VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IMPLEMENTACE NAŘÍZENÍ GDPR NA INFORMAČNÍ SYSTÉM KOLEJNET

IMLEMENTATION OF GDPR REGULATION TO THE KOLEJNET INFORMATION SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Lenka Krýzová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Lenka Krýzová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2017/18

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

Implementace nařízení GDPR na informační systém KolejNet

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Navrhnout systém ochrany osobních údajů implementaví GDPR.

Základní literární prameny:

DOUCEK, P. a kol. Řízení bezpečnosti informací. 2. přeprac. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8.

JORDÁN, V. a V. ONDRÁK. Infrastruktura komunikačních systémů I: Univerzální kabelážní systémy. 2. rozš. vyd. Brno: Akademické nakladatelství CERM, 2015. 352 s. ISBN 978-80-214-5115-5.

ONDRÁK, V., P. SEDLÁK, a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, 2013. 378 s. ISBN 978-80-7204-872-4.

POŽÁR, J. Základy teorie informační bezpečnosti. 1. vyd. Praha: Vydavatelství PA ČR, 2007. 219 s. ISBN 978-80-7251-250-8.

SPURNÁ, I. Počítačové sítě: praktická příručka správce sítě. Kralice na Hané: Computer Media, 2010.180 s. ISBN 978-80-7402-036-0.

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

V Brně dne 28.2.2018

L. S.

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

Abstrakt

Bakalářská práce se zabývá analýzou současného stavu bezpečnosti ochrany osobních údajů v informačním systému kolejní sítě VUT - KolejNet. Dále je část této práce věnována implementaci nařízení GDPR a bezpečnostních opatření na tento informační systém, a zhodnocení potřeb a požadavků pro tuto implementaci.

Klíčová slova

bezpečnost ICT, GDPR, počítačová síť, IP adresa, osobní údaje

Abstract

The bachelor´s thesis aims to make analysis of the current state of the KolejNet information system, personal data security and used internal standards of the company. It discusses the state of existing processes in corporation and improves functionality and quality of this information system, according to European GDPR regulation.

Key words

ICT security, GDPR, computer network, IP address, personal data

Bibliografická citace

KRÝZOVÁ, L. *Implementace nařízení GDPR na informační systém KolejNet*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 83 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

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

V Brně dne 11. května 2018

……

Podpis

Poděkování

Ráda bych tímto poděkovala vedoucímu mé bakalářské práce, Ing. Viktorovi Ondrákovi, Ph.D., za to, že byl ochotný věnovat svůj čas a zkušenosti k vedení této práce, dále také panu Ing. Petrovi Hermanovi, za poskytnuté informace, a taktéž Ing. Petrovi Sedlákovi za čas, který věnoval oponentuře.

OBSAH

ÚVOD

V dnešní době jsou informační technologie jedním z nejrychleji se rozvíjejících vědních odvětví. Vznik tohoto odvětví je soustředěn na druhou polovinu 20. století, kdy lidé začali automatizovat za účelem snížení nákladů, a tedy následného zvýšení zisku. Tento proces, který stále přetrvává, podstatně zrychluje každodenní život, to má za následek vysoké nároky na profesionály v oboru IT, vhodný a kvalitní materiál pro fyzickou výstavbu informačního systému, ale především pravidla pro bezpečnost. Stejně tak, jako je nutné vytvořit projekt pro návrh počítačové sítě, musíme vytvořit také projekt pro zabezpečení všech dat. Nejcennější data pro podnik budou mít nejvyšší klasifikační stupeň při hodnocení klasifikačními schématy a také tomu bude odpovídat riziko vzniku bezpečnostního incidentu. Mezi tyto data řadíme především citlivé osobní údaje, které v České republice chrání zákon č. 101/2000 Sb. neboli Zákon o ochraně osobních údajů, který reguluje Úřad pro ochranu osobních údajů. Dále se těmito daty zabývá směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Kybernetickou bezpečnost pak zajišťuje zákon č. 181/2014 Sb. Jelikož je však Česká republika členem Evropské unie, je podřízená také legislativě EU. Nařízení GDPR je ucelený soubor pravidel, kterým se musí řídit každý, kdo zpracovává či shromažďuje osobní údaje, který začne platit jednotně po celé EU dne 25. května 2018. Nesmíme také opomenout standardy ISO, jako hojně využívané normy (především ISO 27000, ISO 27001, ISO 27017, ISO 27018).

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Hlavním cílem je návrh schématu pro funkční implementaci nařízení General Data Protection Regulation (dále jen GDPR) vydané Evropskou Unií v roce 2016 na informační systém oddělení KolejNet do data účinnosti nařízení. Tento informační systém slouží pro administraci a správu kolejní sítě VUT. Tento systém je sdružen s databází VUT v Brně (IS VUT), a také s databází Kolejí a Menz VUT v Brně (KaM). Data, které informační systém zpracovává jsou získávány z těchto databází. Nejsou-li tyto data popsána, označena nebo neslouží-li jako osobní údaje nebude se jimi tato práce zabývat více, než je nezbytné.

Cíl je stanoven pomocí metody SMART, tento jednoduchý nástroj umožňuje správně a konkrétně definovat libovolný cíl v libovolné oblasti a je hojně využívám v rámci strategického či projektového řízení. Dle metody SMART musí náš cíl být specifický, měřitelný, akceptovaný, reálný a časově ohraničený. (Wagnerová, 2008, str. 51-52)

2 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretických východiscích práce jsou popsány teoretické poznatky, které jsou potřebné pro pochopení dané tématiky. V následujících odstavcích definuji otázky a odpovědi, které je nutné si ujasnit, před zavedením GDPR nařízení do politiky organizace. Ať už se jedná o vytvoření nových či úpravu stávajících pravidel organizace, je třeba jej důkladně zvážit, případné chyby mohou zapříčinit vysoké pokuty pro odpovědné osoby. Podrobně zde rozebereme jednotlivé prvky, které souvisí s pojmem GDPR a další názvosloví, používané v oblasti právní či v oblasti informačních technologií, které je nutné definovat před analýzou současného stavu a následnou implementací.

2.1 Ochrana osobnosti

Nařízení GDPR chrání především základní práva a svobody fyzických osob, a to zejména jejich právo na ochranu osobních údajů. Nařízení rozšiřuje působnost ochrany osobních údajů oproti původní legislativě. Ochranou osobnosti se zpočátku zabývá Všeobecná listina základních práv a svobod ustanovená OSN a následně jej rozšiřuje evropská legislativa, směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a dále také národní legislativa představená zákonem č. 101/2000 Sb. o ochraně osobních údajů.

2.1.1 Charta OSN

Tento dokument, který byl ustanoven Organizací spojených národů, uvádí práva a povinnosti členských států a definuje principy mezinárodních vztahů. Jedná se o smlouvu mezi členskými státy. Obdobným dokumentem je Všeobecná deklarace lidských práv a svobod. Tato listina byla přijata Valným shromážděním v roce 1948 a jasně tak vymezila práva a svobody každého člověka bez rozdílu. Článek 3. v této deklaraci říká, že každý má právo na život, svobodu a osobní bezpečnost. (OSN, 2015, str. 8)

2.1.2 Směrnice 95/46/ES

Tato směrnice ze dne 24. října 1995, vznikla v době, kdy informační technologie nebyly v tak pokročilém vývoji, a osobních údajů fyzických osob sdílených prostřednictvím sítě Internet bylo podstatně méně. Dnes je již nutné aplikovat moderní postupy a zahrnout

mezi osobní údaje i prvky s kterými tato síť běžně pracuje. Diskutovaným prvkem jsou tzv. cookies, malé textové soubory ukládané do paměti počítače v průběhu prohlížení webových stránek. (Kristol, 2001, str. 154) Cookies částečně chrání původní směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikacích, dále také Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009 a Zákon č. 468/2011 Sb. (Zákon 486/2011 Sb., EDPS 2017)

2.1.3 Návrh novely zákona č. 101/2000 Sb.

Datum autorizace Návrhu zákona o zpracování osobních údajů je 18.8. 2017. Návrh nahradí zákon č. 101/2000 Sb. o ochraně osobních údajů a předkladatelem je Ministerstvo vnitra ČR. Zákon je přizpůsoben nařízení Evropského parlamentu a Rady (EU) 2016/679 a zčásti implementuje směrnici Evropského parlamentu a Rady (EU) 2016/680. (Úřad vlády ČR, 2017)

2.2 Osobní údaje

„*Pro účely tohoto nařízení (GDPR) se rozumí:*

„osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě. identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“ (Evropská unie, 2016, Článek 4 Definice)

Genetické znaky fyzické osoby nazýváme genetické údaje, jejich podmnožinou jsou osobní údaje o zdravotním stavu, tyto informace se řadí mezi citlivé osobní údaje, na rozdíl od jména, pohlaví, věku, datumu narození, osobního stavu, cookies, IP adresy či fotografického záznamu, e-mailové adresy, telefonního čísla atd., výše vyjmenované údaje jsou pak zařazeny v kategorii obecné osobní údaje. Citlivé osobní údaje, které také umožňují jedinečnou identifikaci, jsou mimo jiné biometrické údaje – zpracovávají se zde fyziologické či fyzické znaky osoby (např. otisk prstu, podpis, snímek obličeje, snímek sítnice, poloha těžiště lidského těla aj.). Citlivé osobní údaje jsou dle GDPR dále také

informace o rasovém či etnickém původu, údaje o politickém názoru, náboženském nebo filozofickém vyznání, členství v odborech, údaje o sexuální orientaci a trestních deliktech či odsouzení osob a údaje dětí. Citlivé informace jsme nuceni zpracovávat s ještě větší obezřetností než v případě obecných osobních údajů, a řadíme je do kategorie zvláštní osobní údaje. Kategorie osobních údajů tedy definujeme jako obecné a zvláštní. (Evropská unie, 2016, Článek 4 Definice) Jedním z osobních údajů, velmi podstatných pro tuto práci, je rodné číslo, které je jedinečným identifikátorem fyzické osoby. Z pohledu zákona č. 101/2000 Sb., o ochraně osobních údajů, se tedy jedná o osobní údaj, jehož zpracování je upraveno zvláštním zákonem (Zákon č. 133/2000 Sb. a novelizace zákona č. 53/2004 Sb.). Základním ustanovením zákona o evidenci obyvatel je § 13 odst. 9, který svěřuje nositeli RČ nebo jeho zákonnému zástupci právo výlučně rozhodovat o jeho užívání a využívání. Jedním z právních titulů pro takové využívání rodného čísla je souhlas jeho nositele nebo zákonného zástupce. (Zákon č. 133/2000 Sb., Zákon č. 53/2014 Sb.)

2.3 Důležité pojmy

Článek 4 GDPR pak definuje 26 nejdůležitějších pojmů, z nichž byly vybrány pouze některé, relevantní k této práci.

- Zpracování jako jakoukoliv operaci či soubor operací s osobními údaji či soubory osobních údajů, prováděný automatizovaně nebo bez pomoci automatizovaných postupů. Pro osoby mladší 13 let je v České republice zpracování jejich údajů možné pouze se souhlasem jejich zákonného zástupce, podle obecného nařízení GDPR je tato hranice stanovena na 16 let.
- Správce osobních údajů jako fyzickou či právnickou osobu, orgán veřejné moci, agenturu nebo jiný subjekt, který sám nebo s dalšími subjekty určuje účely a prostředky zpracování osobních údajů.
- Zpracovatelem osobních údajů fyzickou nebo právnickou osobu nebo jiný subjekt, který zpracovává osobní údaje pro správce osobních údajů.
- Příjemcem je pak definován jiný subjekt, kterému jsou osobní údaje poskytnuty. Může se také jednat o třetí stranu, která přímo nepodléhá správci ani zpracovateli osobních údajů.

- Porušení zabezpečení osobních údajů, které znamená náhodné či protiprávní zničení, ztrátu nebo změnu osobních údajů či neoprávněné poskytnutí nebo zpřístupnění osobních údajů.
- Souhlas subjektu údajů jako jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, jenž stanovuje subjekt údajů a dovoluje tak zpracování svých osobních údajů.
- Anonymizací, stane-li se subjekt údajů neidentifikovatelným při zpracování osobních údajů. Často se taková data využívají pro statistické či výzkumné účely.
- Pseudonymizací, zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez dodatečných informací, uchovávaných odděleně a technicky a organizačně zabezpečené.
- Dozorovým úřadem se rozumí nezávislý orgán veřejné moci, zřízený členským státem, dle článku 51. (EDPS, 2017)

2.4 Legislativní úprava

Nařízení GDPR (2016/679) posiluje práva osob dotčených zpracováním osobních údajů. Ochrana se nevztahuje na osobní údaje zesnulých osob a anonymní informace. Posíleno je právo získávat informace kdo, jak a proč zpracovává osobní údaje, a právo se domáhat dodržování nařízení anebo nápravy v případě porušení. (Evropská unie, 2016, odstavec 26-27, článek 15)

2.4.1 Práva a povinnosti správce a zpracovatele o. údajů

V této kapitole se budeme zabývat právy a povinnostmi správce osobních údajů.

2.4.1.1 Zpracování

Za výše zmíněné zpracování můžeme považovat činnosti prováděné správcem osobních údajů nebo zpracovatelem jako shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení údajů. Omezení zpracování je pak chápáno jako označení osobních údajů, jejichž zpracování bude v budoucnu omezeno. Takové zpracování platí pro obecné

osobní údaje, při zpracování zvláštních osobních údajů vyžaduje nařízení ještě větší obezřetnost. Tak, jak zpracování udává GDPR (tedy systematické a za nějakým účelem), je definováno také zákonem 101/2000 Sb. o ochraně osobních údajů. (Evropská unie 2016, Článek 4 Definice, Zákon č. 101/2000 Sb.) V případě zaměstnanců nelze zpracovávané informace významně omezit či zaměnit za jiné, neboť legislativa České republiky (Zákoník práce č. 262/2006 Sb., Zákon o nemocenském pojištění č.187/2006 a jiné) vyžaduje zpracování těchto osobních údajů například z důvodu nemocenského pojištění. Zaměstnavatel však nesmí vyžadovat informace od zaměstnance, které přímo nesouvisí se základním pracovněprávním vztahem nebo s výkonem práce zaměstnance. (Zákon č. 262/2006 Sb., Zákon č. 187/2006 Sb.)

2.4.1.2 Zásady zpracování osobních údajů

Zpracovávané osobní údaje musí být:

- zákonné,
- korektní,
- transparentní (Všechny informace určené veřejnosti nebo subjektu údajů musí být stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových prostředků a ve vhodných případech také vizualizované.),
- účelově omezené,
- minimalizované,
- přesné. (Evropská unie, 2016, odstavec 58)

Dále musí ze strany správce splňovat následující vlastnosti:

- omezení uložení,
- integritu,
- důvěrnost,
- odpovědnost. (Evropská unie, 2016, článek 5 Zásady)

„S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobný a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

- *pseudonymizace a šifrování osobních údajů;*
- *schopnosti zajistit neustálou důvěrnost, integritu, dostupnost, a odolnost systémů a služeb zpracování;*
- *schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;*
- *procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.“* (Evropská unie, 2016, článek 5 Zásady)

2.4.1.3 Zákonnost zpracování

„Zpracování by mělo být zákonné, pokud je nezbytné v souvislosti s plněním smlouvy nebo úmyslem smlouvu uzavřít.“ (Evropská unie, 2016, odstavec 44)

„Zákonnost zpracování je splněna pouze, pokud je splněna nejméně jedna z následujících podmínek a pouze v odpovídajícím rozsahu:

a) s*ubjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,*

b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce,

f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.“ (Evropská unie, 2016, Kapitola II, Zásady)

„Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům,

zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.“ (Evropská unie, 2016, Kapitola II, Zásady)

Tedy je nutné poučit zaměstnance, kteří pracují s osobními údaji o změnách v organizaci, neboť změny mohou nastat také ve firemních směrnicích a pravidlech. Dodržováním pravidel se vyhneme nepříjemným situacím a někdy také finančním ztrátám. Mezi tzv. oprávněné zájmy správce můžeme zařadit některé druhy zpracování jako jsou:

- zpracování nezbytně nutné pro účely zamezení podvodům,
- zpracování pro účely přímého marketingu,
- předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely (osobní údaje zaměstnanců a zákazníků). (Evropská unie, 2016, odstavec 47)

2.4.1.4 Zpracování zvláštních kategorií osobních údajů

U osobních údajů zařazených do kategorie zvláštní, jako jsou například údaje vypovídající o rasové či etnickém původu, zdravotním stavu, politických názorech, náboženském vyznání či zpracování genetických údajů za účelem jedinečné identifikace, je dle nařízení zakázáno je zpracovávat, opět ale existují výjimky z pravidla (souhlas subjektu údajů, výkon právních nároků, významný veřejný zájem…).

2.4.1.5 Informace poskytované subjektu údajů

Správce musí dle obecného nařízení v okamžiku získání osobních údajů poskytnou subjektu údajů následující informace:

- totožnost a kontaktní údaje správce, včetně jeho zástupce,
- kontaktní údaje pověřence pro ochranu osobních údajů,
- účely zpracování a právní základ pro zpracování,
- oprávněné zájmy správce nebo třetí strany, v případě že je zpracování založeno na 6 odstavci, 1 písm. f),
- případné příjemce a kategorie příjemců,
- případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci,

včetně těchto informací poskytne správce také další údaje jako (doba uložení, existence práva požadovat přístup k údajům či podat stížnost, viz odst. 2, článek 13, GDPR), a to v případě jsou-li potřebné k zajištění spravedlivého a transparentního zpracování. (Evropská unie, 2016, článek 13)

2.4.1.6 Souhlas subjektu údajů

Souhlas jako jeden z možností, jak zákonně zpracovávat osobní údaje subjektu údajů, má také své ohraničení v obecném nařízení.

