD + Meno a priezvisko, email, telefón, pozície
skype	Oddelenie IT interné	Údaje z AD + Meno a priezvisko, email, telefón, pozície
file servery	Oddelenie IT interné	Meno a priezvisko, email, telefón, pozície
moodle	Oddelenie IT interné	Údaje z AD

Acronis access	Oddelenie IT interné	Meno a priezvisko, e-mail, telefón, IP adresa
SIEM monitoring	Oddelenie IT interné	IP adresa
Ya3er	Oddelenie IT interné	Meno a priezvisko, telefón, e-mail, fotografie, pozície, vzdelania
CarNet	Oddelenie IT interné	meno, priezvisko, telefón, email, vozidlo
poštový server	Oddelenie IT interné	e-mail, IP adresa
Tlačové servery	Oddelenie IT interné	IP adresa
Dátové centrum a dátové sklady	Oddelenie IT interné	Meno a priezvisko
AC portál	Oddelenie IT interné	Meno a priezvisko, pozícia, e-mail, telefón, názov, adresa
Terminal server a centrum publikovaných aplikácií	Oddelenie IT interné	Meno a priezvisko, pozícia, e-mail, telefón, názov, adresa
IP telefónia	Oddelenie IT interné	IP adresa
VPN, PROXY, ANTI-SPAM	Oddelenie IT interné	IP adresa
Servisné a obchodný portál pre zákazníkov	Oddelenie IT interné	IP adresa, meno a priezvisko, názov, IČO / DIČ, telefón, e-mail, číslo účtu, pozície, adresa
webový server	Oddelenie IT interné	IP adresa, DNS meno
Verejné pracovné súbory a portál na zdieľanie informácií, tímovej prac. priestory	Oddelenie IT interné	IP adresa, meno a priezvisko
Business Lease	oddelenie prevádzky	Meno a priezvisko, Adresa, evidenčné číslo vozidla, e-mail, telefón, číslo účtu v prípade hradenia nákladov, podpis
rešpekt	oddelenie prevádzky	Názov, IČO / DIČ, Meno a priezvisko, adresa, rodné číslo, číslo OP, telefón, e-mail, podpis
pokuty	oddelenie prevádzky	Názov, IČO / DIČ, Meno a priezvisko, telefón, e-mail
pokuty	oddelenie prevádzky	Meno a priezvisko, Adresa, evidenčné číslo vozidla, e-mail, telefón, číslo účtu v prípade hradenia nákladov, podpis
Omeškanie s pokutou	oddelenie prevádzky	Meno a priezvisko, Adresa, evidenčné číslo vozidla, e-mail, telefón, číslo účtu v prípade hradenia nákladov, podpis

BOZP	oddelenie prevádzky	Meno a priezvisko, pozícia
vstupné list	personálne oddelenie	Meno, priezvisko, titul, bydlisko, OP, rodné priezvisko, stav, dátum narodenia, miesto, občianstvo, vodičský preukaz, zdravotná poisťovňa, číslo bankového účtu, poberanie dôchodku, zľava na deti, ZŤP, dátová schránka -číslo, ZŤP alebo ZTP- P, vlastnoručne podpis
výstupný list	personálne oddelenie	Meno, priezvisko, titul, bydlisko, OP, rodné priezvisko, stav, dátum narodenia, miesto, občianstvo, vodičský preukaz, zdravotná poisťovňa, číslo bankového účtu, poberanie dôchodku, zľava na deti, ZŤP
Osobný spis	personálne oddelenie	Kategória OU
Evidencia zamestnancov v IS	personálne oddelenie	Meno, priezvisko, titul, trvalé bydlisko, rodné číslo, mzda, zmena stavu, do toho prikladá poistenie, hypotéky, dary, školkovné a manželka
náborový proces	personálne oddelenie	Meno, priezvisko, titul, trvalé bydlisko, rodné číslo, mzda, zmena stavu, do toho prikladá poistenie, hypotéky, dary, školkovné a manželka
penzijné pripoistenie	personálne oddelenie	Meno, priezvisko, trvalé bydlisko, rodné číslo
Cafeteria	personálne oddelenie	Meno, priezvisko, trvalé bydlisko, rodné číslo + zmeny stavu, adresy
Podklady pre mzdy - evidencia dávok nemocenského poistenia	personálne oddelenie	Meno, priezvisko, titul, adresa, od kedy pracuje, rodné číslo, mzdové údaje
Podklady pre mzdy - evidencia stravných lístkov	personálne oddelenie	Meno, priezvisko, rodné číslo, od kedy nastúpil a zárobok za posledných 12 mesiacov

