Specifika ochrany osobních údajů ve vybrané organizaci

Tomáš Vojkůvka

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš Vojkůvka**
Osobní číslo:	**A16055**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Specifika ochrany osobních údajů ve vybrané organizaci**
Téma anglicky:	**Specifics of Privacy in Selected Organization**

Zásady pro vypracování:

1. **Analyzujte základní legislativní požadavky na ochranu osobních údajů v organizaci.**
2. **Vytvořte model organizace, u nějž budete posuzovat specifika ochrany osobních údajů. V navržené organizaci proveďte analýzu rizik spojených s ochranou osobních údajů.**
3. **Analyzujte systém ochrany osobních údajů v organizaci. Zaměřte se na role, procesy a dokumenty. Posuďte, jak jsou hlavní rizika řešena.**
4. **Identifikujte specifika a bezpečnostní problémy ochrany osobních údajů organizace. Navrhněte řešení identifikovaných bezpečnostních problémů.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **NEJEDLÝ, Josef. Ochrana osobních údajů. Vyškov: Irena Spirová, 2004. ISBN 80-239-3896-7.**
2. **MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012. ISBN 978-80-87576-12-0.**
3. **BARTÍK, Václav a Eva JANEČKOVÁ. Zpracování osobních údajů školami. Praha: Wolters Kluwer Česká republika, 2013. ISBN 978-80-7478-359-3.**
4. **MENDROK, Eva, Tomáš VAVRO a Marek ZEMAN. Školy a ochrana osobních údajů podle GDPR. Praha: Verlag Dashöfer, 2018. ISBN 978-80-87963-59-3.**
5. **ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. ISBN 978-80-7554-152-9.**
6. **NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. 2. vydání. Praha: Wolters Kluwer, 2018. ISBN 978-80-7598-068-7.**
7. **E-government a GDPR: (soubor zákonů). Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-717-7.**
8. **KATZOVÁ, Pavla. Školský zákon: komentář. Praha: ASPI, 2008. ISBN 978-80-7357-412-3.**

Vedoucí bakalářské práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **20. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 20. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Abstrakt česky

Bakalářská práce „Specifika ochrany osobních údajů v organizaci“ se zabývá systémem ochrany osobních údajů, včetně legislativních požadavků. Práce je členěna do dvou částí. Teoretická část se zabývá obecným nařízením o ochraně osobních údajů, které udává správcům různá práva a povinnosti při zpracování těchto údajů. Dále zde jsou analyzovány specifika zpracování osobních údajů ve školství. Praktická část analyzuje cíle, podstatu a způsob realizace administrativy, včetně elektronické databáze.

Klíčová slova: osobní údaj, ochrana osobních údajů, školství, bezpečnost, administrativa, evidence, analýza rizik, technické zabezpečení

ABSTRACT

Abstrakt ve světovém jazyce

The bachelor's thesis "Specifics of personal data protection in the organization" deals with the system of protection of personal data, including the legislative requirements. The work is divided into two parts. The theoretical part deals with the general regulation on personal data protection, which gives administrators different rights and responsibilities when processing these data. Further, there are analyzed the specifics of the processing of personal data in education. The practical part analyzes the objectives, the nature and the method of implementation of the presidential administration, including an electronic database.

Keywords: personal data, protection of personal data, education, safety, administration, registration, risk analysis, technical security

Rád bych touto cestou poděkoval panu doc. Ing. Luďkovi Lukášovi, CSc. za jeho ochotu, cenné rady a inspiraci při pravidelných konzultacích ohledně této bakalářské práce. Dále bych chtěl poděkovat své rodině za veškerou podporu a trpělivost během mého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD **9**

I TEORETICKÁ ČÁST **10**

1 ZÁKLADNÍ POJMY SPOJENÉ S GDPR **11**

1.1 Osobní údaj 11

1.2 Soukromí 11

1.3 Zpracování osobních údajů 12

1.4 Správce 12

1.5 Zpracovatel 13

1.6 Citlivý údaj 13

2 LEGISLATIVA A HLAVNÍ PŘÍNOSY GDPR **14**

2.1 Legislativa EU 14

2.2 Legislativa ČR 15

2.3 Hlavní přínosy nařízení 16

3 PRÁVNÍ DŮVODY A POVINNOSTI SPRÁVCE PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ **17**

3.1 Právní důvody pro zpracování osobních údajů 17

3.2 Záznamy o činnostech zpracování 18

3.3 Jmenování pověřence pro ochranu osobních údajů 18

3.4 Posouzení vlivu na ochranu osobních údajů 19

3.5 Předchozí konzultace s dozorovým úřadem 19

3.6 Legislativa spojená se zpracováním osobních údajů ve škole či školském zařízení 20

3.7 Školní matrika 24

3.8 Zabezpečení zpracování osobních údajů 25

4 MODEL ORGANIZACE, U NĚJŽ BUDETE POSUZOVAT SPECIFIKA OCHRANY OSOBNÍCH ÚDAJŮ. **27**

4.1 Charakteristika organizace 27

4.2 Organizační struktura organizace 29

4.3 Pověřenec pro ochranu osobních údajů 32

4.4 Analýza rizik spojená se zpracováním osobních údajů na škole 32

5 PROZKOUMÁNÍ ADMINISTRATIVY NA SPŠ BYSTŘICE POD HOSTÝNEM **38**

5.1 SPRÁVNÍ ŘÍZENÍ 38
5.2 EVIDENCE ŽÁKŮ 39
5.3 PŘIHLÁŠKY KE STRAVOVÁNÍ 40
5.4 PŘIHLÁŠKY DO PROJEKTU ERASMUS 40
5.5 ÚČETNICTVÍ A HOSPODÁŘSKÁ ČINNOST 41
6 UCHOVÁVÁNÍ DOKUMENTŮ S OSOBNÍMI ÚDAJI NA SPŠ BYSTŘICE POD HOSTÝNEM 42
6.1 ELEKTRONICKÁ DATABÁZE 42
6.2 FYZICKÁ ADMINISTRATIVA 44
7 ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ NA SPŠ BYSTŘICE POD HOSTÝNEM 46
7.1 RIZIKA SPOJENÁ SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ NA SPŠ BYSTŘICE POD HOSTÝNEM 46
7.2 DOSAVADNÍ ZABEZPEČENÍ 47
7.2.1 Přístup do objektu 47
7.2.2 Zranitelné místnosti a jejich zabezpečení 48
7.2.3 Komunikační a elektronická bezpečnost 49
7.3 IDENTIFIKOVATELNÉ PROBLÉMY 49
7.4 ZHODNOCENÍ ZABEZPEČENÍ A PŘÍPADNÝ NÁVRH ZLEPŠENÍ 49
ZÁVĚR 52
SEZNAM POUŽITÉ LITERATURY 53
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 55
SEZNAM OBRÁZKŮ 56
SEZNAM TABULEK 57

ÚVOD

Práce se zabývá problematikou „Obecného nařízení o ochraně osobních údajů“ neboli General Data Protection Regulation (dále jen GDPR), jenž oficiálně nabylo platnosti 25. května 2018 v celé Evropské unii.

Bakalářská práce je rozdělena na část teoretickou a část praktickou. V teoretické části jsou v první řadě rozebrány základní pojmy spojené s GDPR a její legislativní požadavky na správce či zpracovatele, pracující s osobními údaji. Dále jsou zde zmíněny práva a povinnosti při zpracování osobních údajů a v neposlední řadě právní důvody ke zpracování. V další části teoretického segmentu je uvedena legislativa spojená se zpracováním osobních údajů ve škole či školském zařízení a obecně popsána školní matrika.

V praktické části se nachází model organizace, u nějž jsou specifikovány jednotlivé aspekty související se zpracováním osobních údajů. Objekt byl zvolen z oblasti školství, konkrétně střední průmyslová škola (dále jen SPŠ) v Bystřici pod Hostýnem. Dále je zde vypracována analýza rizik spojená se zpracováním osobních údajů na SPŠ v Bystřici pod Hostýnem. Ta popisuje veškeré hrozby, které mohou nastat, jejich následky a míra pravděpodobnosti s jakou se tyto hrozby mohou uskutečnit. Analýza rizik byla specifikována tak, aby se vztahovala čistě k řešené problematice. Praktická část se dále zabývá konkrétně zpracováním osobních údajů ve vybrané organizaci. Je zde rozebrána veškerá administrativa obsahující osobní údaje žáků, učitelů, zaměstnanců či zákonných zástupců žáků. Jsou zde uvedeny veškeré vedené dokumenty na škole i vedená databáze v elektronické podobě a posouzeno jejich stávající zabezpečení. Poslední část této práce osahuje zhodnocení stávajícího zabezpečení a návrh řešení identifikovaných problémů.

V průběhu posledních dvou let se na tuhle problematiku klade mnohonásobně větší důraz. Dle mého názoru je to dáno rapidním vývojem výpočetních systémů a přechodem na dokumentaci elektronickou formou. Většina firem, škol či různě rozrostlé společnosti vedou veškerou agendu svých klientů, zaměstnanců nebo studentů především v elektronické podobě. To je také příčinou proč pod GDPR spadají i určité technické parametry jako například cookies v jednotlivých zařízeních. Ovšem zapomínat se nesmí i na papírovou dokumentaci, která se musí vést a archivovat po určitou dobu.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY SPOJENÉ S GDPR

Legislativní forma ochrany osobních údajů používá několik specifických pojmů a výrazů. Tyto pojmy jsou používány denně, avšak v právní formě nabývají úplně jiných významů. Proto je potřeba si základní pojmy v oblasti ochrany osobních údajů definovat.