„Souhlas by měl být dán jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají, a to v podobě písemného prohlášení, i učiněného elektronicky, nebo ústního prohlášení. Mohlo by se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které v této souvislosti jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů. Mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas. Souhlas by se měl vztahovat na veškeré činnosti zpracování prováděné pro stejný účel nebo stejné účely. Jestliže má zpracování několik účelů, měl by být souhlas udělen pro všechny. Má-li subjekt údajů vyjádřit souhlas na základě žádosti podané elektronickými prostředky, musí být žádost jasná a stručná a nesmí zbytečně narušit využívání služby, pro kterou je souhlas dáván.“ (Evropská unie, 2016, odstavec 32)

Souhlasem subjektu údajů je tedy míněn jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. (Evropská unie, 2016, odstavec 4, článek 4 Definice)

„Subjekt údajů má právo svůj souhlas kdykoliv odvolat. Před udělením souhlasu o tom bude subjekt údajů informován.“ (Evropská unie, 2016, Kapitola II, Zásady)

2.4.1.7 DPO

S účinností nového nařízení vznikne také nová pracovní pozice tzv. DPO neboli Data Protection Officer. Dle pokynů rektora VUT musí pověřenec pro ochranu osobních údajů

dohlížet nad souladem zajištěním ochrany osobních údajů s příslušnými zákonnými normami a GDPR a slouží také jako kontaktní místo pro subjekty údajů a dozorový úřad. Pověřence jmenuje a odvolává rektor s tím, že na výkon činnosti pověřence má dotyčná osoba vždy sjednán pracovněprávní vztah. (Cetlová, 2017) Data Protection Officer má tedy především zodpovědnost za zpracování dat a manipulace s nimi, zodpovídá za komunikaci k zákonným vrstvám a kontrolu informací třetích stran a jeho úkolem je také hlášení úniků dat (do 72 hodin je nutné nahlásit významný únik dat). (Evropská unie, 2016, odstavec 37)

2.4.1.8 DPIA

Je nutné zde také zmínit zkratku DPIA (Data Protection Impact Assessment), česky Posouzení vlivu na ochranu osobních údajů. Jedná se o nástroj posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, a je nutné zejména v následujících případech: rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob které je založeno na automatizovaném zpracování, rozsáhlé zpracování zvláštních kategorií osobních údajů a rozsáhlé systematické monitorování veřejně přístupných prostorů. Posouzení by pak mělo obsahovat některé důležité body jako například:

- systematický popis zamýšlených operací a účely zpracování, včetně oprávněných zájmů správce,
- posouzení nezbytnosti a přiměřenosti operací zpracování,
- posouzení rizik pro práva a svobody subjektů údajů,
- plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením. (EDPS, 2017)

V odstavci 66 GDPR je uvedeno, že během procesu vymazávání osobních údajů v prostředí Internetu, je správce, který zveřejnil osobní údaje povinen informovat také správce, kteří osobní údaje zpracovávají, aby vymazali též veškeré odkazy, kopie a replikace těchto údajů. Je tedy důležité, aby byla zajištěna trasovatelnost, neboli odkud a kam se data odesílají, a aby bylo možné doložit provedené procesy. (Evropská unie, 2016, odstavec 66) Dále je také uvedeno, že při posuzování vhodné úrovně bezpečnosti, se zohlední zejména rizika jako náhodné nebo protiprávní zničení, ztráta, pozměňování,

neoprávněné zpřístupnění osobních údajů, nebo neoprávněný přístup k nim. (Evropská unie, 2016, Kapitola II, Zásady)

2.4.1.9 Vedení záznamů a dokumentace

Záznamy o činnostech definované GDPR nařízením nahradí oznamovací povinnost vedenou v zákoně 101/2000. Článek 30 určuje, jak postupovat při vedení záznamů o činnostech zpracování, za které zodpovídá správce a jeho případný zástupce. Takové záznamy obsahují následující informace:

- jméno a kontaktní údaje správce, společného správce, zástupce a pověřence pro ochranu osobních údajů,
- účely zpracování,
- popis kategorií subjektu údajů a kategorií osobních údajů,
- kategorie příjemců, kterým byly nebo budou os. údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích,
- informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci,
- je-li to možné plánované lhůty pro výmaz jednotlivých kategorií os. údajů,
- je-li to možné, popis technických a organizačních bezpečnostních opatření.

Nařízení udává, že záznamy budou vyhotoveny písemně (i elektronickou formou), a záznamy budou poskytnuty na požádání dozorovému úřadu. Organizace s méně než 250 zaměstnanci, mohou být zbaveny této povinnosti, ovšem pouze pokud zpracování osobních údajů, v takové organizaci nebude výrazně omezovat lidská práva a svobody, nebude možné jej považovat za rizikové nebo pokud jsou osobní údaje zpracovávány pouze příležitostně. (Evropská unie, 2016, článek 30)

„Správce by měl využít všech vhodných opatření k ověření identity subjektu údajů, který žádá o přístup, zejména v souvislosti s on-*line službami a síťovými identifikátory. Správce by neměl uchovávat osobní údaje pouze za tím účelem, aby mohl reagovat na případné žádosti.“* (Evropská unie, 2016, článek 64)

2.4.1.10 Správní pokuty

Správní pokuty hrozí všem povinným subjektům, a to v případě porušení nebo nezavedení GDPR nařízení, ale také v případě nepřipravenosti. Jejich maximální výše je stanovena na 20 milionů eur nebo 4 % vypočtená z celkového ročního obratu společnosti, přičemž je upřednostněna vyšší varianta pokuty. Pokuty se udělují s ohledem na závažnost porušení a míru následné škody, dále také dle počtu poškozených osob, a v neposlední řadě také dle reakcí subjektů na vzniklé škody. Správní pokuta je omezena na 10 milionů Kč pro tzv. veřejnoprávní subjekty. (Evropská unie, 2016, článek 83)

2.4.2 Práva subjektu osobních údajů

Jak již bylo zmíněno, nařízení GDPR vzniklo především pro ochranu fyzických osob a jejich práva na ochranu osobních údajů. Nařízení posiluje tato práva především v prostředí počítačových sítí, které se v posledních letech neustále rozšiřují. Za určitých podmínek může vzniknout pro subjekt údajů právo na omezení zpracování, mezi tyto podmínky patří například situace, kdy je zpracování osobních údajů protiprávní, ale subjekt údajů odmítá výmaz osobních údajů a žádá namísto toho omezení jejich použití. (Evropská unie, 2016, článek 18) Právo vznést námitku vzniká, nelze-li uplatnit právo na výmaz osobních údajů. Tímto krokem lze donutit správce osobních údajů k omezenému zpracování předmětných osobních údajů. Fyzická osoba musí být ze strany správce údajů upozorněna, že tato možnost vzniká. Odstavec 74 GDPR uvádí, že by měla být stanovena odpovědnost správce za jakékoliv zpracování osobních údajů prováděné správcem nebo pro něj. Tedy správce by měl být schopen zavést účinná opatření a doložit, že proces zpracovávání je v souladu s nařízením GDPR. (Evropská unie, 2016, odstavec 74)

Podle článku 13, odstavce 2 b) má subjekt údajů následující práva.

- Právo být informován o tom, jak budou osobní údaje zpracovávány a požadovat k nim přístup.

Tento bod definuje jasně odstavec 39 GDPR, a to v následujícím znění:

„Jakékoliv zpracování osobních údajů by mělo být prováděno zákonným a spravedlivým způsobem. Pro fyzické osoby by mělo být transparentní, že osobní údaje, které se jich týkají, jsou shromažďovány, používány, konzultovány nebo jinak zpracovávány, jakož i v j*akém rozsahu tyto osobní údaje jsou či budou zpracovány. Zásada transparentnosti*

vyžaduje, aby všechny informace a všechna sdělení týkající se zpracování těchto osobních údajů byly snadno přístupné a srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků. Tato zásada se dotýká zejména informování subjektů údajů o totožnosti správce a účelech zpracování a o *dalších záležitostech v zájmu zajištění spravedlivého a transparentního zpracování ve vztahu k dotčeným fyzickým osobám a* jejich *práva získat potvrzení a na sdělení zpracovávaných osobních údajů, které se jich týkají. Fyzické osoby by měly být upozorněny na to, jaká rizika, pravidla, záruky a práva existují v souvislosti se zpracováním jejich osobních údajů a* jak *mají v souvislosti s tímto zpracováním uplatňovat svá práva. Zejména je zapotřebí, aby konkrétní účely, pro které jsou osobní údaje zpracovávány, byly jednoznačné a legitimní* a aby byly stanoveny v *okamžiku shromažďování osobních údajů. Osobní údaje by měly být přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelů, pro které jsou zpracovávány. Je nezbytné zejména zajistit, aby byla doba, po kterou jsou osobní údaje uchovávány, omezena na nezbytné minimum. Osobní údaje by měly být zpracovány pouze tehdy, nemůže-li být účelu zpracování přiměřeně dosaženo jinými prostředky. Aby se zajistilo, že osobní údaje nebudou uchovávány déle, než je nezbytné, měl by správce stanovit lhůty pro výmaz nebo pravidelný přezkum. Měla by být přijata veškerá vhodná opatření, aby nepřesné osobní údaje byly opraveny nebo vymazány. Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a* k *zařízení používanému k* jejich *zpracování nebo jejich neoprávněnému použití.“*

- Právo na opravu osobních údajů (s využitím chráněného kanálu pro přenos informací).

Toto právo je také ošetřeno odstavcem 39 GDPR. Nejedná se aktivní povinnost správce.

- Právo na výmaz osobních údajů nebo přenesení osobních údajů.

Podle odstavce 65 GDPR má fyzická osoba tzv. „právo být zapomenuta“ a to především pokud uchovávání osobních údajů porušuje nařízení GDPR nebo právo Unie či členského státu, které se na správce vztahuje. Dále pokud již údaje nejsou potřebné pro účely, pro které byly shromážděny a zpracovávány, pokud subjekt údajů odvolal svůj souhlas se zpracováním nebo pokud vznesl námitku proti zpracování údajů, které se jej týkají. Toto právo fyzické osoby jakožto subjektu údajů je také velmi důležité, pokud byl souhlas se

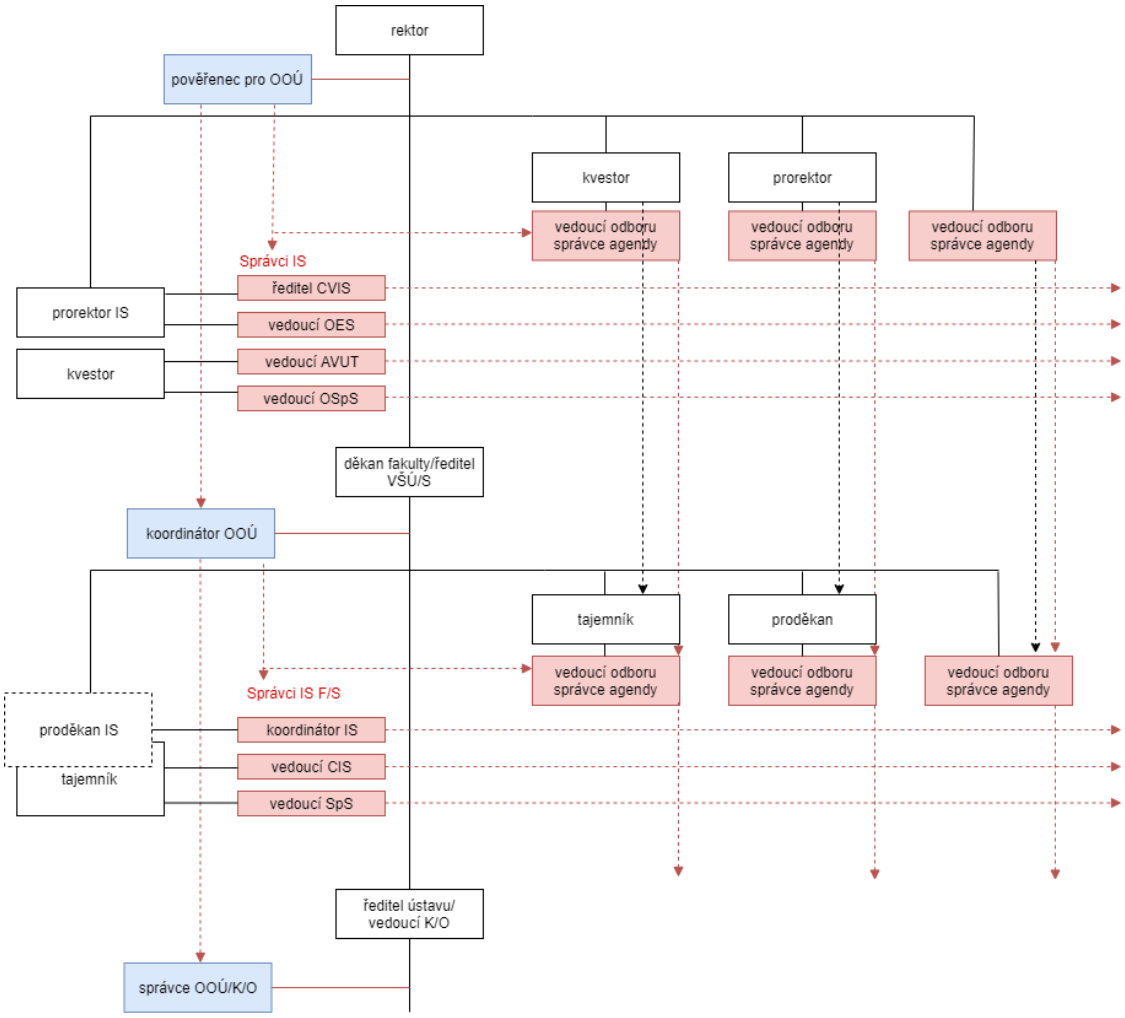
zpracováním udělen v dětském věku, tedy subjekt údajů si nebyl plně vědom rizik, které mohou se souhlasem souviset. (Evropská unie, 2016, odstavec 65)

2.5 Definování postupu

Ministerstvo školství mládeže a tělovýchovy zveřejnilo metodiku zavedení GDPR do provozu, kde napomáhá subjektům (především školám), které budou muset toto nařízení implementovat. Z této metodiky může být použito několik postupů i v této práci. Dle pokynů rektora VUT v Brně podstoupily všechny definované informační systémy auditem zpracovaným na základě Metodického listu č. 5/2017. Vedoucí jednotlivých součástí VUT odpovídají za organizační a technická nastavení pro zabezpečení ochrany osobních údajů a jejich zpracování v souladu s příslušnými zákonnými normami a GDPR, jakožto i za soulad těchto nastavení s metodickými nastaveními stanovenými na VUT v Brně. Dále jsou vedoucí jednotlivých součástí povinni určit tzv. „koordinátora ochrany osobních údajů“, na základě pracovněprávního vztahu bude zodpovídat za následující body:

- komunikace s pověřencem pro ochranu osobních údajů,
- technická implementace a návrh úprav přijatých nastavení za účelem zajištění zákonnosti zpracování,
- aktivní vyhledávání zvláštních činností, které více vyžadují ošetřit zákonným postupem,
- výkon kontrolní činnosti v dané oblasti a navrhování bezpečnostních opatření.

Každý vedoucí zaměstnanec dále odpovídá za konkrétní výkony a dodržování nastavení, za zajištění seznámení všech podřízených zaměstnanců s nastaveními a za ověřování dodržování nastavení k ochraně osobních údajů. Každý zaměstnanec pak zodpovídá za dodržování těchto nastavení na úrovni příslušné součásti VUT. (Cetlová, 2017)



Obrázek 1: Organizace systému ochrany osobních údajů na VUT v Brně.
(Zdroj: Pokyn č. 6/2018, příloha č. 1)

2.6 Řízení bezpečnosti informací

Tato kapitola specifikuje určitá pravidla pro řízení bezpečnosti informací v organizacích. „V *průběhu vývoje informačních technologií vzrostlo povědomí, že informace jsou nejdůležitějším strategickým zdrojem, který musí každá organizace spravovat. Růstu tohoto povědomí se současně přizpůsobovala pravidla, která určují např. postavení* informatiky v *organizační struktuře organizací, hlavní cíle řízení informačních systémů, odpovědnosti za jednotlivé procesy informatiky, metody pořizování a provozu informačních systémů apod.“* (Doucek a kol., 2011, s. 52)

2.6.1 Koncepce řízení informatiky v organizacích

Současný pohled na postavení a řízení informatiky v organizacích reprezentují dvě koncepce řízení:

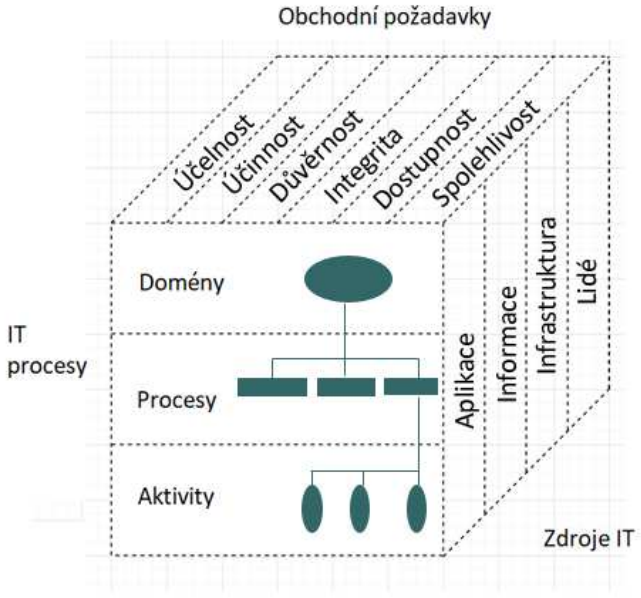
- správa a řízení IT (IT Governance),
- řízení IT služeb (IT Service Management).

Obě tyto koncepce se navzájem doplňují, a to především v praxi. Koncepce řízení IT služeb se zaměřuje na taktickou a operativní rovinu a cílem této koncepce je poskytování kvalitních IT služeb. Správa a řízení IT reprezentuje širší pojetí zaměřené na strategická hlediska jako propojení strategií, realizace hodnoty, řízení rizik informatiky, odpovědné řízení zdrojů informatiky a měření průběhu informatických procesů (Doucek a kol., 2011, s. 30, 52). Důležité pro organizaci je také tzv. řízení přístupu. Po autentizaci uživatele je třeba kontrolovat, která data jsou mu zpřístupněna. V tomto případě se jedná o komplexní systém řízení přístupu, který je zaveden a jsou rozlišeny různé stupně oprávnění uživatelů. O zařazení do skupin rozhoduje správce informačního systému. (Doseděl, 2004, str. 10)

2.6.2 Metodiky řízení informatiky v organizacích

Abychom mohli výše zmíněné koncepce řízení informatiky využívat, je nutné je podpořit vývojem standardů, rámců, metodik a nejlepších zkušeností (anglicky Best Practice). Podrobně se budeme zabývat rámcem ITIL a metodikou COBIT, které jsou obecné a světově rozšířené. Pan doktor Marek Rychlý (2015) ve svých přednáškách pro fakultu informatiky Vysokého učení technického v Brně také uvádí, že zkratka ITIL zahrnuje procesně orientovaný rámec pro správu a poskytování IT služeb v organizaci a popisuje, jak zavést odpovídající procesy, funkce a role. Tento rámec implementuje IT oddělení organizace a za každý jeho proces je odpovědný příslušný zaměstnanec (př. Security Manager). ITIL je tedy vhodné zařadit do IT Service Management, neboť se jedná o operativní řízení, stanovují se krátkodobé cíle a pomocí reaktivního řízení se zajišťují stabilní IT služby. V případě IT Governance je za pomoci spíše strategického a proaktivního řízení, stanovování dlouhodobých cílů či kontrol dosahováno evoluce IT služeb, tu zajišťují zejména ředitelé organizací a CEO. Tedy je využito řídícího rámce COBIT (Control Objectives for Information and Related Technology vydaný a udržovaný společností ISACA), který podporuje procesní řízení, je kombinovatelný s jinými

procesními rámce a je možno jej propojit s řadou standardů a legislativních předpisů. (Doucek a kol., 2011, str. 48-53)



Obrázek 2: COBIT kostka.
(Vlastní zpracování dle: Doucek a kol., 2011, str. 49)

2.6.3 Hodnocení bezpečnosti informací

Jako norma pro hodnocení bezpečnosti informačních technologií pak slouží kromě jiných také takzvaná Společná kritéria (anglicky Common Criteria). První verze těchto kriterií se objevila v lednu roku 1996 a byla přijata Mezinárodní organizací pro normalizaci (ISO) jako pracovní návrh. Další sadu norem nazvanou ISO/IEC 15408 a také řadu ISO/IEC 27000 využíváme dodnes. (Doucek a kol., 2011, str. 68-69, 83)

2.6.4 Bezpečnost z pohledu síťové struktury

Řízení bezpečnosti informací vyžaduje nejen správné řízení a strategii ale také celkovou bezpečnost na všech vrstvách modelu ISO/OSI. Fyzickou vrstvu zabezpečíme pomocí Managementu bezpečnosti pasivní vrstvy (NISS). Linkovou vrstvu můžeme chránit certifikáty, digitálním podpisem a bezpečnostními protokoly. Síťová vrstva využívá především firewall, VPN, IPsec nebo systémy IDS a IPS. Ostatní vrstvy již řeší aplikační bezpečnost, které dosáhneme pomocí řízení přístupu, autorizace, kryptografické bezpečnosti a mnoha dalších zabezpečení. (Ondrák a kol., 2013, str. 166-177)

„V síťové struktuře je občas zajímavé rozlišit tři zóny – zónu se zapojenými uživatelskými počítači, zónu se zapojenými servery a vnější síť.“ (Doseděl, 2004, str. 15)