Blue Care - závodné starostlivosť	personálne oddelenie	Meno, priezvisko, miesto narozneí, trvalé bydlisko, miesto pobytu v čr, od kedy pracuje, pozície
Ponukový list / list	personálne oddelenie	Meno, priezvisko, titul, rodné číslo, trvalé bydlisko, zamestnaný od do, dôvod ukončenia, priemerná výška čistého príjmu
Zmena pracovného zaradenia	personálne oddelenie	Meno, priezvisko, titul, trvalé bydlisko, vzdelanie, pozícia, od kedy do kedy, dátum narodenia
CRM- kontakty	Obchodné oddelenie 1	Meno, priezvisko, rodné číslo, telefón, adresa, údaje o úraze a prikladá sa záznam o pracovnom úraze
Navigácia	Obchodné oddelenie 1	Meno, priezvisko, mzdové údaje
Osobný plán S KPI (Navigácia)	Obchodné oddelenie 1	Meno, priezvisko, rodné číslo, popis úrazu
mzdové tabuľky	Obchodné oddelenie 1	Meno, priezvisko, rodné číslo, trvalé bydlisko, či už sú exekučné príkazy (iba áno / nie), budem / nebudem vykonávať zrážky, bankový ústav, počet vyživovaných osôb
Dokumentácia o forme ukončení pracovného pomeru	Obchodné oddelenie 1	Meno, priezvisko, mzdové údaje, pracovné hodnotenie (záleží na tom, čo je vyšetrovaných)
CRM- evidencia referencií	Obchodné oddelenie 1	Adresa bydliska, dátum narodenia, E-mail, Meno a priezvisko, Osobné číslo, Rodné číslo, Telefón, vlastnoručne podpis
Ankety	marketingové oddelenie	Adresa bydliska, Celkový dlh, Čiastka zrážky dlhu (exekúcie, insolvencie), Čiastka zrážky výživného, Dátum narodenia, Meno a priezvisko, Priemerná mzda, Rodné číslo, Rodné priezvisko, Súdny výkon rozhodnutia, Účet splácanie dlhu (exekúcie, insolvencie), Účet splácanie výživného
elektronický katalóg	marketingové oddelenie	Meno a priezvisko, Neprítomnosť, Odpracovaný čas, Osobné číslo
Prezenčné listiny a spätnej väzby zo seminárov	marketingové oddelenie	Čistá mzda, Meno a priezvisko, Mzda k výplate, Odmeny ku mzde, Osobné číslo, Zduvodneni odmeny ku mzde

Zasielanie poštových zásielok	marketingové oddelenie	narodenia, pozície, osobné číslo, mzdové údaje, najvyššie vzdelanie, zamestnaný od do, koľko odpracoval hodín, aké mal prémie, príplatky, bonusy ...
mzdové tabuľky	Obchodné oddelenie 2	Meno a priezvisko, Adresa, osobné číslo, mzdové údaje, zdravotná poisťovňa
pracovný pohovor	Obchodné oddelenie 2	Meno, priezvisko, osobné číslo, mzdové údaje, zdravotná poisťovňa
Osobný rozvoj zamestnancov	Obchodné oddelenie 2	Meno, priezvisko, názov firmy, podpis, deň účasti
priestupok Etika	Obchodné oddelenie 2	Meno, adresa, rodné číslo alebo OP, adresa, telefón, e-mail, číslo účtu
CRM kontakty	Obchodné oddelenie 2	Osobné číslo, meno, priezvisko, počet stravných lístkov
archivácia zmluvy	Obchodné oddelenie 2	Meno, adresa, zaradenie, údaje o ceste
NDA (dohoda o mlčanlivosti)	Obchodné oddelenie 2	Meno, priezvisko, lokalita, jednotlivé majetky
Certifikát poučenie NBU	Obchodné oddelenie 2	Meno a priezvisko, lokalita, súpis tovar, podpis člena inventárne komisie (3)
Zákaznícky servis (rovnaký ako 1)	Obchodné oddelenie 2	Meno a priezvisko, lokalita, súpis tovar, podpis člena inventárne komisie (2)
odovzdávacie faktúra	Obchodné oddelenie 2	Meno, priezvisko, osobné číslo, mzdové údaje vr. Exekúcií, sporenie atď.
CRM- evidencia referencií	Obchodné oddelenie 2	Meno a priezvisko, Názov
zadávanie kontaktov	Back-office	Meno, priezvisko, suma
Dotácie na vzdelávanie	Back-office	Meno a priezvisko (manažér projektu, nadriadený, pracovník, vlastník, kontakt, kontakt zákaznícky), e-mail, telefón, názov spoločnosti, funkcie, role kontaktu, úplná adresa
evidencia zásielok	Back-office	Meno a priezvisko (zamestnanec, nadriadený, mzdy zadal / schválil), dátum narodenia, osobné číslo, telefón, e-mail