1.1 Osobní údaj

Tento pojem se užívá pro jakoukoliv informaci o identifikované nebo identifikovatelné osobě. Takovou osobou je fyzická osoba, kterou můžeme přímo nebo nepřímo identifikovat. Především se to týká takzvaných identifikátorů, což může být jméno, rodné číslo, síťový identifikátor apod. Ale osobu také můžeme identifikovat pomocí zvláštních prvků fyzické, fyziologické, genetické, psychické, kulturní, společenské nebo ekonomické identity dané fyzické osoby. [1]

Výše bylo poukázáno na to, že identifikace fyzické osoby může nastat pomocí identifikátorů, které mohou být nejen jméno, příjmení, adresa a datum narození, ale třeba i kód, který se přiděluje zaměstnancům ve firmách. Další důležitá skutečnost, co se týče osobních údajů, je, že účinnost zákona o ochraně osobních údajů nastává až při samotném zpracování osobních údajů. [1]

1.2 Soukromí

Na pojem soukromí se můžeme dívat z několika hledisek. Lze tento pojem popsat jako určitou oblast každého člověka, jednotlivce nebo skupiny lidí například rodiny, kterou si každý chrání před zveřejněním, a hlavně před zneužitím. [2]

Ochranu soukromí v České republice zaručuje Listina základních práv a svobod, což je část ústavního pořádku České republiky. Po případném narušení soukromí si vše do svých rukou bere trestní zákoník, který tuhle problematiku řeší ve své druhé hlavě, zabývající se trestnými činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství. [2]

1.3 Zpracování osobních údajů

„Zpracování je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je 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.“ [1]

Výše byla uvedena přesná definice pojmu zpracování osobních údajů, která je z článku 4 odst. 1 obecného nařízení. Ovšem není možné tuhle skutečnost chápat jako jakékoli nakládání s osobními údaji. O zpracování osobních údaji se mluví tehdy, když správce nakládá s osobními údaji z určitého důvodu za určitým účelem.[3]

Zpracování, jakožto definice tohohle pojmu, má stejný význam jako měla v zákoně č. 101/2000 Sb., o ochraně osobních údajů. [3]

1.4 Správce

Správcem osobních údajů (dále jen správce) je určitý subjekt, jakékoliv právní formy, který je hlavní odpovídající za zpracování osobních údajů. Tento subjekt určuje účely a prostředky pro zpracování osobních údajů. Správce zpracovává osobní údaje pro účely vyplývající z jeho činnosti, například zákonem stanovené povinnosti. Ovšem může je zpracovávat i pro vlastní účely, nesmí ovšem přesahovat zájem na ochraně základních práv a svobod fyzických osob. [4]

Správcem může být kdokoliv. Pokud zpracovává osobní údaj fyzická osoba, musí to dělat takovým způsobem, aby nešlo o nakládání osobních údajů, které nesplňuje jejich definici zpracování. V případě zpracování osobních údajů, kde správcem je právnická osoba, nese odpovědnost za zpracování dotyčná právnická osoba, nikoli její některý zaměstnanec, společník nebo například jednatel. [4]

Tento pojem nebyl změněn oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů. [4]

1.5 Zpracovatel

Tento subjekt je najat správcem za účelem, aby pro něj prováděl zpracovatelské operace s určitými osobními údaji. Dalo by se říct, že pro něj dělá práci, kterou by měl zpracovávat on sám. Tudíž zpracovává určité osobní údaje, které jsou mu zadány. Najímání zpracovatele není nutný postup při zpracování osobních údajů. Správce si tohle řešení může dělat sám. [5]

Zpracovatel nakládá pouze s údaji, poskytnutými správcem a takovými operacemi, jenž mu správce zadá, nebo s takovými, které vyplývají z činnosti, pro nějž byl zpracovatel pověřen. Jak správce, tak zpracovatel mohou být subjekty jakékoliv právní formy. [5]

Tento pojem nebyl změněn oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů. [5]

1.6 Citlivý údaj

Jedná se o speciální kategorii podle nařízení GDPR. V případě, kdy zpracovatel či správce zpracovává tyto citlivé údaje, podléhají mnohem přísnějšímu režimu opatření, než je tomu u obecných údajů. V případě citlivých údajů se může jednat například o zdravotní stav subjektu údajů, rasovém či etnickém původu, politické názory, filozofické či náboženské vyznání, sexuální orientaci nebo trestních deliktech. Jedná se tedy o údaje, které mohou subjekt údajů poškodit ve společnosti, ve škole či zaměstnání a v nejhorších případech mohou zapříčinit jeho diskriminaci. [6]

2 LEGISLATIVA A HLAVNÍ PŘÍNOSY GDPR

Jelikož nařízení GDPR platí pro celou Evropskou Unii (dále jen EU), je třeba se na tuhle problematiku podívat zvlášť pro EU a zvlášť pro ČR.

2.1 Legislativa EU

Co se týče mezinárodních dokumentů, ochrana osobních údajů se vyvíjí již několik desítek let. První významné poznatky o ochraně osobních údajů v mezinárodních dokumentech jsou z 80. let 20. století. Prvním platným dokumentem o ochraně osobních údajů se stala úmluva č. 108. [7]

Úmluva č. 108 byla přijata 28. ledna 1981 ve Štrasburku. Čtyři roky poté vstoupila v platnost, kdy ji ratifikovalo prvních 5 členských států Rady Evropy. [7]

Revoluční změny přišly dne 27. dubna roku 2016, kdy na základě nařízení Evropského parlamentu a Rady (EU) 2016/679, z téhož dne, se ochrana fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice, mění. Tohle nařízení nabylo platnosti dne 25. května 2018. [8]

Přesná definice nařízení:

„Nařízení se dotýká všech subjektů zpracovávajících osobní údaje, a to napříč odvětvími. Nahrazuje předchozí právní úpravu - Směrnici 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.“[9]

Nová pravidla obecného nařízení o ochraně osobních údajů byla přijata tzv. formou evropského nařízení. To znamená, že nabyde jednotné platnosti ve všech státech EU tak, aby národní vlády a zákonodárci s nimi nemohli jakkoli manipulovat, ohýbat a přizpůsobovat místním zájmům nebo lobbistům. [10]

Evropská Rada chce tímto maximalizovat bezpečí osobních údajů a minimalizovat případy zneužívání osobních údajů v rámci celé Evropské Unie. Postupně budou zmíněny některé novinky, které GDPR přináší. Jsou to například případy, kdy subjekt má právo na přenositelnost osobních údajů nebo zavedení institutu pověřence pro ochranu osobních údajů. Musí být také důkladně informováni o svých právech co se týče ochrany osobních údajů. [10]

2.2 Legislativa ČR

V České republice upravoval zpracování a ochranu osobních údajů zákon č. 101/2000 Sb., o ochraně osobních údajů. Z toho vyplývá že od roku 2000 se každá organizace musela řídit tímto zákonem při zpracování osobních údajů. Za revoluční změny bychom mohli považovat obecné nařízení a jeho přímou použitelnost v celé Evropské unii.

Především se musí definovat, co přesně znamená obecné nařízení o ochraně osobních údajů, o které se hovořilo v předchozí kapitole.

„Obecné nařízení představuje aktualizovaný právní rámec ochrany osobních údajů v evropském prostoru, který bude od 25. května 2018 přímo stanovovat pravidla pro zpracování osobních údajů, včetně práv subjektu údajů (fyzické osoby). V českém právním prostředí tak obecné nařízení od 25. května 2018 nahradí zákon č. 101/2000 Sb., o ochraně osobních údajů, který v současné době stanovuje povinnosti a práva při zpracování osobních údajů.“ [11]

Z výše uvedeného nařízení vyplývá, že veškerá práva a povinnosti při zpracování osobních údajů, ze zákona č. 101/2000 Sb., o ochraně osobních údajů, jsou nahrazeny těmito novými právy a povinnostmi, které vychází z nařízení GDPR. Obecné nařízení se stalo podnětem pro vytvoření nového zákona č. 110/2019 Sb., o zpracování osobních údajů, který zpracovává příslušné předpisy Evropské unie. Zároveň nahrazuje předešly zákon č. 101/2000 Sb., o ochraně osobních údajů. Ve většině případů tohle nařízení nemění základní zásady zpracování osobních údajů nebo definice základních pojmů, například osobní údaj, správce, zpracovatel apod, avšak na některé subjekty klade vyšší nároky při zpracování osobních údajů. Týká se to především velkých správců osobních údajů. Tím jsou například banky, telekomunikační operátoři atd. Tímto jsou myšleni správci, kteří zpracovávají rozsáhlé množství osobních údajů. Na druhou stranu obecné nařízení nepřináší revoluční změny oproti stávající úpravě týkajících se drobných živnostníků, kteří zpracovávají osobní údaje svých zákazníků pouze za účelem poskytnutí služby či výrobku. [11]

2.3 Hlavní přínosy nařízení

Jedním z nejdůležitějších přínosů nařízení je právo subjektu osobních údajů, vznést námitku proti zpracování, kdy správce musí tohle zpracování údajů ukončit, nemá-li k tomu závažné, prokazatelné důvody, aby tohle ukončení nevykonal. Subjekt údajů by měl mít přístup k údajům, které jsou o jeho osobě shromažďovány. Přístup k těmto údajům by měl být nejlépe přímý a online. S touto novinkou souvisí další nový element, a to je právo na výmaz osobních údajů, což může být dále rozšířeno na právo být zapomenut. To znamená, že osoba může požadovat, aby byly vymazány její osobní údaje, jestliže neexistuje určitý právní důvod pro pokračování jejich zpracování. [12, 14]

Pod GDPR nově spadají i některé technické parametry. Jako jsou například IP adresy, e-maily nebo například cookies v určitém zařízení. Přísnější nařízení se dotkne nové kategorie a to je tzv. genetické a biometrické údaje. [12]

Jedna z nejzásadnějších novinek je oznamovací povinnosti v případě narušení bezpečnosti údajů. Což znamená, že zpracovatel je nucen ohlásit únik či ohrožení zabezpečení osobních dat Úřadu pro ochranu osobních údajů, a to v průběhu 72 hodin od okamžiku, kdy se o téhle skutečnosti dozvěděl. V určitých případech o téhle skutečnosti musí informovat osoby a subjekty, kterých se tato skutečnost týkala. [12]

GDPR se tímto krokem snaží o co největší vymahatelnost práva v ochraně osobních údajů. Klade také důraz na aktivnější přístup správců a zpracovatelů.