„Specifická je především část sítě se servery, pro kterou se vžilo označení demilitarizova*ná zóna. Tyto servery musí být samozřejmě chráněny před útoky z vnějšího světa, dokonce přísněji než ostatní počítače. Jsou chráněny i proti útokům z místní sítě, mohou ale bez problémů komunikovat mezi sebou.“* (Doseděl, 2004, str. 15)

„K ochraně proti útokům na počítače připojené do sítě slouží dobře nakonfigurovaný firewall. Přenášená data nejlépe ochrání správně navržený komunikační protokol.“ (Doseděl, 2004, str. 12)

Tabulka 1: Některé komunikační protokoly
(Vlastní zpracování dle: Doseděl, 2004, str. 12)

Nezabezpečená verze protokolu	**Zabezpečená verze protokolu**	**Využití protokolu**
Remote shell (telnet)	Secure shell (SSH)	ovládání počítače, vzdálená správa
File Tranport Protocol	SecureFTP	přenos souborů
Hypertext Transport Protocol	SecureHTTP (s využitím SSL vrstvy)	webové stránky
POP, IMAP, SMTP	POP/IMAP – přes SSL, PGP, S/MIME	elektronická pošta
-	IPSec	tunelování
WiFi	WPA2	zabezpečení bezdrátových sítí

2.6.5 Analyzování bezpečnosti v organizaci

Pro analýzu využíváme systém řízení bezpečnosti informací (ISMS). Systém je postavený na modelu PDCA (Demingův model). Každý z jednotlivých prvků informačního systému má vliv na informační bezpečnost, proto je nutné nejprve provést dekompozici na určité úrovni, neboli vymezit jednotlivé prvky IS jako samostatné objekty s vlastnostmi a vazbami na ostatní prvky. Úroveň dekompozice závisí na rozsahu zkoumaného IS a také

na tom, jak vysoké nároky na bezpečnost jsou v IS kladeny. (Ondrák a kol., 2013, str. 14, 66)

Je důležité zabezpečit především tyto hlavní prvky bezpečnosti:

1) integrita (odpovědnost za správnost údajů),
2) důvěrnost (poskytnutí přístupu pouze oprávněným osobám),
3) dostupnost (zajištění přístupnosti informací v okamžiku potřeby pro oprávněné uživatele). (Ondrák a kol., 2013, str. 15)

„V systémech pro zpracování a přenos dat se musíme starat o bezpečnost a správnost dat a informací a o dodržování oprávněnosti přístupu k datům, resp. práva na soukromí, tedy ochranu osobních údajů.“ (Požár, 2007, Předmluva)

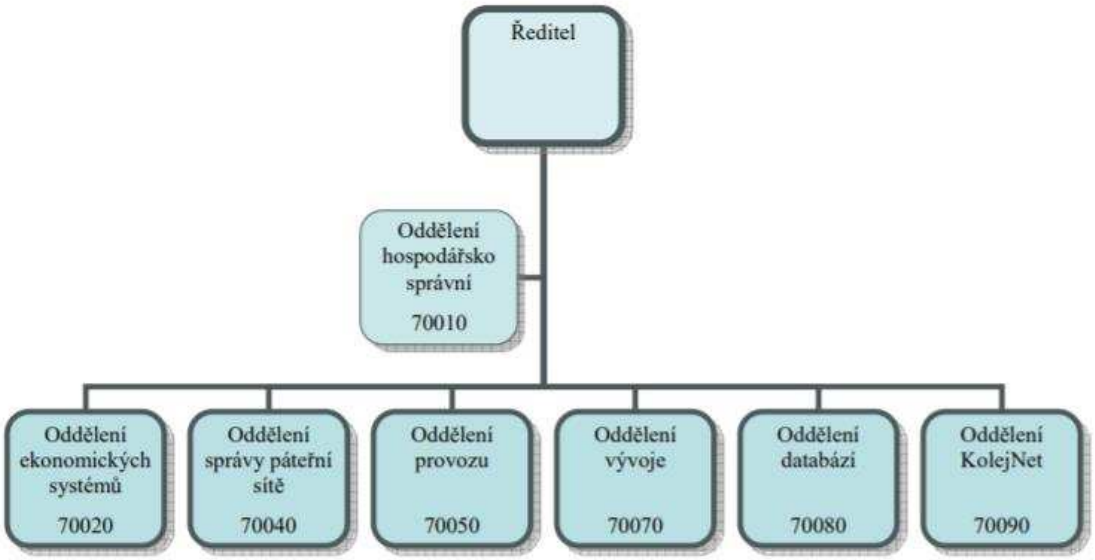
2.6.6 Přenesení odpovědnosti

Bezpečnost informací a její řízení není krátká jednorázová činnost, ale jedná se o dlouhodobou aktivitu. Hlavní aspekt je vývoj v čase. Na přelomu tisíciletí byly hlavními předměty zájmu komunikace a připojení k internetu a s tím spojené bezpečnostní hrozby, toto vše bylo ovlivněno novými zákonnými úpravami o zpracování dat (zákon na ochranu osobních údajů a zákon o utajovaných skutečnostech). V dnešní době patří mezi priority využívání informačních technologií na úřadech a při úředních postupech, využívání zaručeného elektronického podpisu a zisk kvalifikovaných pracovníků na trhu práce. Oblast řízení bezpečnosti informací také bezprostředně ovlivňují vnější faktory, jako je ekonomické a politické dění nejen ve státě, ale v celém světě. Tuto oblast ovlivňuje také rozšiřování a změny mezinárodních celosvětově uznávaných standardů. (Doucek a kol., 2011, str. 231) Před samotnou analýzou je důležité definovat, co přesně budeme v informačním systému hodnotit. Základním stavebním kamenem je jednotka informace, která je obsažena v datech různého druhu. Všechna tato data jsou však uložena v digitální neboli elektronické podobě ve zvoleném úložišti. Správu těchto dat zajišťuje osoba k tomu určená a pověřená, která má odborné znalosti v této oblasti. (Ondrák, 2017)

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Hodnocený informační systém

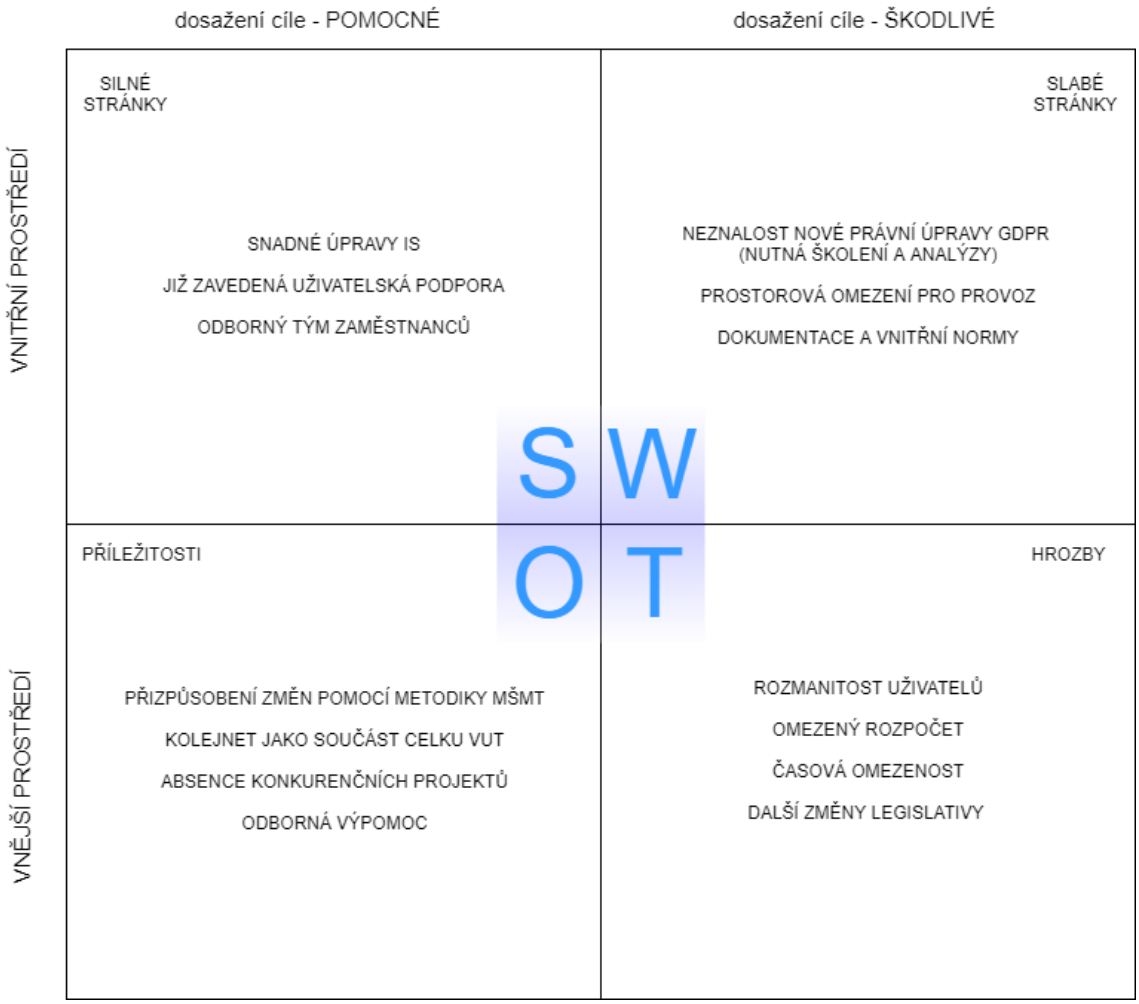
Elektronický informační systém KolejNet slouží ke zprostředkování služeb a správě kolejní sítě VUT v Brně, tento informační systém je navázán na informační systém Kolejí a Menz při VUT v Brně (dále jen KaM) a informační systém Vysokého učení technického v Brně, tyto dva systémy poskytují hodnocenému IS data. V roce 1994 vznikl předchůdce Listnet, následně v roce 1999 vznikl KolejNet jako součást technického oddělení KaM. Organizačně spadá oddělení KolejNet od roku 2005 pod Centrum výpočetních a informačních služeb VUT v Brně, které mimo jiné zajišťuje provoz a správu páteřní počítačové sítě, webových aplikací VUT, centrální databáze VUT a cloudových služeb pro VUT. Vztahy a řízení organizace upravuje Organizační řád VUT.



Obrázek 3: Organizační struktura CVIS
(Zdroj: Organizační řád CVIS, 2006)

Dle organizačního řádu CVIS, zajišťuje oddělení KolejNet také projekty rozvoje studentské počítačové sítě, provoz dohledové sítě nad aktivními prvky a servery studentské sítě a komerčního připojení do sítě KolejNet. Uživatelská data již zaměstnanci běžně zpracovávají (dle pravidel zákona 101/2000 Sb. o ochraně osobních údajů). KolejNet využívá také mnoho komunikačních protokolů. Za zmínku určitě stojí protokol SNMP (Simple Network Management Protocol), který slouží jako účinný nástroj pro

správu neboli management počítačové sítě. Informační systém KolejNetu je hierarchicky nastaven. Administrátorská práva jsou upravována podle pracovní pozice jednotlivých zaměstnanců. Pro interní komunikaci je také využíváno elektronické pošty, nejčastěji se využívá vlákno ve vlastní doméně, do kterého jsou přiřazeni všichni zaměstnanci oddělení, dále jsou schránky děleny podle areálů nebo pro jednotlivé zaměstnance a uživatele. Pro zabezpečenou vzdálenou správu je zavedena možnost připojení přes VPN (Virtual Private Network). Správa sítě je prováděna pomocí zabezpečených šifrovaných kanálů, skrze oddělenou síťovou infrastrukturu určenou pro správu sítě.



Obrázek 4: SWOT analýza pro IS KolejNet.
(Vlastní zpracování)

Na základě vstupní analýzy SWOT připravím v kapitole 4. této práce návrh nové dokumentace a školení, tento postup byl zvolen na základě snahy o vyloučení slabých stránek IS.

3.1.1 Požadavky investora

Požadavky investora (VUT v Brně) byly částečně sepsány do Metodického listu č. 5/2017 a také do Pokynu č. 6/2018 k zajištění implementace Nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR) na VUT. Jedná se především o zajištění administrativních a organizačních opatření, pomocí metodického a organizačního řízení.

3.1.2 Doplnění ePrivacy a Pracovní skupina WP29

Tato kapitola popisuje pojmy, jež by mohly být využity v kontextu s nařízením GDPR. K tomuto nařízení přibude také doplnění zvané ePrivacy Regulation (Nařízení o soukromí a elektronických komunikacích). Pokud uživatel neudělí souhlas se zpracováním osobních údajů, vznikne situace, kdy bude nutné, aby správce data anonymizoval nebo vymazal. Toto nařízení je především určeno pro elektronickou komunikaci mezi předem nedefinovaným počtem koncových uživatelů. Ochrana soukromí bude aplikována také na metadata. Metadata jsou strukturovaná data, popisující jiná data a informace, popř. jejich zdroj, jež obsahují webové stránky v hlavičce kódu. (Pomerantz, 2015, str. 85) Většina společnostní již v dnešní době využívá automatizované zpracování osobních údajů, údaje se tedy zpracovávají pomocí výpočetní techniky, často bez lidského zásahu. Z tohoto jasně vyplývá, že je žádoucí důkladně zabezpečit tyto systémy. Pojem WP29, Article 29 Working Party nebo Pracovní skupina 29, jako nezávislý evropský poradenský orgán na ochranu dat a soukromí, byl dříve stanoven článkem 29. směrnice 95/46/EC, nyní se však s účinností nařízení GDPR změní na Evropský sbor pro ochranu osobních údajů. Tento sbor bude fungovat jako nejvyšší dozorový orgán ve všech zemích EU. Dne 7. února 2018 byla zvolena nová předsedkyně WP29 Andrea Jelinek. (EDPS, 2017)

3.1.3 Fyzická bezpečnost

Fyzická bezpečnost celého systému představuje v oddělení KolejNet významnou roli. Vzhledem k velkému počtu prvků, které tuto bezpečnost zajišťují byla vytvořena následující tabulka, která ukazuje kategorie kritérií fyzické bezpečnosti a jak jsou splněny v hodnoceném IS.

Tabulka 2: Kritéria fyzické bezpečnosti
(Vlastní zpracování dle: Ondrák a kol., 2013, str. 289-292)

vhodná lokalizace pro sídlo organizace	ANO
splnění elektrotechnických předpisů	ANO
splnění požárních předpisů	ANO
zabezpečení klíčových prostor	ANO
vhodné prostředí pro provoz informační a komunikační techniky	ANO
dostatečné označení a dokumentace	ANO
používání kvalitních materiálů, komponent a prvků splňujících standardy	ANO
dodavatelský servis a pojištění	ANO
pravidelné řízené zálohování	ANO
redundance (STP, MRP…)	ANO
správné rozdělení sítě (intranet, DMZ, VLAN…)	ANO
ochrana na rozhraní bezpečnostních zón a VLAN	ANO
ochrana koncových zařízení (uživatelských)	NE
ochrana sítě před uživatelem, ochrana vzdáleného přístupu (SSH, VPN – SSL)	ANO
použití zabezpečených služeb (HTTPS, SMTPS)	ANO
správa sítě a ochrana paměťových medií	ANO
dohledové systémy a bezpečné směrování	ANO
splnění předpisů OHASMS (dříve BOZP) a vyhlášky 50/1978 Sb.	ANO
minimalizace přístupových oprávnění	ANO
dokumentace, právní prostředí a školení	ANO

3.1.4 Datový tok

V hodnoceném informačním systému jsou data a z nich získané informace nenahraditelným zdrojem. Z počátku jsou využita data převedená z jiné databáze, a to k vytvoření podkladu pro následnou správnou autentizaci uživatele do informačního systému. Tedy nelze provoz zajistit jinými prostředky. Každé použití výpočetního systému (včetně testů) je nutné zabezpečit proti úniku dat a je nutné vést záznam o zpracování, který musí být uložen. Tímto dojde k mapování toku dat. V IS KolejNet toto z části zajišťují výpisy jednotlivých zařízení v síti tzv. logy. V případě uživatelských údajů jsou importovaná data využita k plnění smlouvy o poskytování služeb uživatelům

a jsou zpracovávána pouze na základě uděleného souhlasu. Oddělení KolejNet využívá pro komunikaci s uživateli elektronickou poštu. Při komunikaci v zásadních událostech, jako jsou změny uložených údajů, resetování hesla pro přístup do informačního systému, pomoc při registraci uživatelské přípojky a jiné, využívá oddělení KolejNet osobního styku zaměstnance s uživatelem, přičemž na vyžádání je uživatel povinen doložit svou totožnost, a to průkazem s fotografií. Toto ověření slouží především k zajištění integrity dat, ale také jako bezpečnostní opatření.

3.1.5 Kategorie subjektu osobních údajů

Kategorie subjektů údajů určené v tabulce jsou skupiny vlastníků osobních údajů, jejichž údaje oddělení KolejNet zpracovává. Počet uživatelů sítě kolísá v průběhu roku, proto nelze přesněji specifikovat jejich počet.

Tabulka 3: Kategorie subjektů údajů
(Vlastní zpracování)

Název kategorie	Odhadovaný počet prvků ve skupině
Uživatel KolejNet	obvykle více jak 7 000 během školního roku
Zaměstnanec KolejNet	11 + externí zaměstnanci

3.1.6 Osobní údaje

Pro jednotlivé kategorie nyní uvedeme osobní údaje, které jsou relevantní pro zpracovávání. Zdrojem těchto dat je databáze KaM VUT nebo centrální databáze VUT. Osobní údaje **uživatelů** jsou nejčastěji získány z databáze ubytovaných KaM. Přístup k těmto údajům mají v daném rozsahu jednotlivý uživatelé (ke svým vlastním údajům), v omezeném rozsahu všichni uživatelé (pomocí pole vyhledávání, zobrazují se atributy jméno, příjmení, přihlašovací jméno, e-mail, číslo bloku, číslo pokoje) a dále zaměstnanci s oprávněními dle pracovní pozice. Tato data mohou být zpracovávána jak samotným uživatelem, tak také zaměstnanci KN, CVIS či KaM, přičemž účel zpracování je plnění smlouvy o poskytování služeb a následná správa těchto služeb. Data jsou uložena po dobu 10 let od prvního ubytování na kolejích VUT, dle povinnosti uschování záznamů pro vedení účetnictví (dle zákona o účetnictví č. 563/1991). Pokud již uživatel aktivně nevyužívá služby je jeho účet uzamknut. Účet uživatele je možné znovu odemknout, pokud jsou osobní profily po porovnání identické.

Tabulka 4: Osobní údaje uživatelů
(Vlastní zpracování)

Uživatel sítě KolejNet
Jméno
Příjmení
Rodné číslo
Login
UID
VUT ID (centrální databáze VUT)
Kontaktní e-mail (nepovinná položka)
E-mail (v doméně kn.vutbr.cz)
IP adresa (jedna nebo více než jedna)

Identita uživatele sítě KolejNet je skryta pod síťovým identifikátorem (adresa internetového protokolu neboli IP adresa), pod přihlašovacím jménem (login) a také pod KolejNet UID (identifikátor uživatele KolejNet), avšak lze ji zpětně dohledat. Tato IP adresa je vždy přidělena z rozsahu dle typu připojení do sítě, v rozdělení na bezdrátové připojení k Wi-Fi síti KolejNet nebo kabelové připojení. Dále je také síť dělena na menší celky, z důvodu přehlednosti a manipulace s daty, a to dle umístění (na jednotlivé reálné areály kolejí VUT a areály KaM aj.) nebo dle využití (např. komerční zákazníci nebo studenti). Tyto identifikátory jsou stejně jako MAC adresy, využívány v informačním systému při většině činností. Slouží v administraci sítě a monitorování provozu na síti nebo mimo jiné, zaměstnanci k dohledání činitele při prohřešku v síti (porušení autorských práv, útok skrze infikované PC atd.). Důležitou informací je, že IP adresy se mohou stát jednoznačným identifikátorem osoby pouze pokud je osoba registrována do sítě KolejNet. Pokud již není vedena v informačním systému není možné přiřadit tuto adresu IP uživateli.