Zakladanie faktúr - recepcia	Back-office	ID kontaktu, názov spoločnosti, meno a priezvisko, telefón, email, hlavný kontakt, funkcia
RX - Evidencia faktúr bez zaúčtovania	Back-office	Všetky osobné údaje zamestnanci, zákazníci, metadáta
servisy	Back-office	meno a priezvisko, osobné číslo, mzda, číslo účtu, e-mail, telefón, adresa, dátum narodenia, rodné číslo, číslo OP
Vedenie knihy jázd	Back-office	Meno, priezvisko, telefón, email
Firemné akcie (výjezdka)	Back-office	všetky údaje potrebné pre mzdové vyúčtovanie
Kvalifikačné predpoklady do ponúk, insolvencie, exekúcie, pokuty	Back-office	meno a priezvisko, osobné číslo, dochádzka
Zaistenie pracovných ciest	Back-office	meno, priezvisko, email, telefón, organizačné začlenenie (pozícia), osobné číslo, fotografie,
Poistné udalosti u firemných áut	Back-office	názov, meno a priezvisko, e-mail
stravné lístky	Back-office	Údaje z AD + Meno a priezvisko, email, telefón, pozície
Výplatnice Trainee	Back-office	Údaje z AD + Meno a priezvisko, email, telefón, pozície
vstupné karty	Back-office	Meno a priezvisko, email, telefón, pozície
Dohoda o zapožičanie	Back-office	Údaje z AD
Dokumenty typu práceneschopnosť, potvrdenie o štúdiu, ružová vyhlásenie	Back-office	Meno a priezvisko, e-mail, telefón, IP adresa
Carnet	Back-office	IP adresa
faktúry	Back-office	Meno a priezvisko, telefón, e-mail, fotografie, pozície, vzdelania
Plná moc pri rokovaní za AC	Back-office	meno, priezvisko, telefón, email, vozidlo
pracovné pohovory	Obchodné oddelenie 3	e-mail, IP adresa

Osobný rozvoj	Obchodné oddelenie 3	IP adresa
mzdové tabuľky	Obchodné oddelenie 3	Meno a priezvisko
CRM kontakty	Obchodné oddelenie 3	Meno a priezvisko, pozícia, e-mail, telefón, názov, adresa
Excel s kontakty	Obchodné oddelenie 3	Meno a priezvisko, pozícia, e-mail, telefón, názov, adresa
Špecifikácie novej zmluvy	Obchodné oddelenie 3	IP adresa
servisné zmluvy	Obchodné oddelenie 3	IP adresa
Súťažné podklady	Obchodné oddelenie 3	IP adresa, meno a priezvisko, názov, IČO / DIČ, telefón, e-mail, číslo účtu, pozície, adresa
teambuilding	Obchodné oddelenie 3	IP adresa, DNS meno
Získavanie nových zákazníkov	Obchodné oddelenie 3	IP adresa, meno a priezvisko
Servisný portál	Obchodné oddelenie 3	Meno a priezvisko, Adresa, evidenčné číslo vozidla, e-mail, telefón, číslo účtu v prípade hradenia nákladov, podpis
CRM- evidencia referencií	Obchodné oddelenie 3	Názov, IČO / DIČ, Meno a priezvisko, adresa, rodné číslo, číslo OP, telefón, e-mail, podpis