„*Zejména se jedná o to, že před zahájením nového zpracování je třeba posoudit vliv jednotlivých zpracování na ochranu osobních údajů a zvolit vhodné nástroje ochrany údajů.“* [12]

3 PRÁVNÍ DŮVODY A POVINNOSTI SPRÁVCE PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Součástí uzákonění obecného nařízení GDPR ze dne 25. května 2018 byl přístup založený na riziku, který se týká především správců při zpracování osobních údajů. Tento koncept znamená, že správce již od samotného počátku zpracování osobních údajů musí v první řadě brát zřetel na účel a důvody zpracování, rozsah, povahu, kontext a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a od toho se také odvíjet zabezpečení osobních údajů.[13]

V souvislosti s obecným nařízením má správce navíc několik nových povinnosti, které se vztahují ke zpracování osobních údajů. Tyto povinnosti se aktualizovaly z důvodu vysokého rizika práv a svobody fyzické osoby při zpracování osobních údajů. O těchto nových povinnostech nelze hovořit, že se vztahují na všechny správce. [13]

3.1 Právní důvody pro zpracování osobních údajů

Právní důvody správce pro zpracování osobních údajů jsou nezbytným předpokladem k vykonávání této činnosti. Každý správce musí disponovat řádným právním důvodem ke zpracování osobních údajů. Správce může tyto údaje zpracovávat za různými účely, ovšem pro každý jednotlivý účel potřebuje právní důvod pro jeho zpracování. Právní důvody se určují na základě účelů, pro který jsou osobní údaje zpracovávány. Dále je správce povinen likvidací osobních údajů v momentě, kdy vykoná poslední právní důvod ke zpracování osobních údajů.[15]

Právní důvody pro zpracování osobních údajů jsou:

- Zpracování osobních údajů je nezbytnou součástí smlouvy, jejíž smluvní stranou je právě subjekt osobních údajů, nebo v případě nezbytného provedení přijatých opatření před uzavřením smlouvy na žádost právě subjektu osobních údajů,
- na správce se vztahují právní povinnosti nezbytné pro zpracování osobních údajů, což je jeden z právních důvodů ke zpracování,
- pokud je zpracování nezbytností pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování osobních údajů je nezbytností pro splnění prováděného úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen,

- pokud je zpracování nezbytností pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy předností před těmito zájmy jsou zájmy nebo základní práva a svobody subjektu osobních údajů vyžadující ochranu osobních údajů. [15]

3.2 Záznamy o činnostech zpracování

Správce je povinen, dle GDPR, vést záznamy o zpracování osobních údajů a na žádost je zpřístupnit dozorovému orgánu. Jedná se o obecné záznamy nikoliv o každodenní činnosti prováděné s osobními údaji. Vedení této agendy může správce převést na zpracovatele. Údaje, které musí tato dokumentace obsahovat, jsou:

- Účely zpracování,
- jméno a kontaktní údaje správce,
- rozsah zpracovaných osobních údajů,
- informace o příjemcích daných osobních údajů,
- informace o předávání údajů do třetích zemí,
- informace o lhůtách pro výmaz jednotlivých kategorií údajů,
- popis přijatých technický a organizačních opatření k zajištění bezpečnosti údajů. [1]

3.3 Jmenování pověřence pro ochranu osobních údajů

Hlavní úkolem tohoto subjektu při zpracování osobních údajů je provádění interních auditů, školení pracovníků, celkové řízení agendy interní ochrany dat a monitorování souladu zpracování osobních údajů s povinnostmi, které vyplývají z obecného nařízení. [16]

Povinnost pověřit tento subjekt nastává ve třech případech, jestliže:

- Zpracování provádí orgán veřejné moci či veřejný subjekt (nejsou zahrnuty soudy),
- hlavní činnost správce nebo zpracovatele spočívá v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů.
- hlavní činnost správce nebo zpracovatele spočívá v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů. [16]

3.4 Posouzení vlivu na ochranu osobních údajů

Tato povinnost se provádí v případě, kdy určitý druh zpracování údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, a to zejména při využití nových technologií. [17]

Předmět tohoto posouzení může být širší, což znamená, že například když správce údajů hodlá používat kamerový systém na různých místech, tak se tohle posouzení nebude vztahovat na každé místo zvlášť, ale udělá se komplexně jedno posouzení pro všechna místa. [17]

Jsou zde tři případy, kdy je tohle posouzení nutné vykonat:

- Systematické a rozsáhlé vyhodnocování osobních aspektů, týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
- rozsáhlé zpracování zvláštních kategorií údajů (např. údajů o rasovém či etnickém původu, politických názorech či zdravotním stavu anebo biometrických údajů atd.) nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů,
- rozsáhlé systematické monitorování veřejně přístupných prostorů. [17]

3.5 Předchozí konzultace s dozorovým úřadem

Správce má za povinnost konzultovat zpracování osobních údajů s Úřadem pro ochranu osobních údajů v případě, kdy z posouzení vlivu zpracování na ochranu osobních údajů vyplyne, že by zpracování mělo za následek vysoké riziko a správce by nepřijal dané opatření ke zmírnění tohoto rizika. [18]

„Pokud by správce nedostatečně zmírnil riziko či pokud se dozorový úřad domnívá, že by zamyšlené zpracování, uvedené výše, porušilo toto nařízení, upozorní na to správce a případně zpracovatele údajů písemně ve lhůtě nejvýše osmi týdnů od obdržení žádosti o konzultaci a může uplatnit kteroukoli ze svých pravomocí. Tato lhůta může být s ohledem na složitost zamýšleného zpracování prodloužena o šest týdnů.“ [18]

Při konzultaci s dozorovým úřadem má správce za povinnost poskytnout mu informace o těchto aspektech:

- Rozdělení odpovědností správce, společných správců a zpracovatelů zapojených do zpracování, zejména v případě zpracování v rámci skupiny podniků.
- Účely a způsoby zamýšleného zpracování.
- Opatření a záruky poskytnuté za účelem ochrany práv a svobod subjektů údajů podle tohoto nařízení.
- Kontaktní údaje případného pověřence pro ochranu osobních údajů.
- Posouzení vlivu na ochranu osobních údajů podle článku 35 a.
- Veškeré další informace, o které dozorový úřad požádá. [18]

3.6 Legislativa spojená se zpracováním osobních údajů ve škole či školském zařízení

Školská zařízení ve většině případů zpracovávají osobní údaje především učitelů, rodičů, žáků, zákonných zástupců či dokonce třetích osob, jako jsou například babičky, tety apod. Všichni, o kterých se zaznamenávají osobní údaje, mají právo na to, aby tyto osobní údaje byly po určité době vymazány. [19]

Tato legislativa je především směřována všem osobám v oblasti školství a které v rámci své činnosti přicházejí do styku s osobními údaji. Jedná se tedy o:

- Ředitele škol a školského zařízení
- Učitele
- Rektory vysokých škol
- Účetní škol a hospodáře
- Pracovníky IT a správce sítě
- Studijní oddělení [19]

Mimo nového zákona o zpracování osobních údajů, upravuje ve školských organizacích sběr, zpracování a uchovávání osobních údajů také následující legislativa:

- Zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon)

  • dokumentace škol a rozsah osobních údajů vedený ve školní matrice (§ 28 odst. 1 až 4)

• sdružování údajů z dokumentace škol a školních matrik Ministerstvem školství (§ 28 odst. 5)

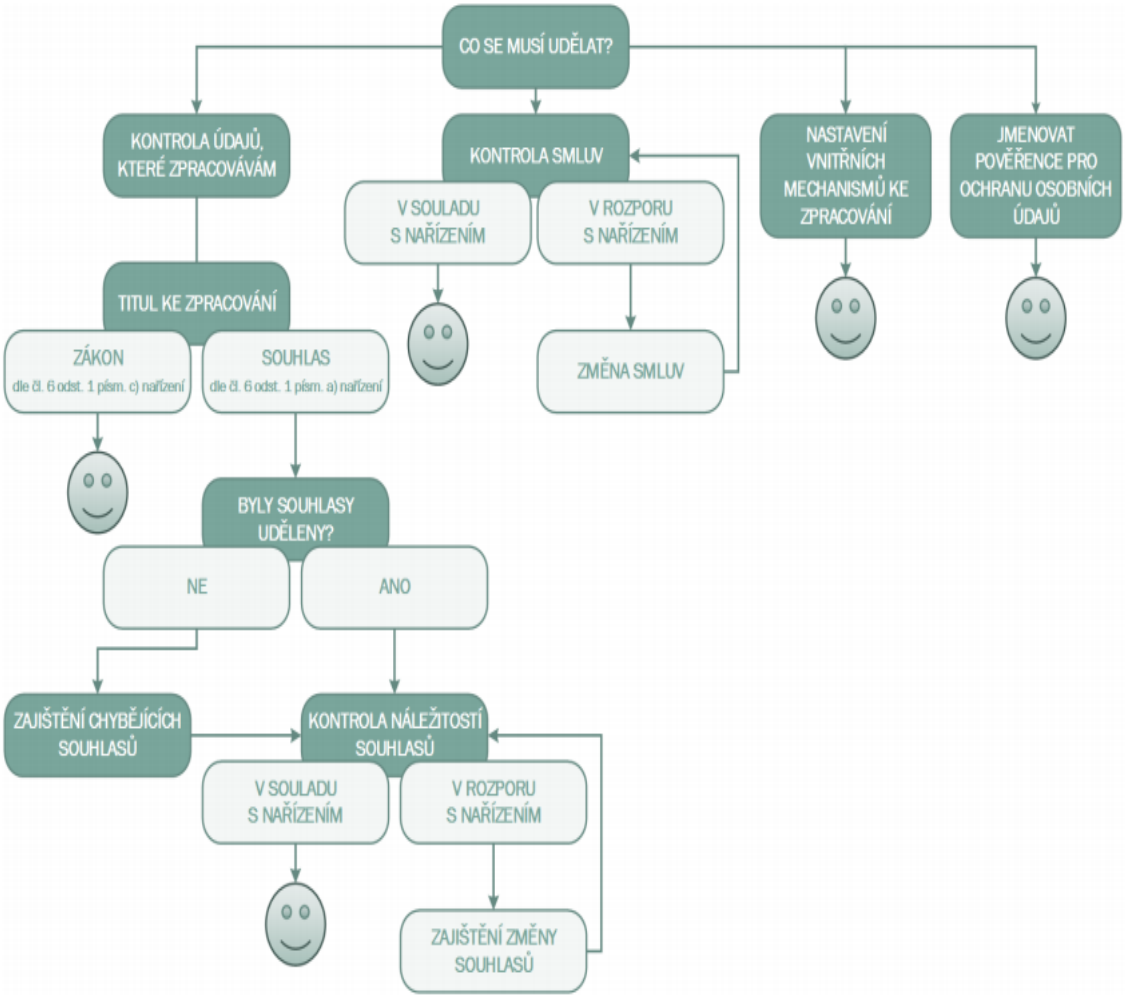
- Zákon č. 109/2002 Sb., o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních a o změně dalších zákonů

  • audiovizuální systémy, možnosti jejich využití (§ 15) [20]

Z výše uvedených legislativ tedy vyplývá, že je zde několik právních aspektů, které se musí dodržet. Mezi nejdůležitější kontroly, které musí být prováděny při zpracování osobních údajů ve školství jsou:

- Zda je při zpracování činěno na základě zákona nebo se souhlasem (osobní informace, jejichž zpracování vyplývá ze zákona lze zpracovávat, v jiném případě je ke zpracování nutný souhlas),
- údaje nesmí být zpracovány nad rámec zákona,
- zda jsou zpracovávané osobní údaje skutečně potřebné pro její činnost,
- zpracovávané údaje jsou zpracovávány řádně a v souladu s právními předpisy (například je třeba kontrolovat smlouvy, které má škola či školské zařízení s poskytovateli informačních systémů nebo jiných IT služeb, které zpracovávají a zaznamenávají osobní údaje; především se jedná u kontroly způsobu zpracování, přístupu do systému nebo například zabezpečení těchto systémů),
- jmenování pověřence pro ochranu osobních údajů (jedná se o osobu, jejíž hlavním úkolem je monitorování souladu zpracování osobních údajů s právy a povinnostmi, které vyplývají z nařízení). [19]