Tabulka 5: Příklad přidělovaných IP adres pro vybrané areály kolejí, kabelové připojení.
(Vlastní zpracování)

název	IP Síť	Maska podsítě	Broadcast
a03	147.229.212.0/22	255.255.252.0	147.229.215.255
a04	147.229.216.0/22	255.255.252.0	147.229.219.255

název	IP Síť	Maska podsítě	Broadcast
a05	147.229.220.0/22	255.255.252.0	147.229.223.255
man	147.229.206.0/23	255.255.254.0	147.229.207.255
list	147.229.200.0/22	255.255.252.0	147.229.203.255

Všechna **zaměstnanecká** data jsou uložena v databázi KN, obvykle jsou tato data sbírána z různých databází. Přístup k datům zveřejněných v IS má vždy zaměstnanec sám a také ostatní zaměstnanci, dle pracovní pozice jsou přidělena oprávnění pro manipulaci s těmito daty v zásadě přes webové rozhraní. Účelem zpracování je vytvoření potřebného základu pro navázání a udržení pracovního poměru, odměňování a také umožnění výkonu práce. Výše zmíněná data jsou uložena po dobu platnosti pracovního poměru. I zde jsou účty uzamykány.

Tabulka 6: Osobní údaje zaměstnanců
(Vlastní zpracování)

Zaměstananec sítě KolejNet
Jméno
Příjmení
Rodné číslo
Login
UID
VUT ID (centrální databáze VUT)
Kontaktní e-mail (nepovinná položka)
E-mail (v doméně kn.vutbr.cz)
IP adresa (jedna nebo více než jedna)

3.1.7 Kategorie osobních údajů

Jednotlivé osobní údaje rozřadíme do kategorií osobních údajů, které jsme stanovili v kapitole 2.2 Osobní údaje. Z obou tabulek pak vyplývá, že oddělení KolejNet nezpracovává žádné citlivé osobní údaje, které bychom mohli zařadit do kategorie zvláštní osobní údaje a které vyžadují výrazně důkladnější zabezpečení.

Tabulka 7: Uživatelé, kategorie jednotlivých osobních údajů
(Vlastní zpracování)

Uživatel sítě KolejNet	Kategorie
Jméno	obecný osobní údaj
Příjmení	obecný osobní údaj
Rodné číslo	obecný osobní údaj
Login	obecný osobní údaj
UID	obecný osobní údaj
VUT ID (centrální databáze VUT)	obecný osobní údaj
Kontaktní e-mail	obecný osobní údaj
E-mail (v doméně kn.vutbr.cz)	obecný osobní údaj
IP adresa (jedna nebo více než jedna)	obecný osobní údaj

Tabulka 8: Zaměstnanci, kategorie jednotlivých osobních údajů
(Vlastní zpracování)

Zaměstnanec sítě KolejNet	Kategorie
Jméno	obecný osobní údaj
Příjmení	obecný osobní údaj
Rodné číslo	obecný osobní údaj
Login	obecný osobní údaj
UID	obecný osobní údaj
OID	obecný osobní údaj
VUT ID (centrální databáze VUT)	obecný osobní údaj
Kontaktní e-mail	obecný osobní údaj
E-mail (v doméně kn.vutbr.cz)	obecný osobní údaj
IP adresa (jedna nebo více než jedna)	obecný osobní údaj

3.1.8 Správce a zpracovatel osobních údajů

Je velmi složité určit pro jednotlivé prvky pozice dle právní úpravy. Hodnocené oddělení je vzhledem ke svým zaměstnancům a jejich osobním údajům správcem osobních údajů, neboť je součástí VUT a tato vazba platí také ve vztahu k uživatelům sítě. Nadřízeným správcem je pak VUT v Brně.

3.2 Analýza ISMS

Následně provedeme „posouzení vlivu“ na ochranu osobních údajů pro zpracování s vysokým rizikem (DPIA Data Protection Impact Assesment), tedy analýzu rizik, kde hodnotíme porušení dostupnosti, integrity, důvěrnosti a ztráty. Použijeme klasifikační schéma, které ke každému prvku přiřazuje klasifikační stupeň dle zvoleného měřítka. Toto měření je nutné provést obousměrně, tedy z pohledu uživatele, kdy je možnost, že narušení integrity či zabezpečení dat může způsobit např. zveřejnění osobních údajů, ale také z pohledu správce dat/zaměstnavatele/osoby odpovědné za tato data, kdy je tento prvek vystaven nebezpečí neoprávněného vniknutí do IS a manipulaci s daty, což může vést k vysoké peněžní sankci. Je tedy důležité zabezpečit IS a data, která zpracovává, ale také je nutné poučit uživatele jakožto subjekt osobních údajů.

ISMS (Information Security Managemet System) neboli systém řízení bezpečnosti informací, jehož rozsah udávají skupiny aktiv (Assets) různého druhu, je dokumentovaný systém řízení informační bezpečnosti a zároveň je strategickým rozhodnutím vedení společnosti. (Ondrák a kol., 2013, str. 66)

Rozdělení IS dle jeho využití:

- hardware

(koncová zařízení uživatelů, strukturovaná kabeláž, aktivní prvky, organizéry, datové rozvaděče s vybavením, UPS,…)

- software

(samotný informační systém, konfigurace aktivních prvků, znalosti zaměstnanců,…)

- údaje

(data o uživatelích, zaměstnancích, a jiné…, uložená v databázi)

- lidská složka

(zaměstnanci, studenti a osoby s přístupovými právy k IS KolejNet)

- organizační uspořádání

(Nařízení správce sítě, pravidla provozu sítě a pravidla správy sítě, předpisy BOZP, pravidla použití IS…)

Informační systém musí poskytovat data uživatelům a vést jejich evidenci, zprostředkovat přístup k registraci uživatelské přípojky, zobrazovat aktuální evidované informace a umožnit jejich úpravu a další operace. Je nutné zabezpečit všechny části IS, a to především již zmíněná aktiva, která budou hodnocena v následující kapitole této práce. V praxi je již zavedeno zabezpečení IS, které je využíváno v provozu a je následující: existuje šifrované spojení mezi servery připojené v síti, šifrování je použito také u webových stránek IS. Datová úložiště se nacházejí v privátní síti bez připojení do vnější sítě (Internetu). Fyzicky jsou jednotlivé prvky sítě umístěny v serverových místnostech v prostorách KaM (v několika lokalitách) s přístupovým systémem EZS s pultem centrální ochrany.

3.2.1 Identifikace aktiv

V této kapitole rozpoznáme jednotlivá aktiva IS KolejNet. V každém případě je naším cílem důsledně zabezpečit IS pomocí realizace analýzy informačních aktiv a předejít tak vzniku bezpečnostních hrozeb nebo následné bezpečnostní události či bezpečnostnímu incidentu. Následující tabulka udává zjištěné aktivum a jeho vlastníka. Vlastníka je nutné určit z důvodu definování jednoznačné odpovědnosti za hodnocené aktivum z hlediska funkčnosti, údržby, opravy a bezpečnosti aktiva. (Ondrák a kol, 2013, str. 82)

Tabulka 9: Aktiva v IS KolejNet.
(Vlastní zpracování)

NÁZEV AKTIVA	VLASTNÍK AKTIVA
databáze Kolejnet (MySQL, PgSQL)	Petr Herman Studený Stanislav
Pravidla provozu počítačové sítě KolejNet	Petr Herman
Pravidla provozu sítě KolejNet pro komerční uživatele	Petr Herman
Pravidla správy počítačové sítě (platná pro celé VUT)	rektor VUT
Pravidla provozu elektronické pošty sítě KolejNet	Petr Herman
Prohřeškový řád sítě KolejNet	Petr Herman
Nařízení správce sítě 1/2015	Petr Herman
Upozornění správce sítě 1/2011	Petr Herman
Zabbix (dohledový systém)	Petr Herman

NÁZEV AKTIVA	VLASTNÍK AKTIVA
vnitřní IS2 (správa sítě)	Petr Herman
logy a testy (switch, test MAC, WiFi AP, ArpWatch, import KaM)	Petr Herman
webMail	Petr Herman
uživatelské zařízení (PC, notebook, mobilní telefon…)	konkrétní uživatel
strukturovaná kabeláž	Petr Herman správci jednotlivých areálů
úložná media	Petr Herman
UPS	Petr Herman
aktivní prvky a příslušenství	Petr Herman
kancelářský nábytek	Petr Herman
rackové skříně s patchpanely a organizéry a příslušenství	Petr Herman
energie a služby	Koleje a menzy VUT
klimatizace	Koleje a menzy VUT
zaměstnanci KolejNet	Petr Herman
uživatelé sítě KolejNet (včetně komerčních uživatelů)	konkrétní uživatel
komerční uživatelé KolejNet	konkrétní komerční uživatel
zaměstnanci KaM VUT	KaM
dostupnost	Petr Herman

3.2.2 Klasifikace aktiv

Klasifikace aktiv znamená předběžné zařazení do jednotlivých skupin aktiv podle předem definovaných klasifikačních kritérií. Tyto kritéria a také klasifikační stupně využíváme v klasifikačním schématu. Pro klasifikaci aktiv lze využít také softwarové programy jako CRAMM nebo RAMSES. Při hodnocení dostupnosti, integrity a důvěrnosti budeme využívat následující tři klasifikační schémata, první schéma slouží pro hodnocení podílových prvků dle významnosti pro organizaci, druhé schéma je sestaveno pro ohodnocení důvěrnosti a poslední schéma poslouží pro celkové zhodnocení. (Ondrák a kol. 2013, str. 33, Ondrák 2017) Tabulka č. 13 následně ohodnocuje jednotlivá aktiva s využitím předchozích schémat.

Tabulka 10: Klasifikační schéma pro podílové prvky
(Vlastní zpracování dle: Ondrák a kol., 2013, str. 82)

Klasifikační stupeň	Klasifikační kritérium
1	Zanedbatelné pro organizaci
2	Méně důležité pro organizaci
3	Středně důležité pro organizaci
4	Důležité pro organizaci
5	Velmi důležité pro organizaci

Tabulka 11: Klasifikační schéma důvěrnosti
(Vlastní zpracování dle: Ondrák a kol., 2013, str. 82)

Klasifikační stupeň	Klasifikační kritérium
1 - Veřejné (Public)	informace je určena pro širokou veřejnost
2 - Interní (Internal)	informace je určena pouze pro zaměstnance dané společnosti a přístup k ní mají jen zaměstnanci dané společnosti
3 - Důvěrné (Confidential)	nežádoucí zpřístupnění těchto informací může mít negativní dopad na společnost (informace o projektech, plánovaných změnách, vývoji cen)
4 - Soukromé (Private)	nežádoucí zpřístupnění těchto informací může mít negativní dopad na společnost (osobní údaje o zaměstnancích a klientech)
5 – Přísně důvěrné (Top confidential)	nejvyšší stupeň, nežádoucí zpřístupnění těchto informací může mít zničující dopad na společnost (strategické plány, zdrojové kódy)

Tabulka 12: Klasifikační schéma celkové
(Vlastní zpracování dle: Ondrák a kol., 2013, str. 82)

Klasifikační stupeň	Klasifikační kritérium
1	Žádný dopad na IS KolejNet
2	Zanedbatelný dopad na IS KolejNet
3	Potíže či finanční ztráty
4	Vážné potíže či podstatné finanční ztráty
5	Existenční potíže

Tabulka 13: Klasifikace jednotlivých aktiv.
(Vlastní zpracování)

Kategorie aktiv	Název aktiva	Dostupnost	Integrita	Důvěrnost	Celkově
Informační aktiva					
	Databáze Kolejnet (MySQL, PgSQL)	5	5	5	**5**
	Pravidla provozu počítačové sítě KolejNet	2	4	1	**2**
	Pravidla provozu sítě KolejNet pro komerční uživatele	2	4	1	**2**
	Pravidla správy počítačové sítě (platná pro celé VUT)	2	4	2	**3**
	Pravidla provozu elektronické pošty sítě KolejNet	2	4	1	**2**
	Prohřeškový řád sítě KolejNet	2	3	1	**2**
	Nařízení správce sítě 1/2015	2	3	1	**2**
	Upozornění správce sítě 1/2011	2	3	1	**2**
Aplikační aktiva					
	Zabbix (dohledový systém)	3	4	4	**4**
	Vnitřní IS2 (správa sítě)	4	5	4	**4**
	Logy a testy (switch, test MAC, WiFi AP, ArpWatch, import KaM)	4	5	4	**4**
	WebMail	4	5	4	**4**
Fyzická aktiva					
	Uživatelské zařízení (PC, notebook, mobilní telefon…)	1	3	2	**2**
	Strukturovaná kabeláž	4	3	3	**3**
	Úložná media	4	3	3	**3**
	UPS	3	3	3	**3**
	Aktivní prvky a příslušenství	4	4	3	**4**
	Kancelářský nábytek	4	3	3	**3**
	Rackové skříně s patchpanely a organizéry a příslušenství	3	2	1	**2**
Služby					
	Energie	4	2	2	**3**
	Klimatizace	4	2	2	**3**
	Napájení	5	4	4	**4**
Lidská aktiva					
	Zaměstnanci KolejNet	4	4	4	**4**
	Uživatelé sítě KolejNet (včetně komerčních uživatelů)	3	2	2	**2**
	Komerční uživatelé KolejNet	3	2	2	**2**
	Zaměstnanci KaM VUT	3	3	2	**3**
Nehmotná aktiva					
	dostupnost	4	4	4	**4**

3.2.3 Identifikace zranitelností aktiv

V této kapitole identifikujeme slabiny zjištěných aktiv. Bezpečnostní hrozba využije zranitelnost jako prostředek k napáchání škody. Zranitelnost určuje vlastnost aktiva, způsob užití aktiva, vada aktiva nebo špatné užití aktiva v informačním systému. Samotný výskyt zranitelnosti nutně neznamená napáchání škody, proto je nutná existence hrozby, která ho využije. (Ondrák, 2013, str. 93)

Tabulka 14: Klasifikační schéma pro zranitelnost
(Vlastní zpracování dle: Ondrák a kol., 2013, str. 82)

klasifikační kritérium	Klasifikační stupně
všeobecně známá zranitelnost, napadení bez odborných znalostí	4 - kritická zranitelnost
všeobecně známá zranitelnost, napadení s odbornou znalostí	3 – vysoká zranitelnost
vyžaduje útočníka v síti	2 - střední zranitelnost
je nutný fyzický přístup k aktivu	1 - nízká zranitelnost

Tabulka 15: Hodnocení zranitelnosti aktiv
(Vlastní zpracování)

Informační aktiva	**Zranitelnost**
Databáze Kolejnet (MySQL, PgSQL)	2
Pravidla provozu počítačové sítě KolejNet	1
Pravidla provozu sítě KolejNet pro komerční uživatele	1
Pravidla správy počítačové sítě (platná pro celé VUT)	1
Pravidla provozu elektronické pošty sítě KolejNet	1
Prohřeškový řád sítě KolejNet	1
Nařízení správce sítě 1/2015	1
Upozornění správce sítě 1/2011	1
Aplikační aktiva	
Zabbix (dohledový systém)	2
Vnitřní IS2 (správa sítě)	2
Logy a testy	2
WebMail	2

Fyzická aktiva	**Zranitelnost**
Uživatelské zařízení (PC, notebook, mobilní telefon…)	3
Strukturovaná kabeláž	4
Úložná media	1
UPS	1
Aktivní prvky a příslušenství	4
Kancelářský nábytek	1
Rackové skříně s patchpanely a organizéry a příslušenství	1
Služby	
Energie	1
Klimatizace	1
Napájení	1
Lidská aktiva	
Zaměstnanci KolejNet	3
Uživatelé sítě KolejNet (včetně komerčních uživatelů)	2
Komerční uživatelé KolejNet	2
Zaměstnanci KaM VUT	3
Nehmotná aktiva	
dostupnost	2

Z tabulky je zřejmé, že pro napadení IS je obvykle nutné se pohybovat v síti KolejNet popř. v síti VUT, nejvíce nezabezpečené jsou Wi-Fi Access Point (přístupové body) s příslušenstvím, které jsou aplikovány na chodbách budov kolejí VUT nebo na jednotlivých uživatelských pokojích. I přesto, že je přístupový bod zabezpečen plastovou krabicí a zabezpečovací samolepkou (bezpečnostní plombou), je násilný fyzický přístup k tomuto zařízení možný, přístup nelze více omezit, protože by nebyla zajištěna dostupnost signálu. Kontrolu zajišťují Wi-Fi AP logy (výpisy z provozu přístupového bodu). Takto umístěné přístupové body mají označení, že není možné nainstalovaný prvek provozovat bez jiného centrálního řídícího prvku. Stejně tak je možný přístup k části strukturované kabeláže, která je vedená k datové zásuvce nástěnnou lištou. Nejčastěji hrozí zničení nebo odcizení. Pro omezení bezpečnostního rizika je provoz přístupových bodů v oddělené síti, bez přímého připojení na kritická místa sítě.

AP 162	d02-2np-ap3	BC:EA:FA:D1:67:A0	online	10.188.0.162	10.188.0.162	BC:EA:FA:D1:67:A0	190434200	22 days, 0:59:02.00
AP 163	d02-2np-ap4	BC:EA:FA:D1:97:20	online	10.188.0.163	10.188.0.163	BC:EA:FA:D1:97:20	190435700	22 days, 0:59:17.00
AP 164	d02-2np-ap5	BC:EA:FA:D1:51:A0	online	10.188.0.164	10.188.0.164	BC:EA:FA:D1:51:A0	190435800	22 days, 0:59:18.00
AP 165	d02-1np-ap1	BC:EA:FA:D1:68:C0	online	10.188.0.165	10.188.0.165	BC:EA:FA:D1:68:C0	190435100	22 days, 0:59:11.00
AP 166	a06-2np-pizz-ap1	BC:EA:FA:D1:6D:20	online	10.188.0.166	10.188.0.166	BC:EA:FA:D1:6D:20	154746200	17 days, 21:51:02.00
AP 167	a06-2np-menz-ap1	BC:EA:FA:D1:6C:A0	online	10.188.0.167	10.188.0.167	BC:EA:FA:D1:6C:A0	154746400	17 days, 21:51:04.00
AP 168	a06-3np-ubyt-ap1	BC:EA:FA:D1:5C:A0	online	10.188.0.168	10.188.0.168	BC:EA:FA:D1:5C:A0	154746500	17 days, 21:51:05.00
AP 169	r01-1np-cukr-ap1	BC:EA:FA:D1:68:20	online	185.62.108.130	10.20.16.10	BC:EA:FA:D1:68:20	222223900	25 days, 17:17:19.00
AP 170	arch-2np-sal-ap205	BC:EA:FA:D1:69:60	online	10.188.0.170	10.188.0.170	BC:EA:FA:D1:69:60	336541900	38 days, 22:50:19.00
AP 171	arch-2np-kancl-ap226	BC:EA:FA:D1:2D:20	online	10.188.0.171	10.188.0.171	BC:EA:FA:D1:2D:20	336540900	38 days, 22:50:09.00
AP 172	arch-3np-kancl-ap307	BC:EA:FA:D1:69:40	online	10.188.0.172	10.188.0.172	BC:EA:FA:D1:69:40	336540300	38 days, 22:50:03.00
AP 173	k67a-1np-zase-ap103	00:00:00:00:00:00	offline					
AP 174	u1-2np-uiak-ap1	BC:EA:FA:D1:48:A0	online	147.229.0.135	147.229.0.135	BC:EA:FA:D1:48:A0	559015700	64 days, 16:49:17.00
AP 175	arch-1np-badat-ap104	BC:EA:FA:D1:68:80	online	10.188.0.175	10.188.0.175	BC:EA:FA:D1:68:80	336541900	38 days, 22:50:19.00
AP 176	k67a-1np-zase-ap128	BC:EA:FA:D1:6B:80	online	147.229.0.133	147.229.0.133	BC:EA:FA:D1:6B:80	559015600	64 days, 16:49:16.00
AP 177	k67a-2np-uceb-ap205	00:00:00:00:00:00	offline					
AP 178	k67a-2np-uceb-ap212	00:00:00:00:00:00	offline					
AP 179	k67a-2np-uceb-ap220	00:00:00:00:00:00	offline					
AP 180	k67a-2np-uceb-ap227	00:00:00:00:00:00	offline					
AP 194	a02-2np-ap202	2C:23:3A:62:49:80	online	10.188.0.194	10.188.0.194	2C:23:3A:62:49:80	337358900	39 days, 1:06:29.00
AP 195	a02-2np-ap205	2C:23:3A:62:49:E0	online	10.188.0.195	10.188.0.195	2C:23:3A:62:49:E0	337357100	39 days, 1:06:11.00
AP 196	a02-2np-ap206	2C:23:3A:62:4A:80	online	10.188.0.196	10.188.0.196	2C:23:3A:62:4A:80	337356800	39 days, 1:06:08.00
AP 197	a02-2np-ap209	2C:23:3A:62:4A:A0	online	10.188.0.197	10.188.0.197	2C:23:3A:62:4A:A0	337358900	39 days, 1:06:29.00
AP 198	a02-2np-ap212	2C:23:3A:62:4B:00	online	10.188.0.198	10.188.0.198	2C:23:3A:62:4B:00	337357300	39 days, 1:06:13.00
AP 199	a02-2np-ap215	2C:23:3A:62:4B:20	online	10.188.0.199	10.188.0.199	2C:23:3A:62:4B:20	337356300	39 days, 1:06:03.00
AP 200	a02-2np-ap216	2C:23:3A:62:1C:C0	online	10.188.0.200	10.188.0.200	2C:23:3A:62:1C:C0	337356600	39 days, 1:06:06.00
AP 201	a02-2np-ap219	2C:23:3A:62:1D:00	online	10.188.0.201	10.188.0.201	2C:23:3A:62:1D:00	337356900	39 days, 1:06:09.00
AP 202	a02-2np-ap222	2C:23:3A:62:1D:40	online	10.188.0.202	10.188.0.202	2C:23:3A:62:1D:40	337358100	39 days, 1:06:21.00
AP 203	a02-2np-ap225	2C:23:3A:62:1E:20	online	10.188.0.203	10.188.0.203	2C:23:3A:62:1E:20	337358600	39 days, 1:06:26.00
AP 204	a02-2np-ap226	2C:23:3A:62:1E:40	online	10.188.0.204	10.188.0.204	2C:23:3A:62:1E:40	337357200	39 days, 1:06:12.00
AP 205	a02-2np-ap229	2C:23:3A:62:1F:00	online	10.188.0.205	10.188.0.205	2C:23:3A:62:1F:00	337352700	39 days, 1:05:27.00
AP 206	a02-2np-ap232	2C:23:3A:62:1F:40	online	10.188.0.206	10.188.0.206	2C:23:3A:62:1F:40	337355500	39 days, 1:05:55.00
AP 207	a02-2np-ap235	2C:23:3A:62:1F:60	online	10.188.0.207	10.188.0.207	2C:23:3A:62:1F:60	337356600	39 days, 1:06:06.00

Obrázek 5: Výpisy z přístupových bodů, děleno dle místa výskytu AP.
(Vlastní zpracování)

V případě oddělení KolejNet jsou výpisy (logy) ukládány jako textové soubory, zvolená varianta je vhodná z hlediska jednoduchosti zpracování.

„Samotné vytvoření logů je zbytečné, pokud nenásleduje jejich důkladná analýza.“ (Doseděl, 2004, str. 83)

Zaměstnanci KolejNet a KaM tvoří další skupinu ohrožující analyzovaný informační systém. Skupina zaměstnanců KolejNet je tvořena pracovníky s odbornou znalostí informačních technologií. Přístupová práva jsou hierarchicky stanovována podle pracovní pozice, individuálně, jednotlivým pracovníkům. Odpovědnost je stanovena dle pozice pracovníka. Skupina pracovníků KaM je většinou pouze poučena o funkčnosti a funkcích informačního systému KolejNet. Nejčastěji je narušena integrita dat (data jsou špatně vyplněna do formulářů) a tím je způsobeno snížení dostupnosti, jelikož správná data nejsou k dispozici v době, kdy je potřeba s nimi manipulovat.

3.2.4 Identifikace možných bezpečnostních incidentů

Bezpečnostní incident můžeme definovat jako případ selhání bezpečnosti. Pro IS je velmi vhodné stanovit (pomocí vnitřních norem organizace) formální řešení bezpečnostních incidentů. (Ondrák a kol., 2013, str. 346) Tyto incidenty mají různý dopad na organizaci (přímý/nepřímý), ve zkoumaném IS by se nejčastěji mohlo jednat o materiální a následné finanční ztráty či poškození. Tabulka č. 16 dále ukazuje možné bezpečnostní incidenty pro jednotlivá aktiva.

Tabulka 16: Bezpečnostní incidenty

(Vlastní zpracování)

Informační aktiva	Bezpečnostní incident
Databáze Kolejnet (MySQL, PgSQL)	data uživatelů byla po útoku zveřejněna
Pravidla provozu počítačové sítě KolejNet	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Pravidla provozu sítě KolejNet pro komerční uživatele	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Pravidla správy počítačové sítě (platná pro celé VUT)	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Pravidla provozu elektronické pošty sítě KolejNet	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Prohřeškový řád sítě KolejNet	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Nařízení správce sítě 1/2015	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Upozornění správce sítě 1/2011	tištěná verze byla fyzicky poškozena nebo byla porušena integrita dat z důvodu neaktuálnosti nařízení
Aplikační aktiva	
Zabbix (dohledový systém)	neoprávněný přístup k datům narušil integritu dat, dostupnost byla omezena DDoS útokem, důvěrnost dat byla omezena prodejem dat další straně
Vnitřní IS2 (správa sítě)	neoprávněný přístup k datům narušil integritu dat, dostupnost byla omezena DDoS útokem, důvěrnost dat byla omezena prodejem dat další straně
Logy a testy	neoprávněný přístup k datům narušil integritu dat, dostupnost byla omezena DDoS útokem
WebMail	neoprávněný přístup k datům narušil integritu dat, dostupnost byla omezena DDoS útokem, důvěrnost dat byla omezena prodejem dat další straně, bylo narušeno filtrování elektronické pošty (koncentrace příchozího spamu).
Fyzická aktiva	
Uživatelské zařízení (PC, notebook, mobilní telefon…)	zařízení je infikováno a útočník má neoprávněný přístup do IS, hrozí porušení integrity, dostupnosti i důvěrnosti dat
Strukturovaná kabeláž	neoprávněná manipulace způsobila poškození nainstalované kabeláže
Úložná media	neoprávněný fyzický přístup k mediu způsobil ztrátu dat
UPS	neoprávněný přístup k zařízení umožnil zničení zařízení, z důvodu nedostatku údržby došlo k úplnému vybití akumulátoru
Aktivní prvky a příslušenství	neoprávněný fyzický přístup k aktivním prvkům a jejich poničení narušilo provoz počítačové sítě
Kancelářský nábytek	neoprávněný přístup do kanceláří umožnil poničení nábytku
Rackové skříně s patchpanely, organizéry a příslušenství	neoprávněný přístup do serverovny umožnil mechanické zničení fyzických částí počítačové sítě, omezení či úplné omezení dostupnosti
Služby	
Energie	aktivum bylo mechanicky porušeno, neplní svůj funkční účel
Klimatizace	aktivum bylo mechanicky porušeno, neplní svůj funkční účel
Napájení	aktivum bylo mechanicky porušeno, neplní svůj funkční účel
Lidská aktiva	
Zaměstnanci KolejNet	zaměstnanci neodborně manipulují s prvky počítačové sítě nebo neodborně zasahují do IS
Uživatelé sítě KolejNet (včetně komerčních uživatelů)	hrozí fyzické zničení prvků počítačové sítě nebo šíření škodlivého softwaru s využitím infikovaného uživatelského PC v počítačové síti
Komerční uživatelé KolejNet	hrozí fyzické zničení prvků počítačové sítě nebo šíření škodlivého softwaru s využitím infikovaného uživatelského PC v počítačové síti
Zaměstnanci KaM VUT	zaměstnanci neodborně manipulují s prvky počítačové sítě nebo neodborně zasahují do IS
Nehmotná aktiva	
dostupnost	dostupnost byla omezena DDoS útokem z nakaženého uživatelského PC, dostupnost byla omezena výpadkem veškerých zdrojů napájení včetně záložních, dostupnost byla omezena útokem do počítačové sítě

3.2.5 Identifikace možných bezpečnostních událostí

Nejčastěji zde pozorujeme fyzické útoky, kdy je útočník nucen použít hrubou sílu k porušení samotného aktiva nebo přístupu k aktivu. Jako příklad lze uvést odcizení přístupového bodu z místa instalace. Dohledový systém hlásí, pokud zařízení nekomunikuje s ostatními prvky v síti. Následuje fyzická kontrola přístupového bodu a opětovné spuštění. Při znepřístupnění aktiva následuje nebo může následovat bezpečnostní incident. Jiná bezpečnostní událost může nastat během neoprávněného přístupu do sítě, přestože je do IS nutné se autentizovat pomocí přihlašovacího jména a hesla, může dojít k šíření škodlivého softwaru v síti skrze infikované uživatelské PC. Často se také setkáváme s řešením porušování autorského zákona ze strany uživatelů, tyto prohřešky nenarušují informační systém, řešení takových prohřešků je vedeno automaticky a z části také správci sítě. A podléhá mimo jiné Nařízení správce sítě 1/2015 a Prohřeškovému řádu sítě KolejNet.

3.2.6 Identifikace možných hrozeb

Hrozba je určitá událost nebo aktivita (může být také osoba), která má na bezpečnost nežádoucí vliv a může způsobovat škody. (Ondrák a kol., 2013, str. 348)

Tabulka 17: Identifikované hrozby
(Vlastní zpracování)

Druh aktiva	Možné hrozby
informační	hackerské útoky, neoprávněný přístup, porušení integrity dat, fyzické poškození, neaktuálnost dat, selhání hardwaru
aplikační	neoprávněný přístup, hackerské útoky, škodlivý software (malware), porušení integrity dat, narušení komunikační infrastruktury nebo přenosového prostředí, porušení dostupnosti dat, využití neaktuálního firmware
fyzická	přírodní katastrofy, odstavení el. energie, mechanické porušení, škodlivý software (malware), nesprávně zvolený/použitý materiál, nesprávná konstrukce a údržba, nevhodné podmínky pro údržbu, krátká střední meziporuchová doba, absence redundance, absence profylaxe, vady materiálu

Druh aktiva	Možné hrozby
služby	přírodní katastrofy, mechanické porušení, absence redundance, absence profylaxe a testování záložních zdrojů, neuhrazené pohledávky za služby
lidská	neodbornost zaměstnanců, legislativní úpravy, absence školení/dodatečného vzdělávání zaměstnanců, neoprávněný přístup a pokus o narušení zabezpečení sítě,
nehmotná	přírodní katastrofy, hackerské útoky, vady materiálu a opotřebování HW, pokusy o narušení zabezpečení sítě, nedostatečná kontrola a správa provozu

3.2.7 Analýza rizik

Kombinace pravděpodobností výskytu hrozby a z ní vzniklého incidentu se nazývá riziko hrozby. Míra ohrožení aktiva je tedy riziko. Výsledná úroveň rizika pak udává nebezpečnost sledované hrozby pro organizaci (v tomto případě oddělení). Aplikací bezpečnostních opatření lze tuto úroveň rizika snížit. (Ondrák a kol., 2013, str. 347, 351)

Ve sledovaném IS představují velké riziko aplikační aktiva, dále také informační a fyzická aktiva. K těmto aktivům je přístup omezený autorizací, avšak není plně zabezpečen, např. pokud uživatel/zaměstnanec sdělí možnému útočníkovi heslo pro přístup do sítě, nelze samotný útok vyloučit. Fyzická aktiva jsou obvykle umístěna v zabezpečených místnostech, jak je zvykem v běžné praxi. I tak však lze přistoupit neoprávněně útokem, (např. vylomení dveří) a fyzicky aktiva znepřístupnit, a to i bez odborných znalostí. Prvky, které jsou součástí fyzických aktiv jsou sice ve správě KolejNet, protože však oddělení KolejNet využívá prostorů Kolejí a menz VUT pro jejich umístění, mají přístup do vyhrazených místností také zaměstnanci KaM. V tabulce je vyjádřeno riziko vzniku bezpečnostní hrozby ve sledovaném informačním systému, v rozdělení do kategorií aktiv. Zde je pro větší přehlednost využito procentuálního vyjádření, tedy celková hodnota by neměla přesahovat 100 %.

Tabulka 18: Identifikované procento rizika.
(Vlastní zpracování)

Druh aktiva	Riziko
informační A	15%
aplikační/program. A	20%
fyzická A	15%
služby	15%
lidská A	15%
nehmotná A	20%
Celkem	100%

3.2.8 Posouzení výsledků

Dle celkového hodnocení se ukazuje že je IS v dobrém stavu a zabezpečen důkladně, stoprocentní bezpečnost ovšem není nikdy možné aplikovat v reálné praxi, a tak se můžeme i v dobře zabezpečeném systémů setkat s bezpečnostními incidenty. Hlavní faktor působící na tuto bezpečnost jsou útočníci, kteří získají přístup k IS a prvkům IS neoprávněně. Dále mohou způsobovat škody nedostatečné znalosti pracovníků či neodborná manipulace s prvky IS a nesprávné užití IS. Vzhledem k tomu, že nejvíce je využíváno napájení elektrickou energií, je její dodávka zabezpečena nejen elektrickými rozvody v jednotlivých areálech ale také záložními zdroji (UPS).

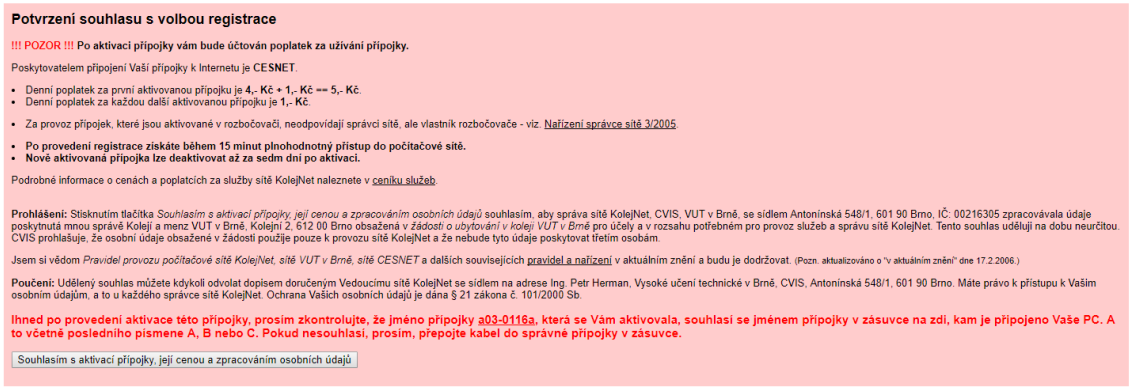
3.3 Současná ochrana osobních údajů v síti KolejNet

Oddělení KolejNet zpracovává podle dostupných údajů až 20 000 unikátních IP adres v rozdílném poměru IPv4 a IPv6 v čase největšího vytížení sítě. Vzhledem k povaze dat, je vhodné udržovat informační systém zabezpečený. Tuto bezpečnost z části pokrývá pracovní pozice DPO. Následující operace jsou dle odstavce 2, článku 4, Definice, GDPR, považovány za zpracování osobních údajů v oddělení KolejNet.

- Shromáždění osobních údajů při registraci ubytování a jejich úprava, vytvoření pracovní smlouvy na základě přijetí zaměstnance,
- zaznamenání těchto dat do informačního systému KolejNet,
- uspořádání, strukturování a uložení dat v databázi KolejNet (CVIS),

- autentizace pomocí osobních údajů do systému NETIS (pro správu VUT sítě, pomocí standardu SAML)
- přizpůsobení dat pro informační systém KolejNet,
- nahlížení a úprava dat uživatelem či zaměstnancem KolejNet,
- použití dat pro autentizaci a autorizaci uživatele či zaměstnance,
- šíření či zpřístupnění dat zaměstnanců za účelem plnění pracovních úkolů,
- využití dat k ověřování identity uživatele při nelegálním nebo nepřiměřeném užívání sítě KolejNet,
- řazení dat pro potřeby informačního systému,
- výmaz údajů při zrušení uživatelské přípojky, výmaz údajů při ukončení ubytování uživatele.

Operace s daty jsou tedy ve sledovaném oddělení nutné pro správný chod informačního systému a pro správu studentské sítě. Před zavedením nařízení GDPR je v síti KolejNet vyžadován souhlas s ukládáním osobních údajů a jejich zpracování, prostřednictvím elektronického formuláře v průběhu registrace uživatelské přípojky na webové adrese https://www.kn.vutbr.cz/reg/. Zde je v první části uveden poskytovatel internetu (ISP), cena za konkrétní aktivovanou přípojku a doplňující informace pro uživatele.



Potvrzení souhlasu s volbou registrace

!!! POZOR !!! **Po aktivaci přípojky vám bude účtován poplatek za užívání přípojky.**

Poskytovatelem připojení Vaší přípojky k Internetu je **CESNET**.

- Denní poplatek za první aktivovanou přípojku je **4,- Kč + 1,- Kč == 5,- Kč**.
- Denní poplatek za každou další aktivovanou přípojku je **1,- Kč**.

- Za provoz přípojek, které jsou aktivované v rozbočovači, neodpovídají správci sítě, ale vlastník rozbočovače - viz. Nařízení správce sítě 3/2005.

- **Po provedení registrace získáte během 15 minut plnohodnotný přístup do počítačové sítě.**
- **Nově aktivovaná přípojka lze deaktivovat až za sedm dní po aktivaci.**

Podrobné informace o cenách a poplatcích za služby sítě KolejNet naleznete v ceníku služeb.

Prohlášení: Stisknutím tlačítka *Souhlasím s aktivací přípojky, její cenou a zpracováním osobních údajů* souhlasím, aby správa sítě KolejNet, CVIS, VUT v Brně, se sídlem Antonínská 548/1, 601 90 Brno, IČ: 00216305 zpracovávala údaje poskytnutá mnou správě Kolejí a menz VUT v Brně, Kolejní 2, 612 00 Brno obsažená v *žádosti o ubytování v koleji VUT v Brně* pro účely a v rozsahu potřebném pro provoz služeb a správu sítě KolejNet. Tento souhlas udělují na dobu neurčitou. CVIS prohlašuje, že osobní údaje obsažené v žádosti použije pouze k provozu sítě KolejNet a že nebude tyto údaje poskytovat třetím osobám.

Jsem si vědom *Pravidel provozu počítačové sítě KolejNet, sítě VUT v Brně, sítě CESNET* a dalších souvisejících pravidel a nařízení v aktuálním znění a budu je dodržovat. (Pozn. aktualizováno o "v aktuálním znění" dne 17.2.2006.)

Poučení: Udělený souhlas můžete kdykoli odvolat dopisem doručeným Vedoucímu sítě KolejNet se sídlem na adrese Ing. Petr Herman, Vysoké učení technické v Brně, CVIS, Antonínská 548/1, 601 90 Brno. Máte právo k přístupu k Vašim osobním údajům, a to u každého správce sítě KolejNet. Ochrana Vašich osobních údajů je dána § 21 zákona č. 101/2000 Sb.