Před nabytím platnosti nového obecného nařízení GDPR vydalo Ministerstvo školství, mládeže a tělovýchovy pomůcku ke zpracování osobních údajů, která do jisté míry uvádí zavedené novinky:



Obrázek 1 - Hlavní úkony, které se musely provést před nabytím platnosti obecného nařízení [19]

3.7 Školní matrika

Ve školském zákoně je školní matrika formulována jako evidence dětí, žáků a studentů škol a školských zařízení. V §28 školského zákona je výslovně vymezen okruh údajů, jenž jsou vedeny ve školní matrice a subjekty, které jsou odpovědné za vedení této školní matriky. Dále zahrnuje veškeré subjekty, které mohou být zapojené do zpracování údajů ze školních matrik a některé další záležitosti, spojené s vedením školní matriky. Dalším aspektem, který upravuje především předávání vedených údajů, je vyhláška č. 364/2005 Sb., o vedení dokumentace škol a školských zařízení a školní matriky a o předávání údajů z dokumentace škol a školských zařízení a ze školní matriky. [21]

Data ze školních matrik musí předávat veškeré školy poskytující stupeň vzdělání, vyjmou jsou školy, které nemají své kmenové žáky, to jsou především školy při zdravotnických zařízeních. Tato povinnosti předávání se tedy týká vyšších odborných škol, středních škol, konzervatoří a základních škol. [21]

Předávání údajů ze školních matrik probíhá ve dvou termínech: [21]

- V tzv. „hlavním podzimním sběru“, ve kterém se předávají soubory s údaji o všech osobách, které byly alespoň jeden den žáky školského zařízení, pokud měly přerušené vzdělávání nebo vykonávaly závěrečnou nebo maturitní zkoušku. Hlavní pozdní sběr se koná od 1. října minulého roku do 30. září probíhajícího roku.
- Dalším termínem je tzv. „jarní aktualizační sběr“, který se váže k datu od 1. září do 31. března probíhajícího školního roku. V tomto období se předávají soubory s větami, které nabyly platnosti alespoň jeden den.

Tyto předávané soubory musí obsahovat údaje o všech kmenových žácích nebo studentech, forma a druh vzdělávání nehraje v předávání roli. Dále obsahuje údaje o konaných závěrečných nebo maturitních zkouškách a absolutoriích, bez ohledu na výsledek těchto zkoušek. [21]

3.8 Zabezpečení zpracování osobních údajů

Dalším důležitým aspektem, který se týká přímo zabezpečení zpracování osobních dat, je článek 32 EU obecné nařízení o ochraně osobních údajů. V první řadě tento právní aspekt pojednává o povinnostech správce a zpracovatele provést vhodná technická a organizační opatření, za účelem zajištění úrovně zabezpečení, která musí odpovídat danému riziku. Při těchto krocích, která jsou povinná pro správce a zpracovatele, je přihlíženo ke stavu techniky a nákladům na provedení daného zabezpečení. Dále se přihlíží na rozsah, kontext a účel zpracování osobních údajů a k různě pravděpodobným rizikům s různou závažností pro práva a svobody fyzických osob. [22]

Další odstavec tohoto článku pojednává o posuzování vhodné úrovně zabezpečení. Při tomto kroku správce či zpracovatel zohledňuje veškerá rizika hrozeb, která by mohla mít za následky například náhodné nebo protiprávní zničení, ztrátu či pozměňování dat při zpracování, neoprávněné zpřístupnění zaznamenaných nebo jinak zpracovávaných osobních informací. Při tomto úkonu musí správce či zpracovatel dbát také na neoprávněný přístup k osobním údajům, přičemž opatření proti tomuhle jednání by mělo být maximální.

Další důležitou částí tohoto článku, je přijetí opatření pro zajištění toho, aby všechny fyzické osoby, které jsou pověřeny správcem či zpracovatelem a mají přístup k osobním údajům, konaly zpracování určených osobních údajů pouze na pokyn správce, jestliže jim již nejsou oprávněni ze strany Unie nebo členského státu. [22]

II. PRAKTICKÁ ČÁST

4 MODEL ORGANIZACE, U NĚJŽ BUDETE POSUZOVAT SPECIFIKA OCHRANY OSOBNÍCH ÚDAJŮ.

V této části je detailně rozebrána charakteristika organizace, u které se bude implementovat nové obecné nařízení GDPR. Současně budou analyzovány specifika zpracování a ochrana osobních údajů. Zvolena organizace je z oblasti školství, tudíž se zde budou vztahovat všechny právní aspekty GDPR spojené se školou či školským zařízením. Jedná se o smyšlenou střední průmyslovou školu v Bystřici pod Hostýnem, avšak veškeré informace jsou čerpány z několika různých středních škol.

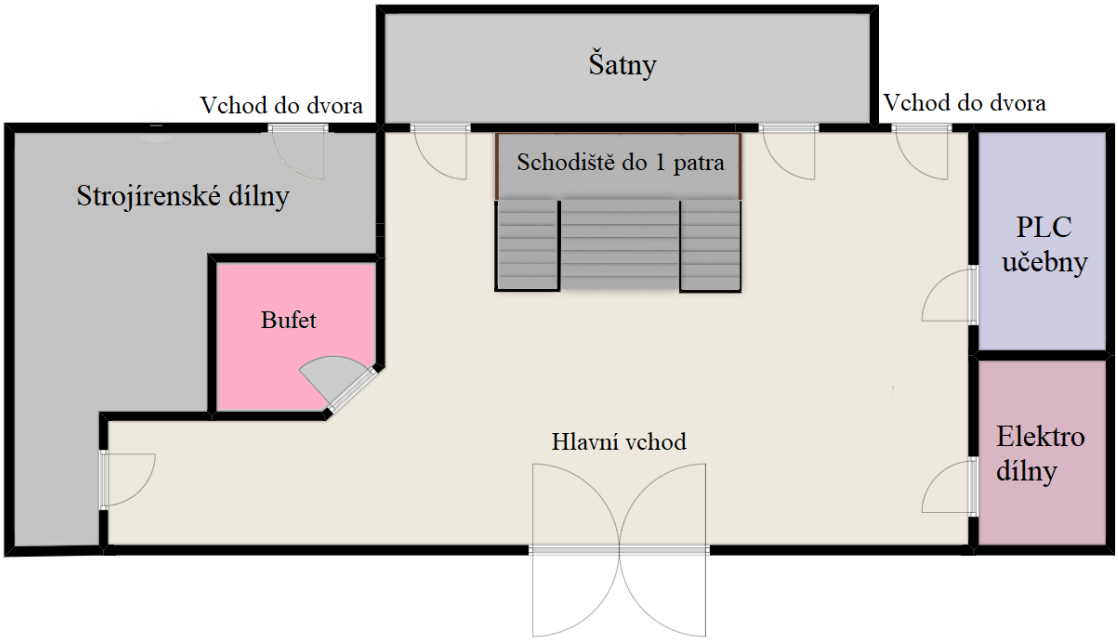
4.1 Charakteristika organizace

Pro bakalářskou práci byla vybrána Střední průmyslová škola v Bystřici pod Hostýnem. Tato škola stojí na rohu ulice Školní a Komenského od roku 1909. V počátcích byla škola směřována jen ve strojnickém oboru, avšak ve školním roce 1919/1920 byla přeměněna na státní průmyslovou školu. [23]

Největší rozmach bystřické průmyslové školy nastává v poválečné době, avšak začátky byly velice obtížné, neboť prioritní bylo překonat následky války. Generální oprava hlavní budovy v letech 1971/1972 přinesla nové laboratoře fyziky, chemie, elektrotechniky a automatizační techniky. Roku 1984 byla uskutečňována obsahová a organizační přestavba středních škol, která přinesla změnu oborů. Především obor strojírenství se rozdělil na strojírenskou technologii a strojírenskou konstrukci. [23]

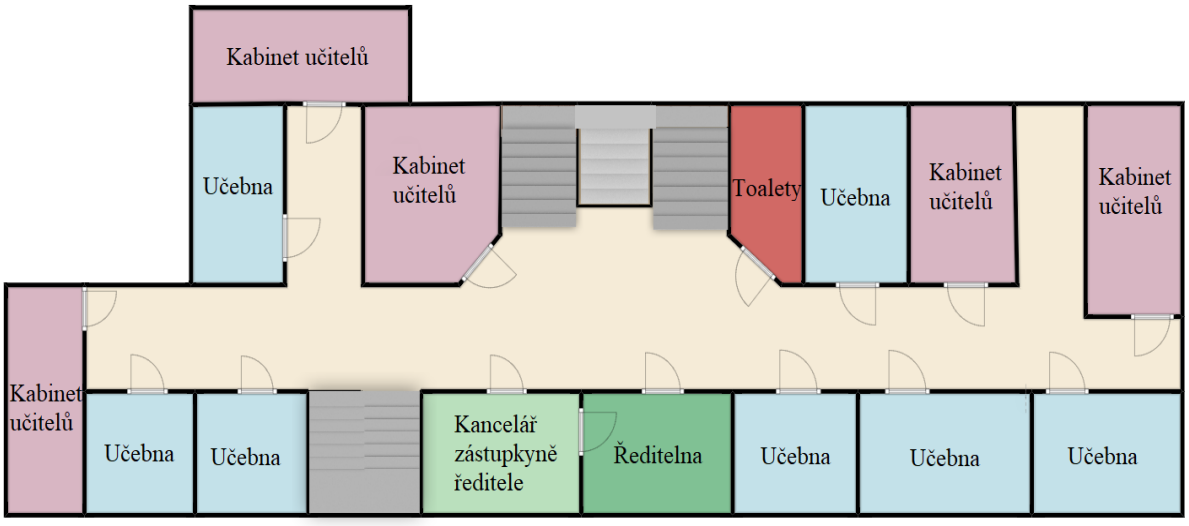
Obrázek 2 - Střední průmyslová škola v Bystřici pod Hostýnem [28]

Škola se skládá z přízemí a dvou pater. V přízemí se nachází šatny, kde se žáci přezouvají a převlékají, bufet, a především učebny a dílny pro praktické činnosti žáků.