Ihned po provedení aktivace této přípojky, prosím zkontrolujte, že jméno přípojky a03-0116a, která se Vám aktivovala, souhlasí se jménem přípojky v zásuvce na zdi, kam je připojeno Vaše PC. A to včetně posledního písmene A, B nebo C. Pokud nesouhlasí, prosím, přepojte kabel do správné přípojky v zásuvce.

Souhlasím s aktivací přípojky, její cenou a zpracováním osobních údajů

Obrázek 6: Formulář pro potvrzení aktivace a zpracování uživ. údajů.
(Vlastní zpracování)

V druhé části formuláře je uveden následující text:

„Prohlášení: Stisknutím tlačítka Souhlasím s aktivací přípojky, její cenou a zpracováním osobních údajů souhlasím, aby správa sítě KolejNet, CVIS, VUT v Brně, se sídlem Antonínská 548/1, 601 90 Brno, IČ: 00216305 zpracovávala údaje poskytnutá mnou správě Kolejí a menz VUT v Brně, Kolejní 2, 612 00 Brno obsažená v žádosti o ubytování

v koleji VUT v Brně pro účely a v rozsahu potřebném pro provoz služeb a správu sítě KolejNet. Tento souhlas uděluji na dobu neurčitou. CVIS prohlašuje, že osobní údaje obsažené v žádosti použije pouze k provozu sítě KolejNet a že nebude tyto údaje poskytovat třetím osobám.“

„Jsem si vědom Pravidel provozu počítačové sítě KolejNet, sítě VUT v Brně, sítě CESNET a dalších souvisejících pravidel a nařízení v aktuálním znění, a budu je dodržovat.“

„Poučení: udělený souhlas může kdikoli dovolat dopisem doporučeným Vedoucímu sítě KolejNet se sídlem na adrese Ing. Petr Hermann, Vysoké učení technické v Brně, CVIS, Antonínská 548/1, 601 90 Brno. Máte právo k přístupu k Vašim osobním údajům, a to u každého správce sítě KolejNet. Ochrana Vašich osobních údajů je dána § 21 zákona č. 101/2000 Sb. “

3.3.1 Zálohování a bezpečnost dat

V hodnoceném IS nejsou zálohy databází a serverů provedeny kopírováním dat a tvořením obrazů (image) jednotlivých disků, jak je obvyklé, ale zálohují se jen podstatné části jako jednotlivé skripty, weby, konfigurace a jiné. Archivovány jsou pak na 3, maximálně 4 roky. Neexistuje zde žádné úložiště dat uživatelů ani jeho záloha. Bezpečnost také zaručuje vlastní poštovní server spirit.kn.vutbr.cz, doména pro příjem elektronické pošty je kn.vutbr.cz, na příchozím poštovním serveru je zavedeno filtrování elektronické pošty pomocí programu MIMEDefang. Také je využívám antivirový program CLAM AV (aplikace virus scanneru na přílohy, zavirované adresy se dále nedoručují) a antispamová ochrana, jenž je založena na DNS blokovacích databázích a programech SpamAssassin a Razor (probíhá zde kontrola IP adres všech zařízení, které chtějí přes SMTP servery VUT odeslat zprávu. Pokud je IP adresa totožná s IP adresou v databázi, spojení je odmítnuto).

3.3.2 Souhlas subjektu

Tento souhlas je potvrzován uživatelem, a to tlačítkem na webové stránce KolejNet. Dá se považovat za svobodný, jelikož tomuto kroku předchází manuální registrace přípojky uživatelem. Avšak mohl by být více konkretizovaný, a to souhrnem jednotlivých položek, které se mezi osobní údaje řadí a také jak se s nimi manipuluje. Informovanost uživatele

se zdá nedostatečná, je uvedeno sídlo a IČ organizace, kde byly informace získány, v jakém rozsahu s nimi bude nakládáno a na jakou dobu je souhlas udělen. Také lze souhlas v libovolné době odvolat u osoby jež je k tomu oprávněná a je uvedena ve formuláři. Přístup k informacím je uživateli povolen z prostředí informačního systému po ověření identity uživatele za přítomnosti zaměstnance organizace KolejNet (nejčastěji na pozici správce sítě) jemuž je umožněn přístup do administrátorského informačního systému nebo uživatelem samotným po autentizaci do informačního systému skrze webový prohlížeč. Souhlasem uživatel umožňuje oddělení KolejNet zpracovávat osobní údaje, jelikož jsou nezbytné pro administraci a provoz sítě KolejNet. Tedy jsou vyžadovány za účelem plnění služeb uvedených ve smlouvě mezi subjektem údajů a jejich správcem.

3.3.3 Třetí strana

Formulář informací pro uživatele udává, že získané informace nebudou poskytovány třetím „osobám“, takto definuje jiné osoby s přístupem k osobním údajům oddělení KolejNet. Nařízení však používá formulaci „třetí strana“. Dle ustanovení v GDPR (oprávněný zájem správce osobních údajů) má správce možnost sdílet a předávat informace o subjektech údajů v rámci jedné organizace nebo skupiny podniků pro vnitřní administrativní účely.

3.3.4 Rodné číslo

Zde je především nutné specifikovat, že je uživatelské RČ využíváno pro zajištění poskytování služeb KolejNet. Rodné číslo zpracovává KolejNet jako přidělené výchozí heslo pro uživatele připojení k síti. V případě osob, které nemají RČ, je použit rodný kód nebo variabilní symbol. Tímto heslem se uživatel přihlásí do informačního systému a následně je vyzván ke změně původního hesla. Takto určené heslo je jednoznačné a pro každého uživatele snadno definovatelné. Zároveň se vytrácí nutnost sdělovat přihlašovací údaje individuálně např. doporučeným dopisem. Takový způsob je neúsporný a nevhodný v mnoha ohledech. Z tabulky č. 19 vyplývá, že i přes nebezpečí, které z použití rodného čísla jako hesla vyplývá, je vhodnější k použití. Zabezpečení je z velké části ošetřeno vynucenou změnou uživatelského hesla uživatelem, v průběhu první registrace k síti a zadáním kontaktního účtu elektronické pošty (zvolené v jiné doméně než kn.vutbr.cz).

Využití uživatelského hesla tedy odpovídá pouze procesu prvního přihlášení a následně je uchováváno za účelem správy uživatelských účtů (zpravidla pro obnovení hesla, pokud své nové heslo uživatel zapomene).

Tabulka 19: Tabulka přizpůsobení uživatelského hesla.
(Vlastní zpracování)

Způsob doručení/zjištění	Výhody	Nevýhody
Heslo složené z vygenerovaných znaků, doporučeně poštou	Do vlastních rukou uživatele.	Dlouhá doba doručení (především v případě zahraničních studentů) Uživatel vlastní přihlašovací údaje uvedené fyzicky na nějakém médiu. Ekologie (použití recyklovaného/recyklovatelného média) Oddělení vznikají náklady spojené s administrací tohoto firemního procesu.
Rodné číslo	Jednoduše identifikovatelné pro uživatele.	Je znám algoritmus pro výpočet rodného čísla. Neoprávněná osoba jej může velmi snadno zjistit a zneužít. Z RČ lze identifikovat další osobní údaje (pohlaví, datum narození).

4 VLASTNÍ NÁVRHY ŘEŠENÍ

Nyní definujeme všechny důležité části konečné implementace nařízení na informační systém. Tato kapitola využívá poznatků z předešlých částí práce.

4.1 Přípravy zavedení do organizace

Prvním krokem je souhlas vedení organizace se změnami systému a jeho podpora. Před zavedením do organizace byl nařízen audit informačního systému. Na tento audit navázala analýza ISMS (částečné řešení DPIA), identifikace osobních údajů a důkladné zhodnocení kdo a jakým způsobem pracuje s osobními údaji a jak jsou technicky zabezpečeny. Následně se stanoví určité návrhy na opatření při vzniku rizika, jeho změření, nebo jeho akceptace. Na základě výstupů byl informační systém zhodnocen jako dostatečně zabezpečený, a to především proto, že splňoval všechny zásady k dodržování zákona č. 101/2000 o ochraně osobních údajů. Následná opatření pro zákonnost v rámci GDPR již byla pouze nadstavbou. Organizace provedla kromě auditu a analýzy informačního systému a jeho okolí také informační schůzku se zaměstnanci, kde bylo téma prezentováno a bylo tak s dostatečným předstihem upozorněno na následující změny. VUT jako právnická osoba, dle Úplného znění statutu VUT, s velkou množinou propojených organizačních jednotek, musí řešit nasazení a údržbu zákonnosti zpracování vzhledem k GDPR více či méně centralizovaně. (VUT, 2017)

4.2 Právní základ

Dle odstavce 44 je zpracování osobních údajů zákonné, neboť je nezbytné pro plnění smlouvy (nebo v souvislosti s úmyslem smlouvu uzavřít) mezi poskytovatelem služeb a jeho zákazníkem. Vzhledem k charakteru poskytované služby lze zpracovávání očekávat a právním důvodem se stává smlouva. Významnými právními podklady pro tuto konkrétní implementaci jsou také odstavce 47 a 48. V odstavci 47 jsou definovány oprávněné zájmy správce, které umožňují zákonné zpracování osobních údajů bez souhlasu subjektu údajů. Následující odstavec pak stanovuje oprávněný zájem na předání osobních údajů v rámci skupiny podniků nebo instituce přidružené k ústřednímu orgánu. Pro tuto práci je dále relevantní článek 49 GDPR, který umožňuje zpracovávání jako oprávněný zájem správce pro zajištění bezpečnosti sítě a komunikace. **Pro zpracovávání**

osobních údajů nemusí oddělení KolejNet vyžadovat souhlas, avšak vzhledem k povaze dat a aktuálně platné legislativě ČR, doporučuji zpracovávání na základě uživatelského souhlasu. Také doporučuji upravit dobu archivace osobních údajů za účelem vedení účetnictví (dle paragrafu 31 a 32 zákonu o účetnictví) a zrušit funkci uzamykání uživatelských účtů.

4.3 Obecný postup

Následující 4 kategorie zahrnují některé důležité prvky, které by měla každá organizace zvážit a definovat (nejlépe písemně) před zavedením GDPR.

- Mapování: jaké osobní údaje vlastní organizace, kde se nacházejí, jak jsou tyto údaje předávány, je stanovena osoba zodpovědná za agendu osobních údajů, jsou zavedeny interní směrnice podporující toto téma, jsou prováděna školení na dané téma v organizaci, po jak dlouhou dobu jsou údaje zpracovávány a jak často jsou aktualizovány, je zpracování automatizované či manuální, kdo je správce či zpracovatel osobních údajů, je požadován souhlas se zpracováním a v jaké míře, lze zajistit výmaz či opravu osobních údajů…
- Správa: rozhodnutí o způsobech využití a přístupu k osobním údajům, kdo je zodpovědný za řízení informační bezpečnosti, je zaveden systém ISMS, je zavedena vnitřní směrnice či bezpečnostní politika, existuje evidence bezpečnostních incidentů, je zajištěna dostatečná autentizace uživatelů či zaměstnanců a jejich školení, jaké komunikační kanály organizace využívá…
- Ochrana: zavedení bezpečnostních kontroly k předcházení, detekci a řešení hrozeb a bezpečnostních incidentů, bezpečnostní opatření…
- Dokumentace: uchovávání požadovaných záznamů, pravidla, řády a manuály, vyřizování žádostí týkající se osobních údajů, upozornění na rizika…

4.4 Návrh opatření

Opatření by měla mít za cíl úplně zamezit vytvoření hrozby, nebo alespoň minimalizovat rizika a vzniklé škody. V rámci ISMS lze opatření realizovat například pomocí ČSN ISO/IEC 27002:2005, tato norma dělí 133 bezpečnostních opatření do 11 oblastí, doplněných o dokumentaci.

Tabulka 20: Oblasti bezpečnostních opatření pro hodnocený IS dle ČSN ISO/IEC 27002:2005
(Vlastní zpracování dle: Ondrák a kol., 2013, str. 104-128)

	OBLAST	ROZSAH	NÁZEV DOKUMENTU
A.5	Bezpečnostní politika	ochrana, řízení a distribuce aktiv	Globální bezpečnostní politika organizace VUT
A.6	Organizace bezpečnosti informací	interní (důvěrné informace, osobní údaje) a externí (přístup klientů, třetích stran)	Pravidla údržby a provozu ochrany osobních údajů
A.7	Řízení aktiv	evidence, klasifikace a použití aktiv a kategorizace dat a nakládání s informacemi	Analýza ISMS
A.8	Bezpečnost lidských zdrojů	životní cyklus pracovníka	Pravidla údržby a provozu ochrany osobních údajů a Systém řízení ochrany zdraví a bezpečnosti práce
A.9	Fyzická bezpečnost a bezpečnost prostředí	ochrana prostředí organizace jako celku a současně opatření chránící prvky infrastruktury IT	Pravidla provozu počítačové sítě a Nařízení správce sítě
A.10	Řízení komunikací a řízení provozu	bezpečný provoz IS/ICT, provozní postupy, dodávky třetích stran	Prohřeškový řád a Service Level Agreement (smlouva mezi poskyt. služby a zákazníkem)
A.11	Řízení přístupu	přístup uživatelů, přístup k síti, k operačnímu systému, k aplikacím a řízení vzdálené správy	Pravidla správy počítačové sítě
A.12	Akvizice vývoj a údržba informačních systémů	požadavky na bezpečnost SW aplikací, implementace a údržby	Pravidla údržby a provozu ochrany osobních údajů
A.13	Zvládání bezpečnostních incidentů	hlášení bezpečnostních incidentů uživateli a řešení bezpečnostními odborníky	Formulář hlášení bezpečnostního incidentu
A.14	Řízení kontinuity činnosti organizace	řízení kontinuity činností organizace (BCM) jako řídící proces na úrovni vedení org., plán obnovy po havárii	Plán obnovy po havárii (DR - Disaster Recovery Plan)
A.15	Soulad s požadavky	soulad s legislativou, soulad s bezpečnostní politikou, normami a technická shoda a stanovisko auditu	Analýza požadavků legislativy, bezpečnostní politiky a norem

4.5 Dokumentace

Vznik nové dokumentace či úprava nebo rozšíření stávající by v organizaci měl zajistit jasně definovaný postup při zpracování osobních údajů. Takový postup by zajistil zaznamenání jednotlivých procesů, přes které putují osobní údaje (trasovatelnost), či které využívají osobní údaje a v případě žádosti uživatele by jej bylo možné předložit. Trasovatelnost může posloužit také při vzniku bezpečnostních incidentů. Dokumentace by měla být tvořena relevantně k ostatním směrnicím a řádům v organizaci.

4.5.1 Pravidla údržby a provozu ochrany osobních údajů

Prvně budou vytvořena pravidla, která budou shrnovat informace o zpracovávaných datech, o jednotlivých subjektech údajů, správcích, zpracovatelích a dalších osobách, jež spolupracují na zpracování osobních údajů a o samotném zpracování a jeho zabezpečení, nebo také oprávněné zájmy, práva a povinnosti jednotlivých subjektů a pověřené osoby. Taková dokumentace může sloužit jako jeden z podkladů pro dozorové orgány při

kontrole dodržování zákonnosti zpracování. Tento dokument je uveden na konci práce jako příloha č. 1.

4.5.2 Řád ochrany osobních údajů

Vytvořením řádu, který bude platný pro uživatele sítě KolejNet definujeme práva subjektů údajů, jejich další oprávněné zájmy a možnosti. Řád bude sloužit subjektům údajů jako obecnější pohled na nové nařízení a s ním spojené změny. Bude obsahovat včetně uvedených příkladů také modelové situace, aby byla legislativa snadněji pochopitelná a bude sloužit také jako soubor minimálních bezpečnostních pravidel pro uživatele. Tento dokument je uveden na konci práce jako příloha č. 2.

4.5.3 Schéma toku konkretizovaných dat

Toto schéma ukáže tok osobních údajů skrze oddělení i s ostatními vstupy a výstupy. Schéma bude doplněno o legendu, tak aby bylo čitelné pro všechny subjekty. Vzhledem k zajištění bezpečnosti a rozsahu sítě, nelze schéma transformovat na fyzickou topologii sítě KolejNet a proto je popsán datový tok vývojovým diagramem. Tento dokument je uveden na konci práce jako příloha číslo 3.

4.6 Poučení o ochraně osobních údajů

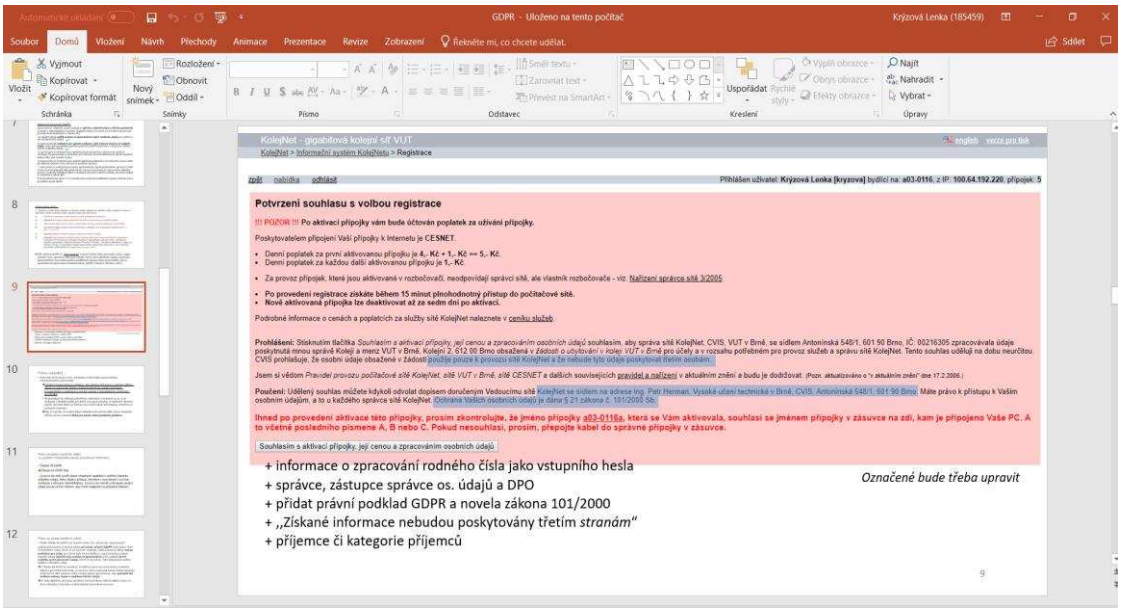
4.6.1 Poučení zaměstnanců

Poučení zaměstnanců oddělení KolejNet proběhlo formou prezentace s podstatnými informacemi v lednu roku 2018 na schůzi správců sítě. Zaměstnanci byli seznámeni se základními pojmy, byly představeny možnosti řešení a konzultovány nedostatky návrhu na implementaci GDPR, během této schůzky byl také prezentován současný stav sítě KolejNet a plány na následující období. Do budoucnosti navrhuji dále projednávat změny a získávat zpětnou vazbu od zaměstnanců na začátku každé schůze správců sítě. Dále by také bylo vhodné školit zaměstnance alespoň jedenkrát za rok o změnách v IS a případných změnách legislativy. Pro takové školení by pak byly důležité především následující body:

- ujasnění názvosloví a vysvětlení pojmů (právní úprava, ISMS…),

- aktuální stav bezpečnostní politiky organizace a dokumentace,
- zdůraznění změn oproti předchozímu školení a jejich přínosy,
- ověření znalostí školených subjektů.

Pokud by oddělení KolejNet v budoucnu zpracovávala také citlivé údaje, bylo by nutné aplikovat také tzv. „Dohodu o důvěrnosti“.