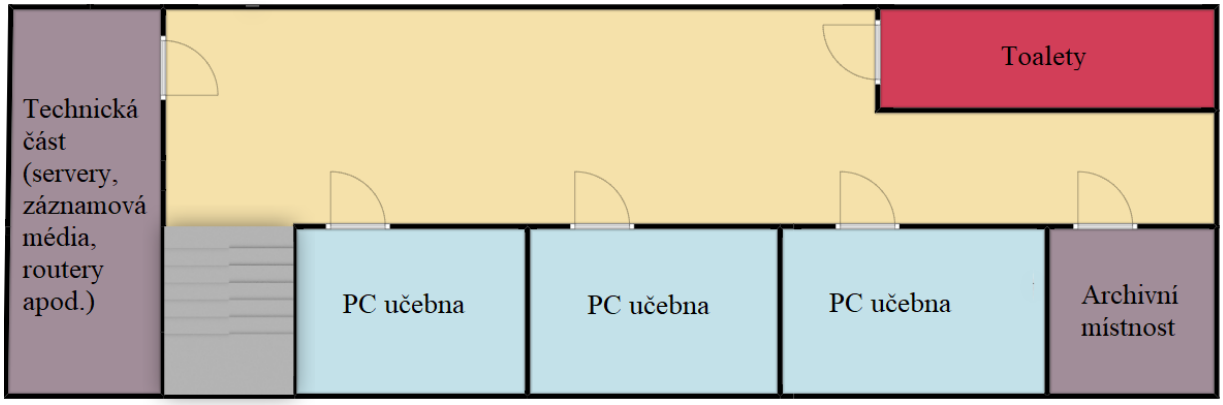
Obrázek 3 - půdorys přízemí na SPŠ v Bystřici pod Hostýnem

V prvním patře se nachází několik vyučovacích učeben, kabinety učitelů a ředitelna, vedle které je kancelář pro zástupkyni ředitele.



Obrázek 4 - půdorys 1. patra na SPŠ v Bystřici pod Hostýnem

Třetí patro slouží zejména pro učebny s počítačovou a elektrotechnickou výbavou. Jsou to především místnosti pro obory elektrotechniky. Nachází se zde také technická část, která obsahuje servery, záznamová média, routery apod. a archivní část, kde se uchovávají veškeré dokumenty a spisy.



Obrázek 5 - půdorys 2. patra na SPŠ v Bystřici pod Hostýnem

Mimo hlavní budovu se zde nachází školní dvůr, který je po celém perimetru oplocen.

4.2 Organizační struktura organizace

Škola poskytuje vzdělávání ve třech maturitních oborech:

- Elektrotechnika: – zaměření na techniku počítačů nebo počítačové řízení
- Strojírenství
- Technické lyceum [24]

Všechny studijní obory jsou čtyřleté a zakončené maturitní zkouškou. Je možné je studovat pouze denní formou. Obor Technické lyceum, byl poprvé otevřen až v roce 2000. Tento obor se zaměřuje především na všeobecné vzdělávací předměty a svojí výukou připravuje studenty na následné vysokoškolské studium. Naopak zbylé dva obory se zaměřují na praktickou část výuky. [24]

Tabulka 1 – Přehled oborů na SPŠ v Bystřici pod Hostýnem [24]

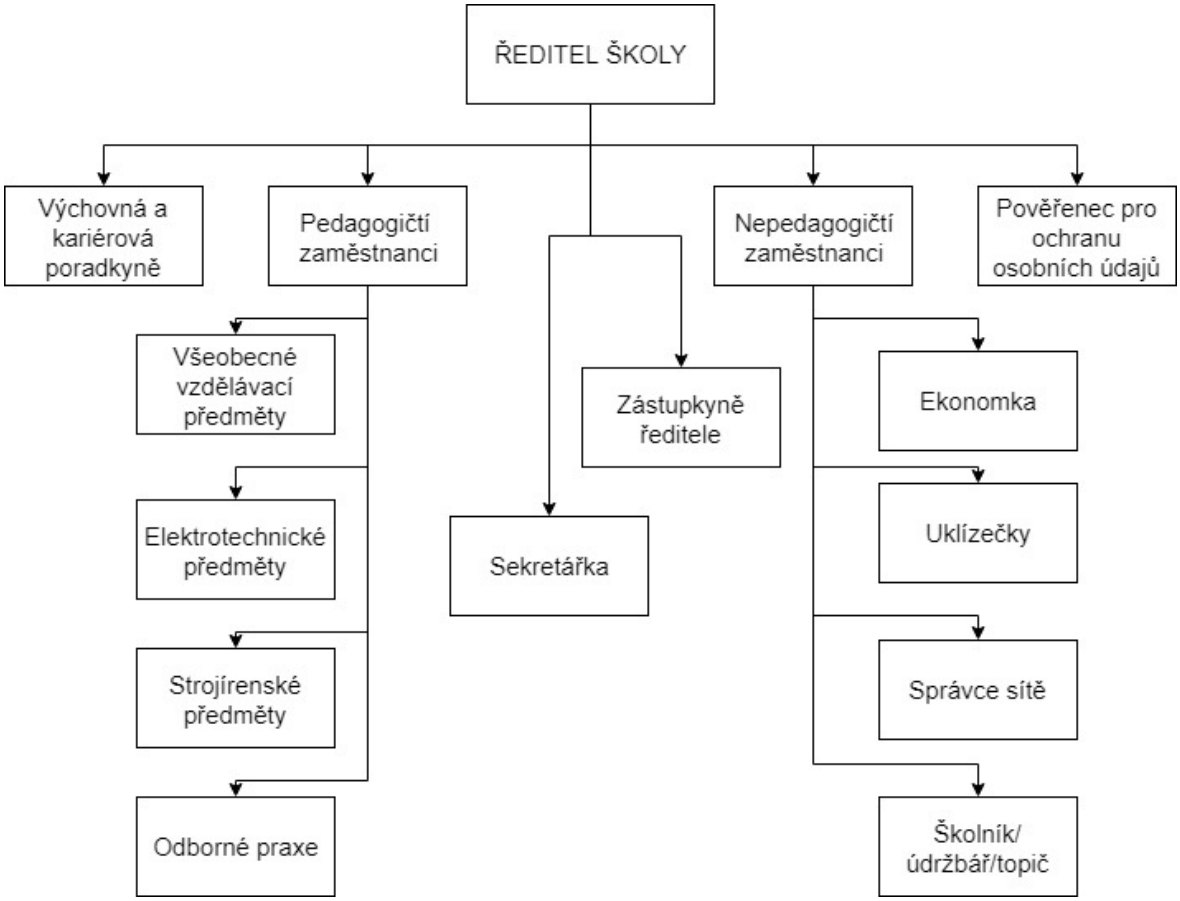
Obor	Přijatí žáci
Elektrotechnika – zaměření na techniku počítačů	24
Elektrotechnika – počítačové řízení	19
Technické lyceum	19
Strojírenství	29

Jen pro představu zde byla zmíněna statistika z minulého roku, která nám udává počet přijatých žáků konkrétních oborů na škole. Celkem tedy za rok 2017/2018 bylo přijato 91 žáků. [24]

Tabulka 2 – Přehled počtu učitelů na SPŠ v Bystřici pod Hostýnem [24]

Všeobecné vzdělávací předměty	18
Strojírenské předměty	5
Elektrotechnické předměty	5
Odborná praxe	3
Celkem	31

Tabulka 2 nám udává počet pracovníků školy s jejich konkrétním zaměřením. Největší zastoupení mají všeobecné vzdělávací předměty, což jsou například český jazyk, cizí jazyk, matematika, fyzika apod. Dále se zde nachází osm nepedagogických pracovníků, kteří se starají o správný chod školy. Na obrázku 5 je zobrazena organizační struktura školy.[24]



Obrázek 6 - Organizační struktura na SPŠ v Bystřici pod Hostýnem

4.3 Pověřenec pro ochranu osobních údajů

Funkci pověřence pro ochranu osobních údajů pro SPŠ Bystřice pod Hostýnem vykonává společnost Schoola Servis GDPR, s.r.o. Osoba určena pro jednání za pověřence je pan JUDr. Ing. Et Ing. Radim Ondrásek, Ph.D., MBA.

4.4 Analýza rizik spojená se zpracováním osobních údajů na škole

V předchozích kapitolách byly popsány právní povinnosti správce či zpracovatele při návrhu zabezpečení osobních údajů v průběhu jejich zpracování. Při těchto úkonech se musí stanovit rizika a závažnosti určitých hrozeb, dle kterých se nadále navrhují vhodné úrovně bezpečnosti. V této části bude provedena analýza rizik v souvislosti se zpracováním osobních údajů. V první řadě je třeba si stanovit co vlastně chceme chránit před hrozbami.

Prioritní je pro nás zabezpečit zaznamenávané osobní údaje před odcizením, zneužitím, zničením, neoprávněným přístupem nebo například před pozměňováním osobních informací. Veškeré tyto hrozby mají negativní dopad na subjekty údajů.

Ve škole či školském zařízení jsou to především tyto subjekty zpracování osobních údajů:

- Žáci
- Uchazeči o vzdělávání
- Zaměstnanci školy
- Uchazeči o zaměstnání
- Zákonní zástupci nezletilých žáků

Při zpracování žádný subjekt nespadá do zvláštní kategorie osobních údajů spojený s čl. 9 nařízení Evropského parlamentu a Radu (EU) 2016/679, jenž například zakazuje zpracování osobních údajů, které by mohlo vypovídat o rasovém nebo etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení. Výjimkou ovšem mohou představovat osobní údaje zaměstnanců, jenž jsou vyžadované právními předpisy ve smyslu plnění zákonných povinností zaměstnavatele. Jsou to například údaje o zdravotní způsobilosti zaměstnanců. [25]

Následující dvě tabulky byly vykonstruovány pro lepší pochopení konečné analýzy. Představují míry rizik a závažnost hrozeb spojené se zpracováním osobních údajů.

Tabulka 3 – Určení míry pravděpodobností

ÚROVEŇ	OZNAČENÍ	ČÍSELNÉ VYJÁDŘENÍ	POPIS VÝSKYTU
4	Velmi pravděpodobná	Od 3,1 do 4	Vyskytne se s velkou pravděpodobností. Průměrně jednou za rok.
3	Pravděpodobná	Od 2,1 do 3	Vyskytne se ojediněle. Průměrně jednou za pět let.
2	Méně pravděpodobná	Od 1,1 do 2	Vyskytne se výjimečně. Průměrně jednou za deset let.
1	Nepravděpodobná	Od 0,1 do 1	Nevyskytne se skoro vůbec.