Obrázek 7: Ukázka prezentace pro schůzi správců sítě v roce 2018, vytvořeno pomocí programu MS PowerPoint.

(Vlastní zpracování)

4.6.2 Poučení uživatelů

Poučení uživatelů o jejich právech a povinnostech proběhne při každé nové registraci přípojky k síti KolejNet (bez této registrace nelze připojení provozovat) a na základě uživatelského souhlasu je připojení navázáno Na základě právní úpravy nařízení GDPR byl upraven původní webový formulář pro získání souhlasu se zpracováním osobních údajů od uživatelů sítě KolejNet. V původním formuláři, který odpovídal zákonu č. 101/2000 Sb. o ochraně osobních údajů chyběly některé prvky, které jsou nyní podstatné z hlediska GDPR. Jednalo se o následující výčet prvků:

- zákonnost zpracování dle GDPR,
- úplný popis správce osobních údajů, jeho zástupce či DPO,
- informace o zpracování rodného čísla,

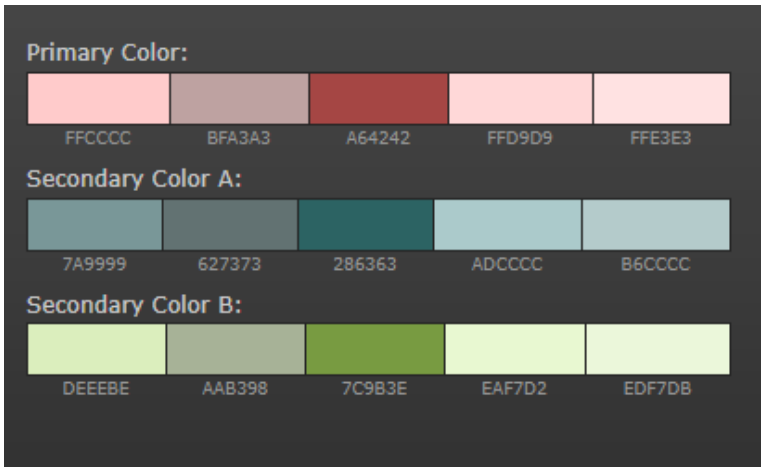
- případné příjemce či kategorie příjemců osobních údajů, pokud existují (orgány veřejné moci se mezi příjemce neřadí),
- upozornění na zpracování cookies, metadat....

Nový formulář bude po úpravě obsahovat informace odpovídající této struktuře.

1. Odstavec s informacemi pro uživatele:
    a. upozornění o poplatku za aktivaci přípojky,
    b. poskytovatele internetu,
    c. poplatky za služby,
    d. odpovědnost za přípojky umístěné v rozbočovači (router),
    e. prodlení při registraci, deaktivace přípojky, odkazy na podrobný ceník,
    f. poučení o pravidlech a nařízeních sítě.
    - Souhlas s aktivací přípojky, její cenou a pravidly počítačové sítě.
2. Odstavec prohlášení a poučení:
    a. cíl uživatelského souhlasu s náležitostmi dle GDPR: definované osobní údaje, rozsah a doba uložení a zpracování, účel zpracování a informace o technickém zabezpečení,
    b. kategorie osobních údajů a kategorie subjektu údajů,
    c. poučení o právech uživatele a právní podklad.
3. Doplnění:
    a. kontrola správnosti zapojení,
    - souhlas se zpracováním osobních údajů za účelem provozu sítě KolejNet, na základě smluvního vztahu o poskytování služeb,
    b. potvrzovací tlačítko.

4.7 Zdrojový kód pro webový formulář souhlasu subjektu údajů

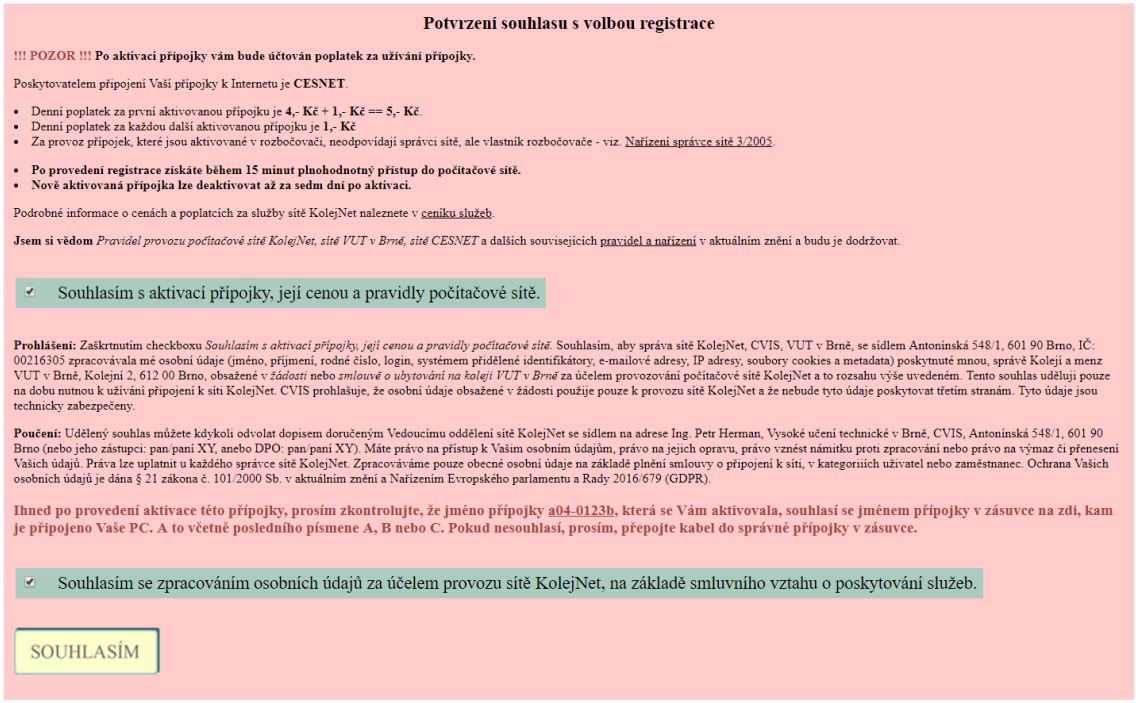
Pro implementaci byl připraven zdrojový kód pro webovou stránku obsahující potvrzení souhlasu, a to za použití jazyku HTML. Šablona webové stránky je původní, ponechaná ve standardním formátu, jež oddělení používá. Dále jsou zde také ponechány odkazy a prvky, které využívají JavaScipt. Ve formuláři jsou barevně zvýrazněny podstatné informace a grafika také slouží k navedení uživatele ke správnému postupu.



Obrázek 8: Zvolené barevné schéma.
(Vlastní zpracování dle: Colorschemedesigner)

4.8 Aplikace na webové stránky

Vytvořený skript z předchozí podkapitoly aplikujeme na webové stránky sloužící pro přístup do informačního systému KolejNet. Formulář bude sloužit pro plnohodnotné udělení uživatelského souhlasu. Platí, že mezi předmětem plnění a typem zpracovávaných dat je reálná objektivní a přímá vazba. Souhlas je archivován, je zřejmé, že byl uživatelem udělen, pokud je aktivována uživatelská přípojka. Datum a čas udělení souhlasu je zapsán v databázi. Správce by však měl vzít v úvahu také obnovu tohoto souhlasu se zpracováváním osobních údajů, pokud údaje zpracovává po delší dobu. Souhlas poskytnutý před zavedením GDPR do organizace, který je v souladu s tímto nařízením není nutné vyžadovat znovu, pokud splňuje všechny náležitosti nařízení GDPR.



Potvrzení souhlasu s volbou registrace

!!! POZOR !!! **Po aktivaci přípojky vám bude účtován poplatek za užívání přípojky.**

Poskytovatelem připojení Vaší přípojky k Internetu je **CESNET**.

- Denní poplatek za první aktivovanou přípojku je **4,- Kč + 1,- Kč == 5,- Kč**.
- Denní poplatek za každou další aktivovanou přípojku je **1,- Kč**
- Za provoz přípojek, které jsou aktivované v rozbočovači, neodpovídají správci sítě, ale vlastník rozbočovače - viz. Nařízení správce sítě 3/2005.

- **Po provedení registrace získáte během 15 minut plnohodnotný přístup do počítačové sítě.**
- **Nově aktivovaná přípojka lze deaktivovat až za sedm dní po aktivaci.**

Podrobné informace o cenách a poplatcích za služby sítě KolejNet naleznete v ceníku služeb.

Jsem si vědom *Pravidel provozu počítačové sítě KolejNet, sítě VUT v Brně, sítě CESNET* a dalších souvisejících pravidel a nařízení v aktuálním znění a budu je dodržovat.

Souhlasím s aktivací přípojky, její cenou a pravidly počítačové sítě.

Prohlášení: Zaškrtnutím checkboxu *Souhlasím s aktivací přípojky, její cenou a pravidly počítačové sítě.* Souhlasím, aby správa sítě KolejNet, CVIS, VUT v Brně, se sídlem Antonínská 548/1, 601 90 Brno, IČ: 00216305 zpracovávala mé osobní údaje (jméno, příjmení, rodné číslo, login, systémem přidělené identifikátory, e-mailové adresy, IP adresy, soubory cookies a metadata) poskytnuté mnou, správě Kolejí a menz VUT v Brně, Kolejní 2, 612 00 Brno, obsažené v *žádosti* nebo *smlouvě o ubytování na koleji VUT v Brně* za účelem provozování počítačové sítě KolejNet a to rozsahu výše uvedeném. Tento souhlas uděluji pouze na dobu nutnou k užívání připojení k síti KolejNet. CVIS prohlašuje, že osobní údaje obsažené v žádosti použije pouze k provozu sítě KolejNet a že nebude tyto údaje poskytovat třetím stranám. Tyto údaje jsou technicky zabezpečeny.

Poučení: Udělený souhlas můžete kdykoli odvolat dopisem doručeným Vedoucímu oddělení sítě KolejNet se sídlem na adrese Ing. Petr Herman, Vysoké učení technické v Brně, CVIS, Antonínská 548/1, 601 90 Brno (nebo jeho zástupci: pan/paní XY, anebo DPO: pan/paní XY). Máte právo na přístup k Vašim osobním údajům, právo na jejich opravu, právo vznést námitku proti zpracování nebo právo na výmaz či přenesení Vašich údajů. Práva lze uplatnit u každého správce sítě KolejNet. Zpracováváme pouze obecné osobní údaje na základě plnění smlouvy o připojení k síti, v kategoriiích uživatel nebo zaměstnanec. Ochrana Vašich osobních údajů je dána § 21 zákona č. 101/2000 Sb. v aktuálním znění a Nařízením Evropského parlamentu a Rady 2016/679 (GDPR).

Ihned po provedení aktivace této přípojky, prosím zkontrolujte, že jméno přípojky a04-0123b, která se Vám aktivovala, souhlasí se jménem přípojky v zásuvce na zdi, kam je připojeno Vaše PC. A to včetně posledního písmene A, B nebo C. Pokud nesouhlasí, prosím, přepojte kabel do správné přípojky v zásuvce.

Souhlasím se zpracováním osobních údajů za účelem provozu sítě KolejNet, na základě smluvního vztahu o poskytování služeb.

SOUHLASÍM

Obrázek 9: Konečná verze formuláře pro uživatelský souhlas.
(Vlastní zpracování)

4.9 Zpětná vazba

V každém projektu je velmi důležitou součástí fáze po-projektová, která zahrnuje mimo jiné také získávání zpětné vazby. I přesto, že se zde zpětná vazba nejeví jako příliš důležitá, vzhledem k jasně stanoveným pravidlům legislativy, může vhodně posloužit při vylepšování strategie řízení, vylepšování funkčnosti a vzhledu informačního systému nebo úpravě dokumentace. Vzhledem k velkému počtu různých uživatelů, navrhuji získávat zpětnou vazbu pomocí elektronické pošty výhradně od zaměstnanců oddělení KolejNet nebo KaM.

4.10 Přínosy navržených řešení

Navržené řešení má pro oddělení KolejNet několik přínosů. Hlavním přínosem je nyní již zákonné zpracovávání osobních údajů dle nařízení GDPR, pomocí zajištění dostatečných technických opatření na základě vyhodnocení analýz. Zákonnost dle GDPR nyní splňuje také formulář uživatelského souhlasu. Předešlá verze formuláře splňovala zákonnost dle zákona č. 101/2000 Sb., tato zákonnost byla zachována i v novém formuláři. Vedlejšími přínosy jsou především kontrola stavu informačního systému KolejNet, včetně jeho

součástí a analýza ISMS v oddělení KolejNet, která může následně sloužit jako část podkladové dokumentace pro dozorové orgány. Přínosem je také další vytvořená dokumentace, usnadňuje pochopení nově implementovaného nařízení uživatelům i zaměstnancům. Neméně významným přínosem jsou aktualizace a změny dat v informačním systému, pro zajištění integrity.

4.11 Ekonomické zhodnocení řešení

Takové řešení vyžaduje uvědomění toho, že všechna data v podniku nelze za žádnou cenu plně technicky zabezpečit. Lze však úspěšně předcházet problémům, které vznikají při provozu, a to především jasnými pravidly a jejich dodržováním. Tento informační systém je dostatečně fyzicky zabezpečen a není tedy nutný nákup a instalace kvalitnějšího hardwaru. Odhadem lze říci, že pokud by měla být stanovena cena této implementace, je možné ji určovat pouze na základě času, který byl věnován přípravě a nasazení (audit, analýzy, porady, režijní náklady…). Následující tabulka poukazuje na odhady nákladů na zavedení GDPR do organizace (jednorázové náklady) a na následný provoz (na 1 rok).

Tabulka 21: Odhady nákladů na zavedení a provoz GDPR
(Vlastní zpracování)

Název nákladu	jednotka	cena za jednotku	externí náklady	CELKEM JEDNOTEK	CELKEM CENA
Náklady na zavedení GDPR					
studie proveditelnosti	člověkoden	1 200 Kč	- Kč	5	6 000 Kč
analýza prostředí, legislativy a norem	člověkoden	1 200 Kč	- Kč	10	12 000 Kč
analýza ISMS	člověkoden	1 200 Kč	- Kč	10	12 000 Kč
audit			20 000 Kč		20 000 Kč
dokumentace	člověkoden	1 200 Kč	- Kč	14	16 800 Kč
implentace na web	člověkoden	1 200 Kč	- Kč	1	1 200 Kč
režijní náklady			5 000 Kč		5 000 Kč
				Celkem náklady na zavedení:	**73 000 Kč**
Náklady na provoz (za 1 rok)					
mzdové náklady (12 zaměstnanců)	den	30 000 Kč	- Kč	356	10 680 000 Kč
provoz HW a komunikační infrastruktury	den	10 000 Kč	- Kč	356	3 560 000 Kč
profylaxe a redundance	den	10 000 Kč	- Kč	356	3 560 000 Kč
režijní náklady			250 000 Kč		250 000 Kč
				Celkem náklady na provoz:	**18 050 000 Kč**
				Celkem náklady:	**18 123 000 Kč**

ZÁVĚR

Navrhnout celkově zabezpečený informační systém je velký oříšek i pro zkušené odborníky. Ve většině případů se nejedná o krátkodobý projekt, ale o důkladnou přípravu podloženou studií proveditelnosti, přesně definovaný návrh ohraničený rozpočtem, vhodně zvolené materiály a odborně nainstalované prvky. Zajištění bezpečnosti fyzických prvků lze aplikovat velmi dobře s dostatečnými zkušenostmi, velmi náročné je však zabezpečit data a z nich získané informace. Důkladným teoretickým rozpoznáním problému a kompletní analýzou vnitřního a vnějšího prostředí, byly stanoveny hranice pro návrh na implementaci. V takovém návrhu pak vznikla nová pravidla a proběhly změny v informačním systému a pracovních postupech oddělení. Nově vzniklá dokumentace by měla sloužit jako podklad pro správnou údržbu a provoz ochrany osobních údajů, v následujících obdobích fungování oddělení KolejNet.

SEZNAM POUŽITÝCH ZDROJŮ

CETLOVÁ, P., 2018. *Návrh vnitřní normy – Pokyn k zajištění implementace GDPR* [online]. Brno: VUT [cit. 2018-03-24]. Dostupné z: https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/navrhy-vnitrnich-norem-pokyn-k-zajisteni-implementace-gdpr-d167990

DOSEDĚL, T., 2004. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 190 s. ISBN 80-251-0106-1.

DOUCEK, Petr., Luděk Novák, Lea Nedomová a kolektiv, 2011. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. Praha: Professional Publishing, 286 s. ISBN 978-80-7431-050-8.

DVORSKÁ, D., 2018. *Pokyn č. 6/2018 – Pokyn k zajištění implementace Nařízení Evropského parlamentu a Rady 2016/679 (GDPR) na VUT* [online]. Brno: VUT [cit. 2018-03-24]. Dostupné z: https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/pokyny-6-2018-pokyn-k-zajisteni-implementace-narizeni-evropskeho-parlamentu-a-rady-2016-679-(gdpr)-na-vut-d169569

EUROPEAN DATA PROTECTION SUPERVISOR, 2017. Data Protection [online]. EDPS ©2017 [cit. 2017-11-28]. Dostupné z: https://edps.europa.eu/data-protection_en

EVROPSKÁ UNIE, 2016. *Nařízení Evropského parlamentu a Rady* (EU) 2016/679 [online]. Evropská unie ©1998-2018 [cit. 2018-04-24]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32016R0679

KRISTOL, D. M., 2001. HTTP Cookies: Standards, Privacy, and Politics [online]. Vol. 1, Is. 2, p. 151-198 [cit. 2017-12-09]. ISSN: 15335399. Dostupné z: DOI: 10.1145/502152.502153

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK, 2013. *Problematika ISMS v manažerské* informatice. Brno: CERM. 378 s. ISBN 978-80-7204-872-4.

ONDRÁK, V., 2017 *Bezpečnost ICT* [přednáška]. Brno: VUT, 19. dubna 2017.

ORGANIZACE SPOJENÝCH NÁRODŮ, 2015. *Všeobecná deklarace lidských práv* [online]. Praha: UNIC ©2015 [cit. 2018-02-26]. Dostupné z: http://www.osn.cz/wp-content/uploads/2015/12/UDHR_2015_11x11_CZ2.pdf

POMERANTZ, J., 2015. Metadata. Cambridge: MIT Press. 256 s.
ISBN 978-02-6252-851-1

POŽÁR, J., 2007. *Základy teorie informační bezpeč*nosti. 1. vyd. Praha: Vydavatelství PA ČR, 219 s. ISBN 978-80-7251-250-8.

RYCHLÝ, M., 2015. *Návrh a implementace IT služeb* [přednáška]. Brno: VUT, 23. září 2015.

SPURNÁ, I., 2010. *Počítačové sítě: praktická příručka správce sítě.* Kralice na Hané: Computer Media, 180 s. ISBN 978-80-7402-036-0.

STANÍČEK, P., 2002. Color Scheme Designer (Palleton) [online]. ©2002-2010 [cit. 2018-04-24]. Dostupné z: http://colorschemedesigner.com/csd-3.5/

SUCHÁNEK, P., 2017. *Metodický list č. 5/2017 – Audit informačních systémů zpracovávajících osobní údaje* [online]. Brno: VUT [cit. 2018-02-17].
Dostupné z: https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/metodicke-listy-5-2017-audit-informacnich-systemu-zpracovavajicich-osobni-udaje-d157359/metodicky-list-5-2017-audit-is-pdf-p147691

ÚŘAD VLÁDY ČESKÉ REPUBLIKY, 2017. Aplikace VeKLEP – *Návrh zákona o zpracování osobních údajů* [online]. Česká republika ©2018 [cit. 2017-11-29].
Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, 2017. *Úplné znění statutu Vysokého učení technického v Brně* [online]. Brno: VUT [cit. 2017-11-29].
Dostupné z: https://www.vutbr.cz/uredni-deska/vnitrni-predpisy-a-dokumenty/-d128667/uplne-zneni-statutu-vut-p135509

Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) ze dne 15. prosince 2014.