Tabulka 4 – Určení závažnosti hrozeb

ÚROVEŇ	DOPAD	ČÍSELNÉ VYJÁDŘENÍ	POPIS VÝSKYTU
4	Katastrofický	Od 3,1 do 4	Zničení systému zpracování osobních údajů, kdy tento problém je řešitelný během týdne až jednoho měsíce. Zničení, odcizení či pozměnění veškerých záznamů, maximální zneužití osobních údajů. Fatální dopad na následný chod školy či školského zařízení.
3	Kritický	Od 2,1 do 3	Nabourání do systému zpracování osobních údajů, kdy tento útok může představovat výpadek systému až na týden, možnost zneužití osobních informací v menší míře. Možnost zachycení a odvrácení tohoto probíhajícího útoku. Významný problém v následném chodu školy či školského zařízení.
2	Významný	Od 1,1 do 2	Možnost nabourání do systému zpracování osobních údajů v menší míře. Tento útok nepředstavuje výpadek systému, avšak je zde možnost, kdy pachatel zjistí osobní informace subjektu údajů. Tenhle útok je ve většině případů odrazen v počátcích útoku. Malý dopad na následný chod školy či školského zařízení.
1	Zanedbatelný	Od 0,1 do 1	Veškeré tyto útoku jsou odrazeny v počátcích či ještě v rámci pokusu o

			útok na systém zpracování osobních údajů či přímo na osobní informace subjektů. Nemají vliv na následný chod školy či školského zařízení.

Tabulka 5 – Hodnocení rizik

Hrozba	Příčina	Pravděpodobnost P	Dopad D	Součin S = P*D
Záměrné jednáni zaměstnance	Ve většině těchto případů je to zjištění osobních údajů o určitém jedinci, nikoliv o více lidí zároveň, za účelem zneužití těchto informací.	3	3	9
Vniknutí do zabezpečené místnosti za účelem zneužití osobních údajů	Zničení, odcizení či pozměnění a případně následné zneužití osobních údajů.	2	4	8
Kybernetický útok	Zničení systému zpracování osobních údajů. Odcizení a následné zneužití osobních informací subjektů.	2	4	8
Požár	Manipulace s otevřeným ohněm či zkratování elektřiny. Skladování administrativy, papír lze snadno zapálit.	3	4	12
Živelní pohromy	Přírodní živly. Například vichřice, povodeň, zemětřesení apod.	1	4	4

Technické chyby	Chyba může být ve špatném nastavení softwaru správcem sítě nebo výpadku systému.	3	3	9
Neúmyslné chyby zaměstnance	Může to být například ztráta třídní knihy, nebo záznamy zaměstnanců z hodin, které obsahují osobní údaje subjektu.	2	3	6

Tabulka 6 – Klasifikace rizika

Stupeň rizika	S	Míra rizika
I.	0 – 4	Zanedbatelné riziko
II.	5 – 9	Nežádoucí riziko
III.	10 – 14	Významné riziko
IV.	15 - 16	Nepřijatelné riziko

Míry pravděpodobností a závažnosti hrozby byly stanoveny tak, že se vztahují čistě k problematice bezpečnosti osobních údajů (především tedy míry pravděpodobnosti). Tyto útoky na zpracování osobních údajů či přímo na osobní informace se nevyskytují v takové míře jako například krádež či vandalismus. Ovšem doba se vyvíjí a můžeme předpokládat, že útoky budou narůstat, především tedy na informační systémy či různá záznamová média, která obsahují osobní údaje subjektů.

Tabulka 6 nám udává součin míry pravděpodobnosti a její závažnosti. Tato tabulka byla zkonstruována pro vyhodnocení rizik a její klasifikaci. První stupeň nám představuje hrozby, které nejsou příliš pravděpodobné, ovšem když nastanou mají velký dopad na školu či školské zařízení. Jsou to například živelní pohromy, jejichž průběh nelze ovlivnit.

Dalším stupněm je tzv. nežádoucí riziko. Mezi tuto klasifikaci se řadí většina hrozeb z provedené analýzy. Tyto skutečnosti s negativními následky jsou prakticky uskutečnitelné za jakýkoliv podmínek a ve většině případů představují riziko, které by

mohlo ovlivnit chod školy či školského zařízení. Výjimkou může být násilné vniknutí pachatelem do zabezpečení místnosti, jejichž průběh se dá předpokládat a je možnost zvýšení bezpečnostních prvků.

Záměrně může zaměstnanec jednat za účelem zjištění osobních informací konkrétních subjektů. S touto hrozbou se v dnešní době setkáváme častěji. Informace, které lze tímto způsobem získat, mohou pro určité subjekty představovat velkou hodnotu. Ovšem tohle záměrné protiprávní jednání zaměstnancem by mělo být do určité míry kontrolováno, například zaznamenávání veškerých přístupů do systému či do místností s archivovanými dokumenty obsahující osobní údaje subjektů, a následně řešeno okamžitým propuštěním příslušného zaměstnance. Tohle protiprávní jednání je následně řešeno příslušnými státními orgány.

Požár se jako jediný umístil na úrovni „Významné riziko“. Je to z důvodu velkého dopadu a pravděpodobnosti této hrozby. Zde se jedná především o archivní místnosti s papírovými dokumenty či místnosti vybavené servery, harddisky, routery apod., kde může dojít ke zkratování elektřiny a následnému zničení záznamových médií.

Všichni zaměstnanci přichází do styku s osobními údaji subjektů a jsou vázáni mlčenlivostí o těchto osobních informací. Dále musí dodržovat zásady práce s těmito údaji, které jsou v souladu s nařízením GDPR. Před nástupem do zaměstnání musí být zaměstnanec seznámen s pravidly zacházení s osobními údaji subjektů. Výše zmiňovaný souhlas se zachováním mlčenlivosti je součástí pracovní smlouvy každého zaměstnance. V případech, kdy například dojde ke ztrátě média, obsahující osobní údaje, musí zaměstnanec příslušné rozvrhové akce doložit důkazy, že jeho počínání nebylo v rozporu s pravidly a zásadami, k jejímž se zavázal podpisem pracovní smlouvy.

5 PROZKOUMÁNÍ ADMINISTRATIVY NA SPŠ BYSTŘICE POD HOSTÝNEM

V této fázi analýzy stavu ochrany osobních údajů se zaměřujeme na osobní údaje žáků, jejich zákonných zástupců a například zaměstnanců, které organizace shromažďuje, zpracovává a uchovává na základě povinností vyplývajících z legislativy. Především se jedná o:

- osobní údaje žáků,
- osobní údaje zákonných zástupců žáků,
- osobní údaje zaměstnanců školy,
- osobní údaje smluvních partnerů.

5.1 Správní řízení

Prvním dokumentem, který obsahuje osobní údaje, je přihláška ke studiu, jíž podává uchazeč řediteli školy. Na základě této přihlášky se uchazeč zúčastní přijímacího řízení. Po vyhodnocení přijímacího řízení ředitel školy vydá rozhodnutí o přijetí či nepřijetí uchazeče ke studiu. Aby se mohlo tohle správní řízení konat, je potřeba zaznamenat osobní údaje uchazečů a jejich zákonných zástupců. [26]

Jsou to především následující osobní informace:

- V případě zpracování osobních údajů uchazeče: jméno a příjmení, rodné číslo, míst o trvalého pobytu nebo kontaktní adresa, státní občanství
- V případě zpracování osobních údajů zákonných zástupců: jméno a příjmení, adresa trvalého pobytu nebo kontaktní adresa, telefonní číslo nebo e-mail. [26]

Výše zmíněné osobní údaje jsou zpracovávány za účelem plnění právní povinnosti, konkrétně vedení správního řízení. Zpracování těchto osobních údajů probíhá podle článku 6 odst. 1 písm. c) GDPR plnění právní povinnosti, a to podle ustanovení § 60a, § 60d, § 60e, § 183 zákona č. 561/2004 Sb., školský zákon a dále §1 odst. 2 vyhlášky č. 353/2016 Sb., zákon č. 373/2011 Sb., vyhlášky č. 98/2012 Sb., § 16 a současně školského zákona a vyhlášky č. 27/2016 Sb., § 37 odst. 2 zákona č. 500/2004 Sb., správní řád. Právním titulem pro výše zmíněné zpracování osobních údajů je také podle článku 6 odst. 1 písm. e) GDPR výkon veřejné moci, jenž je správce pověřen. [26]

Podle spisového a skartačního plánu školy jsou osobní údaje shromažďovány a archivovány po určitou dobu. V případě rozhodnutí o přijetí a žádosti o přijetí je doba stanovena na 10 let. [26]

5.2 Evidence žáků

Všechny střední školy mají povinnost vést určitou dokumentaci o své činnosti, jenž jim udává Školský zákon. Patří zde i tzv. evidence žáků neboli školní matrika, jejíž patřičné povinnosti jsou také stanoveny v § 28 odst. 2 školského zákona. [26]

Školní matrika proto musí obsahovat následující osobní údaje:

- V případě zpracování osobních údajů žáků: jméno a příjmení, rodné číslo, datum narození, státní občanství, místo trvalého pobytu a místo narození, do určité míry údaje o zdravotní způsobilosti žáka, které jsou vedeny jako zvláštní kategorie osobních údajů, tzv citlivé údaje, pokud nepobývá žák na území ČR, je nutnost uvést místo pobytu v zahraničí, veškeré údaje o předchozím vzdělání žáka či studenta společně s dosaženým stupněm vzdělání; Dále školní matrika zaznamenává obor, formu a délku vzdělávání, datum zahájení vzdělávání na škole, údaje, které se vedou v průběhu vzdělávání jako například výsledky, vyučovací jazyk, údaje o neobyčejném nadání, údaje o poskytovaných podpůrných opatření, údaje o zdravotních potížích, které by mohly vést k negativním následkům na průběh vzdělávání, datum ukončení vzdělávání na škole a údaje o závěrečných zkouškách.
- Pokud se jedná o zpracování osobních údajů zákonných zástupců, jedná se o údaje typu: jméno a příjmení, telefonické spojení, místo trvalého pobytu, pokud nemá bydliště na území ČR, je nutno zaznamenat adresu pro doručování písemností.
- Zákonní zástupci mají možnost dobrovolně dát svůj e-mail, za účelem rychlé a efektivní komunikace. Takový osobní údaj je následně zpracován na základě oprávněného zájmu správce osobních údajů, což je uvedeno v článku 6 odst. 1 písm. f) GDPR. [26]

Veškeré osobní údaje vedené ve školní matrice, jsou zpracovávány na základě plnění právní povinnosti, jenž vyplývá ze školského zákona. Zmíněné zpracovávání je v souladu s článkem 6 odst. 1 písm. c) GDPR. Dobu, po kterou jsou údaje uchovávány upravuje zákon o archivnictví a spisové službě. V případě školní matriky se jedná o dobu 10 let. [25]

5.3 Přihlášky ke stravování

Při poskytování stravovacích služeb pro žáky či zaměstnance, se musí zpracovávat informace, které se objevují v přihláškách ke stravování. Jedná se o osobní údaje žáků a zákonných zástupců. [26]

Jsou zpracovány následující osobní údaje:

- V případě zpracování osobních údajů žáků: jméno a příjmení, rodné číslo nebo datum narození, probíhající školní rok, místo trvalého pobytu nebo kontaktní adresa, třída, bankovní účet, datum zahájení a ukončení využívání těchto stravovacích služeb, údaje o zdravotních potížích, které by mohly mít negativní vliv na stravovací služby (například alergie), v tomto případě se opět jedná o zvláštní kategorii osobních údajů, tzv citlivé údaje.
- V případě zákonných zástupců: jméno a příjmení, adresa trvalého pobytu nebo kontaktní adresa, bankovní účet, telefonní číslo nebo email. [26]

Na základě této přihlášky ke stravování se uzavírá určitý právní vztah, kdy na jedné straně má provozovatel povinnost poskytnout určitou službu a na druhé straně má příjemce povinnost tyto stravovací služby uhradit. Veškeré osobní údaje jsou zpracovávány za účelem poskytování stravovacích služeb, jenž se odkazuje na uzavřený smluvní vztah podle článku 6 odst. 1 písm. b) GDPR. [26]

5.4 Přihlášky do projektu ERASMUS

Jde zde možnost, že se škola stane účastníkem v rámci projektu ERASMUS. Jedná se o výměnný pobyt žáků v zahraničí za účelem rozšíření vzdělání a jazykových dovedností. Při tomto jednání musí být správce uzpůsoben zpracovávat osobní údaje na základě řádně uděleného souhlasu. [26]

Jedná se především o následující informace: [26]

- Jméno a příjmení studenta, rodné číslo a datum narození, číslo občanského průkazu, e-mail, telefonní číslo, adresa trvalého pobytu, jméno a příjmení zákonného zástupce.

S výše uvedenými osobními údaji mohou nakládat pouze pověření pracovníci a za takovým účelem, jenž je nutný pro jejich činnost v rámci projektu Erasmus.

5.5 Účetnictví a hospodářská činnost

Za účelem řádného chodu školy jsou uzavírány různé soukromoprávní smlouvy například k zajištění provozu IT sítě, telefonů nebo třeba k běžné údržbě budovy. Tyto smlouvy obsahují osobní informace smluvních partnerů. [26]

Především se jedná o: [26]

- Jméno a příjmení, identifikační číslo organizace, adresa sídla nebo provozovny, adresa trvalého pobytu nebo kontaktní adresa, daňové identifikační číslo, telefonní číslo a e-mail.

Zpracování těchto osobních údajů se koná za účelem plnění uzavřené smlouvy podle článku 6 odst. 1 písm. b) GDPR a současně pro plnění smluvních povinnosti podle, tj podle článku 6 odst. 1 písm. c) GDPR. Výše zmiňované plnění smluvních povinnosti nastává v moment, kdy musí být evidovány faktury nebo jiné daňové doklady v rámci účetnictví podle zákona č. 563/1191 Sb., o účetnictví. Smlouvy jsou uchovávány po dobu 10 let a faktury po dobu 5 let. [26]

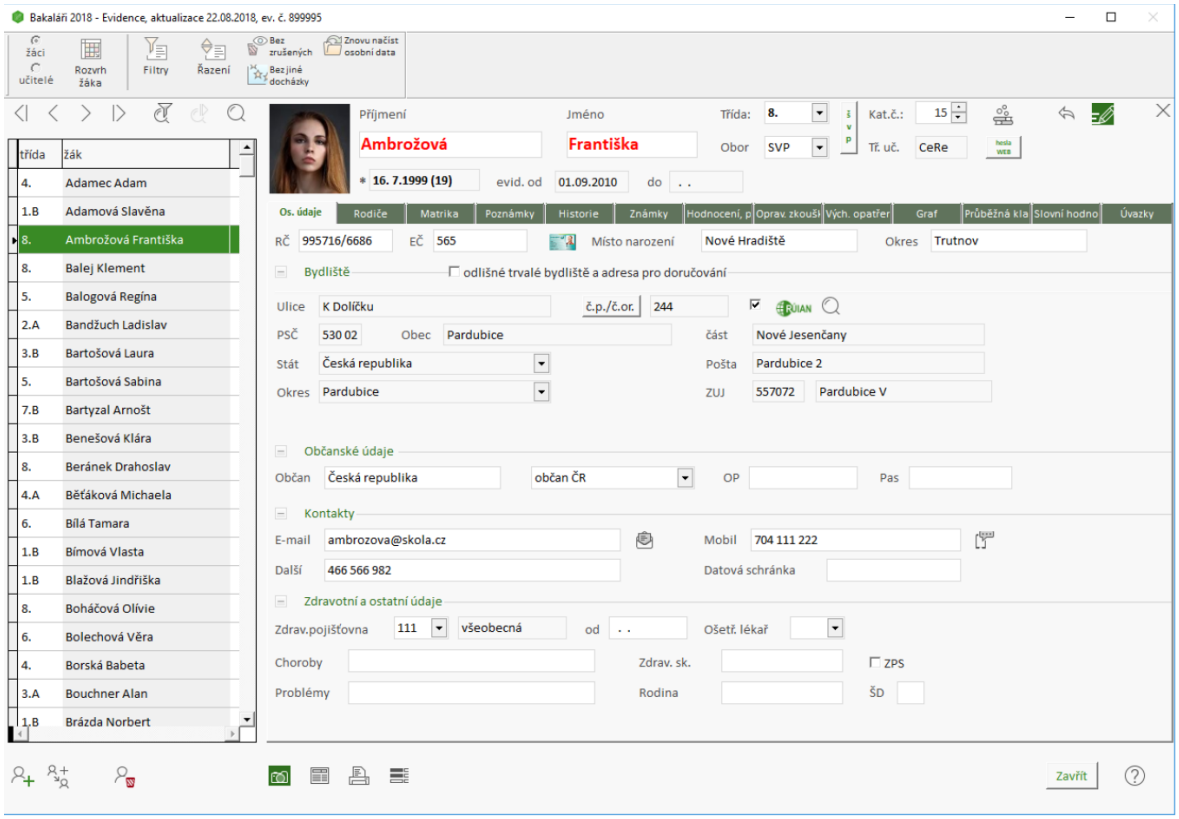
6 UCHOVÁVÁNÍ DOKUMENTŮ S OSOBNÍMI ÚDAJI NA SPŠ BYSTŘICE POD HOSTÝNEM

Ať už se jedná o zpracování osobních údajů v elektronické podobě či fyzicky papírovou formou, je nutné veškeré zpracování těchto údajů zaznamenávat a archivovat po určitou dobu. Tuhle problematiku například řeší zákon č. 499/2004 Sb., o archivnictví a spisové službě.

6.1 Elektronická databáze

Osobní údaje subjektu jsou uchovány především v elektronické podobě. K vedení databáze osobních údajů je využito služeb školního systému Bakaláři. Tento software nabízí veškerou komunikaci mezi školou a rodinnou, což zahrnuje především přehled rozvrhu žáka, klasifikace nebo například absence žáka. Program vede veškerou databázi žáků a učitelů na škole a také nabízí podporu odevzdávání dat z matriky na Ministerstvo školství, mládeže a tělovýchovy ČR. Jedná se tedy o podzimní a jarní sběr matriky a také o měsíční hlášení ve změně poskytovaných podpůrných opatření.

K přihlášení do tohoto portálu jsou potřeba přihlašovací údaje žáků či učitelů. K databázi studentů mají přístup jen oprávnění zaměstnanci školy a především správce IT. Ovšem tento školní systém Bakaláři nabízí přehled všech učitelů na škole. Přístup k této sekci „Učitelé“ je umožněn všem žákům či zaměstnancům, kteří mají přístup do portálu Bakaláři. Konfigurovat databázi může pouze správce IT s příslušnými přihlašovacími údaji. Dalším, kdo má přístup do systému, je pověřená a osvědčená osoba za dodavatele softwaru, která provádí veškerá nastavení systému, podporu servisu nebo například pravidelné aktualizace. Další důležitou sekcí je tzv. „Evidence“. Zde je veden veškerý zápis osobních dat žáků a zaměstnanců. Škola k uchování těchto citlivých údaji využívá ukládání na SQL server, který je instalován na příslušné záznamové médium na škole. K zabezpečení údajů je využito také šifrovacích technik. SPŠ Bystřice pod Hostýnem využívá podpory šifrování „https“ přímo od dodavatele školního systému Bakaláři.



Obrázek 7 - Evidence žáků školního systému Bakaláři [27]

Školní stránky nemají zabezpečení metodou šifrování „https“, neboť tyto stránky slouží pouze k prohlížení například fotogalerie, organizace studia a provozu školy nebo například k přehledu novinek. Pro zdokonalení prezentace školy jsou využity a zveřejněny některé fotografie, videozáznam nebo dokonce i jméno a příjmení žáka. V takových případech je vyžádán souhlas žáka se zpracováním osobních údajů. Ovšem v některých případech tento souhlas není potřeba. Tohle řešení nastává ve chvíli, kdy na fotografii či videozáznamu není osoba konkrétně identifikovatelná.

Na hlavních stránkách školy je možnost přesměrování na výukové materiály. K těmto údajům má přístup kdokoliv. Ovšem k přidávání či odebírání jednotlivých výukových složek mají pouze oprávnění zaměstnanci školy a ke konfiguraci systému má přístup pouze správce IT.

Osobní údaje všech zaměstnanců školy jsou elektronicky vedeny a primárně uloženy v databázi mzdového softwaru POKLADNA. Tento program je instalován pouze na jednom počítači, který je trvale chráněný heslem. Další přihlašovací údaje jsou potřeba k přístupu do aplikace POKLADNA. Tento přístup je uzpůsoben pouze pro hlavní účetní školy, která zde vede veškeré zpracování údajů, které jsou potřebné k vedení účetnictví.

Jsou to především údaje typu jméno a příjmení a číslo bankovního účtu. Přístup do tohoto systému je umožněn servisnímu technikovi, který provádí veškeré konfigurace a aktualizace systému. Tento přístup je ošetřen licenční smlouvou s dodavatelem systému.

Veškerá hardwarová zařízení jako například servery, pevné disky, routery, zdroje, aj., jsou z důvodu bezpečnosti, především proti neoprávněným přístupům nebo k udržení provozních podmínek, umístěny v samostatné části budovy, ve kterých jsou veškeré komponenty navíc uloženy v uzamykatelných rackových skříních. Tato místnost obsahuje detektor kouře a teploty, který v případě detekce vyhlásí poplach v podobě akustického alarmu až 85 dB. Místnost je neustále uzamčená bezpečnostní vložkou třídy 3. Rackové skříně v místnosti jsou uzamykatelné visacím zámkem bezpečnostní třídy 2.