WAGNEROVÁ, I., 2008. *Hodnocení a řízení výkonnos*ti. Praha: Grada, 117 s. ISBN: 978-80-247-2361-7

Zákon č. 563/1991 Sb., o účetnictví ze dne 12. prosince 1991.

Zákon č. 101/2000 Sb., o ochraně osobních údajů ze dne 4. dubna 2000.

Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel, Zákon č. 53/2004 Sb.) ze dne 12. dubna 2000.

Zákon č. 187/2006 Sb., o nemocenském pojištění ze dne 14. března 2006.

Zákon č. 262/2006 Sb., zákoník práce ze dne 21. dubna 2006.

Zákon č. 468/2011 Sb., kterým se mění zákon č. 127/2005 o elektronických komunikacích ze dne 6. prosince 2011.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

AP	Access Point
BMC	Bussines Continuity Management
CRM	Customer Relationship Management
CVIS	Centrum výpočetních a informačních služeb při VUT v Brně
DMZ	Demilitarizovaná zóna
DR	Disaster Recovery
GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IS	Informační System
ISP	Internet Service Provider
IT	Informační Technologie
MAC	Media Access Control
MRP	Media Redundancy Protocol
PC	Personal Computer
RČ	Rodné číslo
SAML	Security Assertion Markup Language
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Socket Layer
STP	Spaning Tree Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VUT	Vysoké učení technické v Brně

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHY

Přílohy jsou vzhledem ke své povaze umístěny na následující prázdné stránce.

Příloha A: Pravidla údržby a provozu ochrany osobních údajů v síti KolejNet
(Vlastní zpracování)

Čj.: XXX/XXXX/XX

V Brně, dne 14. 04. 2018

Rozdělovník: XYZ

Zpracoval: Krýzová Lenka

Směrnice XXX č. XX/XXXX

PRAVIDLA ÚDRŽBY A PROVOZU OCHRANY OSOBNÍCH ÚDAJŮ V SÍTI KOLEJNET

Článek 1

Základní ustanovení

1. **Osobní údaje** jsou veškeré informace, pomocí nichž můžeme identifikovat fyzickou osobu. Taková fyzická osoba je pak považována za **subjekt údajů**.

2. **Správce osobních údajů** systematicky a účelně zpracovává, na základě uděleného souhlasu, osobní údaje subjektu údajů.

3. **Zpracovatel** zpracovává osobní údaje pro správce osobních údajů.

4. **Zpracováním** se pak rozumí jakákoliv činnost správce nebo zpracovatele, kdy je manipulováno s osobními údaji.

5. **Pověřenec osobních údajů (anglicky Data Protection Officer)** je osoba, jež zodpovídá především za komunikaci s dozorovými orgány.

6. **Posouzení vlinu na ochranu osobních údajů (anglicky Data Protection Impact Assessment)** zahrnuje analytické činnosti jako audit, analýzu ISMS a jiné, které posuzují stav informačního systému a jeho okolí a slouží jako podklad pro správu, zabezpečení a provoz informačního systému.

Článek 2

Provoz

1. **Provozem**, se míní všechny procesy probíhající ve všech organizačních jednotkách Vysokého učení technického v Brně

2. Každá z těchto jednotek zpracovává osobní údaje svých zaměstnanců, uživatelů a jiných fyzických osob. Takové zpracování je provozováno na základě zákona 101/2000 Sb. v aktuálním znění a nařízení Evropské unie 2016/679 (GDPR).

3. Každý správce osobních údajů, jejich zpracovatel a také subjekt údajů se řídí výše uvedenou legislativou při vykonávání činností souvisejících se zpracováním osobních údajů, tak aby nedošlo k neoprávněnému zasahování do soukromého a rodinného života a neoprávněnému shromažďování, zveřejňování nebo jinému zneužívání údajů o dané osobě.

4. Správce zpracovává osobní údaje na základě souhlasu subjektu údajů, pokud neexistuje jiný oprávněný zájem.

5. Správce má povinnost obnovovat souhlas subjektu údajů, pokud osobní údaje zpracovává po delší dobu.

7. Správce má povinnost informovat subjekt údajů o tom, jaké údaje budou zpracovávány, jakým způsobem a za jakým účelem je bude zpracovávat. Subjekt údajů také musí získat informace o všech jeho právech, včetně informací o správci a jeho případném zástupci. To vše, ještě před udělením souhlasu subjektu údajů.

Článek 3

Údržba

1. Správce má povinnost technicky osobní údaje **zabezpečit** a udržovat toto zabezpečení, pomocí aktivní správy a pravidelné kontroly.

2. Správce zajistí trasovatelnost osobních údajů pro dané oddělení, tedy vede **dokumentaci** o tom, jak osobní údaje zpracovává při průchodu provozem. Správce je také schopen tyto materiály doložit, a to včetně souhlasu subjektu údajů.

3. Správce zajišťuje archivaci dokumentů dle aktuálně platné legislativy.

4. Správce pro dané oddělení jmenuje **pověřence pro ochranu osobních údajů**, ten následně komunikuje s nadřízenými pracovníky nebo dozorovými úřady, ve věcech týkajících se zajištění ochrany osobních údajů.

5. Správce zabezpečuje aktualizaci interních pravidel, řádů a nařízení, jsou-li provedeny nějaké změny v organizaci nebo mimo ni (např. novelizace zákonů).

6. Správce je povinen informovat subjekt údajů, pokud hodlá předat osobní údaje do třetí země nebo třetí straně.

Článek 4

Definice

1. Oddělení KolejNet zpracovává následující osobní údaje: jméno a příjmení, e-mail v doméně KN a případně kontaktní e-mail, IP adresu, přihlašovací jméno, identifikátor uživatele KN, identifikátor uživatele IS VUT a rodné číslo.

2. Správcem těchto údajů je VUT v Brně a všechny jeho organizační součásti.

3. VUT v Brně neposkytuje osobní údaje třetím stranám.

4. Zpracovatel je každý externí subjekt, který pro VUT v Brně zpracovává osobní údaje.

5. Oddělení KolejNet zpracovává osobní údaje na základě odstavce 48, oprávněného zájmu správce (zde VUT), kdy jsou data přenositelná v rámci organizace.

6. Oddělení KolejNet zpracovává osobní údaje na základě odstavce 49 nařízení GDPR, který umožňuje zpracovávání jako oprávněný zájem správce pro zajištění bezpečnosti sítě a komunikace.

7. Oddělení KolejNet zpracovává osobní údaje na základě odstavce 47 nařízení GDPR, kdy vzniká oprávněný zájem správce na zpracování v případě, že existuje odpovídající vztah mezi subjektem údajů a správcem (zákazník a poskytovatel služeb).

8. Neexistují žádní další příjemci ani kategorie příjemců osobních údajů oddělení KolejNet.

9. Osobní údaje, které oddělení KolejNet zpracovává, jsou rozděleny do kategorií obecné osobní údaje a zvláštní osobní údaje.

10. Oddělení KolejNet nezpracovává žádné zvláštní osobní údaje.

Článek 5

Závěrečná ustanovení

1. Všechny prvky, včetně lidských zdrojů, související s ochranou osobních údajů jsou udržovány ve stavu, kdy je dodržováno vše stanovené v těchto pravidlech, nebo v aktuálně platné legislativě.

2. Dále všechny zúčastněné subjekty dodržují také ostatní pravidla pro správu a provoz počítačové sítě VUT a Prohřeškový řád sítě KolejNet, v souladu s těmito pravidly.

3. Každý subjekt pak musí být prokazatelně obeznámen s těmito pravidly.

4. Tyto pravidla nabývají účinnosti dne XX. YY. ZZZZ.

Schválil

Pracovní pozice

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ CENTRUM VÝPOČETNÍCH A INFORMAČNÍCH SLUŽEB

Příloha B: Řád ochrany osobních údajů v síti KolejNet
(Vlastní zpracování)

Čj.: XXX/XXXX/XX

V Brně, dne 14. 04. 2018

Rozdělovník: XYZ

Zpracoval: Krýzová Lenka

Směrnice XXX č. XX/XXXX

ŘÁD OCHRANY OSOBNÍCH ÚDAJŮ V SÍTI KOLEJNET

Článek 1

Základní ustanovení

1. **Tento řád je platný pro všechny uživatele sítě KolejNet a také pro zaměstnance tohoto oddělení.**

2. **Osobní údaje** jsou veškeré informace, pomocí nichž můžeme identifikovat fyzickou osobu. Taková fyzická osoba je pak považována za **subjekt údajů**.

3. **Správce osobních údajů** systematicky a účelně zpracovává, na základě uděleného souhlasu, osobní údaje subjektu údajů.

4. **Zpracovatel** zpracovává osobní údaje pro správce osobních údajů.

5. **Zpracováním** se pak rozumí jakákoliv činnost správce nebo zpracovatele, kdy je manipulováno s osobními údaji.

6. Souhlas je svobodný, konkrétní, informovaný a jednoznačný projev vůle subjektu údajů.

6. **Pověřenec osobních údajů** (anglicky Data Protection Officer) je osoba, jež zodpovídá především za komunikaci s dozorovými orgány.

7. **Posouzení vlinu na ochranu osobních údajů (anglicky Data Protection Impact Assessment)** zahrnuje analytické činnosti jako audit, analýzu ISMS a jiné, které posuzují stav informačního systému a jeho okolí a slouží jako podklad pro správu, zabezpečení a provoz informačního systému.

8. Tento řád stanovuje práva subjektů údajů, jejich další oprávněné zájmy a možnosti ve věcech ochrany osobních údajů.

Článek 2

Zpracování a souhlas se zpracováním

1. Oddělení KolejNet zpracovává osobní údaje subjektů údajů za účelem poskytování služeb připojení do sítě KolejNet. Bez těchto údajů nelze řádně provádět správu a údržbu počítačové sítě KolejNet.

2. Tyto údaje jsou zpracovávány na základě souhlasu subjektů údajů. Před udělením souhlasu je subjekt údajů obeznámen se svými právy.

3. Souhlasem umožňuje subjekt údajů zpracování svých osobních údajů správci osobních údajů.

4. Souhlas je udělován elektronickou formou.

5. Souhlas udělený před nasazením nařízení GDPR do organizace je neplatný, pokud nesplňuje požadavky nařízení GDPR a novely zákona č. 101/2000 Sb.

6. Souhlas je ve stanovených intervalech obnovován a to z důvodu zajištění jeho zákonnosti.

7. Subjekt údajů má právo svůj souhlas kdykoliv odvolat dopisem doručeným vedoucímu pracovníkovi oddělení sítě KolejNet.

Článek 3

Práva subjektu údajů

6. Právo na přístup k osobním údajům.

MODELOVÁ SITUACE:

Na základě aktivní žádosti subjektu údajů, má subjekt údajů oprávnění získat informace o zpracovávání a informace o zpracovávaných údajích, včetně dalších doplňujících informací (uvedeno v čl. 15, EU 2016/679).

7. Právo na opravu nebo doplnění osobních údajů, které však neznamená aktivní vyhledávání chybných osobních údajů správcem osobních údajů.

MODELOVÁ SITUACE:

Zpracovávané údaje týkající se konkrétního subjektu údajů jsou nepřesné, subjekt údajů upozorní správce na nepřesnosti a správce je povinen se žádostí na opravu zabývat.

8. Právo na výmaz osobních údajů vzniká, je-li zpracování osobních údajů protiprávní.

MODELOVÁ SITUACE:

Správce nezpracovává osobní údaje zákonným způsobem (jedná protiprávně), subjekt údajů má právo požadovat výmaz osobních údajů ze všech úložišť správce osobních údajů, včetně úložišť zpracovatelů, třetích stran atd. a odkazů.

9. Právo na omezení zpracování vzniká, je-li zpracování osobních údajů protiprávní.

MODELOVÁ SITUACE:

Správce nezpracovává osobní údaje zákonným způsobem (jedná protiprávně), avšak subjekt údajů odmítá výmaz osobních údajů a chce nadále využívat služby správce. Subjekt údajů může využít právo na omezení zpracování.

10. Právo vznést námitku vzniká, nelze-li uplatnit právo na výmaz osobních údajů.

MODELOVÁ SITUACE:

Nelze-li uplatnit právo na výmaz, poté lze tímto krokem donutit správce údajů (např. společnost) k omezenému zpracování předmětných osobních údajů.

11. Právo na přenositelnost údajů, pokud má subjekt údajů v úmyslu předat osobní údaje jinému správci.

MODELOVÁ SITUACE:

Za podmínek automatizovaného zpracování na základě souhlasu nebo smlouvy, může subjekt údajů získat své osobní údaje ve strukturovaném, běžně používaném a strojově čitelném formátu a předat je jinému správci.

12. Právo nebýt předmětem automatizovaného individuálního rozhodování s právními či obdobnými účinky, včetně profilování.

MODELOVÁ SITUACE:

Toto právo zajišťuje, aby nebylo o právních účincích rozhodováno automatizovanými postupy bez lidské přítomnosti. Příkladem může sloužit

situace, kdy nelze pokutovat řidiče překračujícího rychlost jízdy, aniž by přestupek nebyl přezkoumán člověkem.

13. Všechny opravy a jiné úkony, sdělení a podané informace se poskytují bezplatně.

Článek 4

Chování uživatele při práci s výpočetní technikou a informačním systémem

1. Uživatel nesděluje přístupové heslo do IS jiným osobám.

2. Uživatel by neměl otevírat a odpovídat na podezřelé e-mailové zprávy.

3. Uživatel nezasílá svá hesla a přihlašovací jména skrze nezabezpečený komunikační kanál.

4. Uživatel volí dostatečně dlouhé heslo, které není snadno uhodnutelné (datum narození, jméno nebo příjmení…).

5. Uživatel by měl vlastní důležitá data pravidelně zálohovat.

6. Uživatel dbá na to, aby nezavlekl virovou nákazu do systému.

7. Uživatel by měl informovat správce, pokud odhalí nedostatek v zabezpečení systému.

Článek 5

Závěrečná ustanovení

1. Tento řád následuje aktuální legislativní úpravu Evropské unie, jež jsou povinni dodržovat všechny členské státy a také aktuální právní úpravu České republiky.

2. Všechny body tohoto řádu platí bez rozdílu, pro každou fyzickou osobu.

3. Každý subjekt by měl být obeznámen s těmito pravidly.

4. Tyto pravidla nabývají účinnosti dne XX. YY. ZZZZ.

Schválil

Pracovní pozice

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
CENTRUM VÝPOČETNÍCH A INFORMAČNÍCH SLUŽEB

Příloha C: Schéma toku konkretizovaných dat
(Vlastní zpracování)

Čj.: XXX/XXXX/XX

V Brně, dne 14. 04. 2018

Rozdělovník: XYZ

Zpracoval: Krýzová Lenka

Schéma XXX č. XX/XXXX

SCHÉMA TOKU KONKRETIZOVANÝCH DAT

1. Toto schéma znázorňuje tok konkretizovaných dat (uživatelských osobních údajů/dat subjektu údajů).

2. **Osobní údaje** jsou veškeré informace, pomocí nichž můžeme identifikovat fyzickou osobu. Taková fyzická osoba je pak považována za **subjekt údajů**. Subjekt údajů poskytuje své osobní údaje při úvodní registraci k pobytu na kolejích VUT nebo při podání přihlášky ke studiu na VUT.

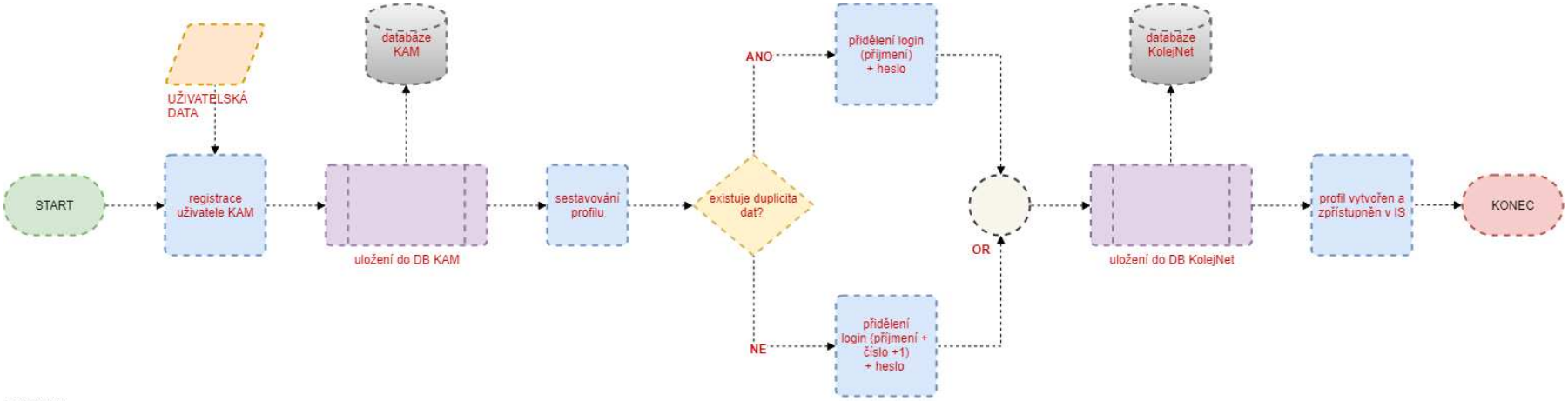
3. Tok dat je znázorněn vývojovým diagramem s legendou, tato legenda znázorňuje význam jednotlivých grafických značek.

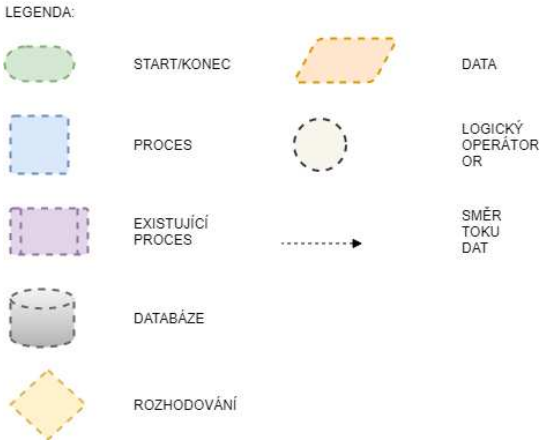
4. Data jsou zpracovávána v rámci jedné organizace (VUT) a slouží především pro vnitřní administrativní účely a poskytování služeb zákazníkům.

5. Oprávněné zájmy správce (oddělení KolejNet) jsou definovány odstavci 47, 48 a 49 nařízení GDPR.

6. Zpracovávané údaje a operace s nimi, jsou minimální možné a nezbytné k zajištění bezpečnosti sítě, včetně jejího správného provozu. Rozsah je také uzpůsoben pro požadavky vnitrostátní legislativy.

7. Vznik rizika pro práva a svobody subjektu údajů je co nejvíce minimalizován. V případě vzniku rizika jsou nasazena plánovaná opatření k zajištění ochrany osobních údajů, v souladu s nařízením GDPR.


START
UŽIVATELSKÁ DATA
registrace uživatele KAM
databáze KAM
uložení do DB KAM
sestavování profilu
existuje duplicita dat?
ANO
přidělení login (příjmení) + heslo
NE
přidělení login (příjmení + číslo +1) + heslo
OR
databáze KolejNet
uložení do DB KolejNet
profil vytvořen a zpřístupněn v IS
KONEC


LEGENDA:
START/KONEC
DATA
PROCES
LOGICKÝ OPERÁTOR OR
EXISTUJÍCÍ PROCES
SMĚR TOKU DAT
DATABÁZE
ROZHODOVÁNÍ