6.2 Fyzická administrativa

S prvním osobním údajem zaznamenaným v papírové formě se v případě školy či školského zařízení setkáme v přihlášce na studium, které musí být vždy podepsány uchazečem či jeho zákonným zástupcem. Tato dokumentace musí být uchovány a archivována na určitou dobu. SPŠ Bystřice pod Hostýnem používá ještě třídní knihy, kde se mimo docházky žáků také zapisují různé poznámky učitelů či prováděné aktivity. Tyto dokumenty obsahují osobní údaje žáků, učitelů a také kontaktní údaje zákonných zástupců, pro případ, kdy by bylo nutné se s nimi spojit během rozvrhových aktivit. Další částí jsou výsledky z přijímacího řízení. Tyto dokumenty se musí také uchovávat po určitou dobu, avšak v tomto případě je zde využita tzv. pseudonymizace, kdy výsledky uchazečů nejsou zveřejňovány pod jejich jménem ale, pod určitým identifikátorem, podle kterého není možné odhalit konkrétní identitu subjektu.

V případě zaměstnanců se jedná o velikou škálu zpracování osobních či citlivých údajů v papírové formě. Každému zaměstnanci je vedena osobní složka, jenž obsahuje veškeré dokumenty, které vyžaduje zaměstnavatel. Jsou to především pracovní smlouvy, doklady o jejich nejvyšším ukončeném vzdělání, doklady o zdravotní způsobilosti nebo souhlas k bezhotovostnímu převodu na bankovní účet. Tyto osobní složky zaměstnanců jsou vedeny zástupkyní ředitele.

Tyto osobní složky zaměstnanců jsou umístěny ve středu budovy poblíž ředitelny. V této místnosti sídli zástupkyně ředitele školy, která se stará o veškerou administrativu. Dokumenty jsou umístěny v uzamykatelných skříních. Skříně lze uzamknout visacím

zámkem bezpečnostní třídy 2. Zbylé dokumenty obsahující osobní údaje žáků jsou uschovány v archivní místnosti zabezpečenou cylindrickou vložkou bezpečnostní třídy 3. Archivní část budovy se nachází v druhém patře budovy na konci chodby. Kancelář pro zástupkyni ředitele je otevřena v době od 6:00 do 17:00 pracovních dnech. Mimo tyto hodiny a dny je místnost permanentně uzamčena. Archivní část je neustále uzamčena. Do této místnosti má přístup každý, avšak musí požádat školníka o klíč, jenž je spolu s ostatními důležitými klíči v uzamykatelné skříni.

Poměrně často se s těmito spisy pracuje nebo se zakládají nové dokumenty s osobními údaji. Ovšem je nutností si uvědomit, že veškeré zabezpečení těchto papírových dokumentů a složek, obsahujících osobní údaje žáků či učitelů, je pouze v kompetenci zaměstnanců, kteří s těmito dokumenty pracují a zakládají zpět do archivu.

7 ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ NA SPŠ BYSTŘICE POD HOSTÝNEM

Zabezpečení takových informací jako jsou osobní údaje žáků, jejich zákonných zástupců či učitelů by mělo být v takové míře, aby zabránilo veškerým možným hrozbám nebo alespoň redukovalo možná rizika. V mnoha případech ovšem zabezpečení těchto osobních údajů je v kompetenci zaměstnanců, kteří s informacemi pracují. V této části budou rozebrány možná rizika, spojená s osobními údaji na SPŠ Bystřice pod Hostýnem. Další část této kapitoly je obsažena možným opatřením konkrétních rizik spojených se zpracováním osobních údajů na škole.

7.1 Rizika spojená se zpracováním osobních údajů na SPŠ Bystřice pod Hostýnem

Jednou z nejdůležitějších ochran budovy je plášť. Každý pachatel v první řadě zkoumá tento typ ochrany, především otvory pláště a možnosti přístupu do budovy. Zkoumá tedy veškeré dveře, okna, střešní světlíky nebo například zadní či únikové vchody. V provozní době školy jsou míry pravděpodobností tohoto rizika zanedbatelné, neboť v této době se na škole pohybuje několik desítek zaměstnanců. Mimo tohle časové ohraničení, což v našem případě je od 17:00 do 6:00 hodin, se možnosti pachatele vniknout do objektu zužují, avšak v případě, kdy se dostane do prostorů školy se pachatel stává velice nebezpečnou hrozbou pro chráněné osobní údaje.

V případě, kdy se pachatel nachází v objektu a má v úmyslu odcizit, zneužit či zničit uchovávané osobní údaje, měl by mít potíže s překonáním zabezpečovacích prvků. Může se zde jednat o komponenty mechanických zabraných systémů či různých prvků poplachového zabezpečovacího systému, především tedy PIR detektory nebo magnetické kontakty. Významné riziko nastává tehdy, kdy pachatel překoná veškeré zabezpečovací prvky, které mu brání k dokončení jeho protiprávním činům. V našem případě pachatele zajímají místnosti, které jsou umístěny ve druhém patře budovy. Je to především technická místnost, kde jsou umístěny veškeré servery, záznamová média, routery apod. a archivní část budovy, ve které je uchována veškerá fyzická administrativa.

Jedno z nejvážnějšího rizika pro nás představuje vypuknutí požáru. Především se tedy jedná o zkratování elektřiny v části budovy s elektronikou a v archivní místnosti riziko představuje papír, který může snadno vzplanout. V tomto případě mohou být zničeny

veškeré technické prvky, kterými je provozována celá počítačová síť nebo zaznamenávající různé databáze v elektronické podobě, či může být zničena veškerá papírová administrativa v objektu. Ať už by se jednalo o úmyslné či neúmyslné vypuknutí požáru, tato skutečnost představuje riziko, které má velký dopad na budoucí chod SPŠ Bystřice pod Hostýnem.

V případě elektronické databáze pro náš objekt může představovat významnou hrozbu právě kybernetický útok. Zranitelnost v tomto případě může představovat nutnost připojení k internetu. V takovém případě může hackerský útok představovat významné riziko s následky jako například odcizení a následné zneužití osobních údajů.

7.2 Dosavadní zabezpečení

Tato část obsahuje konkrétní zabezpečovací aspekty proti výše zmiňovaným rizikům na SPŠ Bystřice pod Hostýnem.

7.2.1 Přístup do objektu

Jsou zde čtyři možnosti, které nám umožňují dostat se do objektu. Prvním z nich je hlavní vchod. Tato varianta je zabezpečena hlavními vraty, která je otevřena pouze v provozních hodinách, a dalšími dveřmi, jenž jsou vybaveny čipovým přístupovým systémem. Všichni zaměstnanci a žáci vlastní svůj jedinečný čip, který umožní přístup do budovy přes tento vchod. Je zde také možnost využití zvonku, který se nachází vedle uzavřeného hlavního vchodu. Při použití zvonku s návštěvníkem začne komunikovat zástupkyně ředitele, která mu v případě pádného důvodu může otevřít. Hlavní vchod je také možné otevřít pomocí kódu, který se zadává na klávesnici. Tento čtyřmístný kód zná pouze část zaměstnanců školy především správce IT a školník. Další variantou vstupu do objektu jsou dva možné přístupy ze dvora. První je umístěn přímo na chodbě nedaleko hlavního vchodu a druhý ve strojírenských dílnách. Z vnitřní části objektu lze tyto dveře využít k průchodu do dvora či k bezpečnému úniku osob při požáru. Ze dvora nelze tyto otvory pláště využít k přístupu do budovy, neboť dveře obsahují kouli z venkovní části objektu. Mimo provozní dobu jsou tyto přístupové body uzamčeny. V případě, kdy je potřeba přístup ze dvora za účelem konání různých rozvrhových akcí, je možnost vyžádat si klíč u školníka. Poslední možností pro pachatele je možnost vniknutí do objektu okny, která jsou ovšem zvenčí umístěny ve výšce zhruba tří metrů. Z toho vyplývá, že tato varianta je z části vyloučena z možností vniknutí do objektu. Část chodby u hlavního vchodu je zaznamenávána kamerovým systémem, který ovšem slouží pouze k zaznamenávání v případě detekce pohybu.

Záznamy se průběžně automaticky mažou a nahrazují novými, přičemž je zaznamenán nejméně tři dny. Tyto fixní kamery zabírají prostor mezi hlavním vchodem a schodištěm. Z toho vyplývá, že v případě vniknutí pachatele do objektu, ať už to hlavním vchodem či zadními dveřmi do dvora, tak bude zaznamenán na kamerovém záznamu. V přízemí se nachází ještě jedna kamera, která je umístěna v chodbě mezi hlavními vraty a dveřmi s čipovým přístupovým systémem. Tato fixní kamera slouží především k zaznamenávání přístupu všech osob přes jediný možný vchod do objektu.

7.2.2 Zranitelné místnosti a jejich zabezpečení

V předchozích kapitolách byly popsány místnosti, kde jsou uložena záznamová média či archivovány papírové dokumenty, jenž souvisí se zpracováním osobních údajů. Jsou to tedy dvě místnosti ve druhém patře. Případný pachatel musí tedy projít přes první patro, které je monitorováno kamerovým systémem. Tato fixní kamera zaznamenává pouze část chodby před ředitelnou tak, aby zabírala prostor přístupu ze schodiště. Záznamy se automaticky ukládají a promazávají na záznamová média v technické místnosti ve druhém patře. Případný pachatel může být také detekován na kamerovém záznamu ze druhého patra, kde fixní kamera zaznamenává část chodby určenou pro přístup ze schodiště z prvního patra. Kamera také zabírá přímo dveře do technické místnosti. Obě zranitelné části druhého patra z hlediska zpracování osobních údajů jsou zabezpečeny pouze cylindrickou vložkou bezpečnostní třídy 3. Dále jsou vybaveny detektorem kouře a teploty s vestavěnou sirénou 85 dB, které jsou připojeny na ústřednu elektronické požární signalizace (dále jen EPS). Na chodbách jsou umístěny práškové hasící přístroje.

Další část objektu, jenž souvisí se zpracováním osobních údajů je kancelář zástupkyně ředitele s průchodem do ředitelny. Zde se uchovávají osobní složky zaměstnanců v uzamykatelných skříních. Obě místnosti jak kancelář pro zástupkyni, tak přímo ředitelna jsou mimo provozní dobu trvale uzamčeny cylindrickou vložkou bezpečnostní třídy 3, avšak průchod mezi místnostmi je trvale průchozí. V provozních hodinách školy je v těchto místností vždy přítomen alespoň jeden zaměstnanec.

7.2.3 Komunikační a elektronická bezpečnost

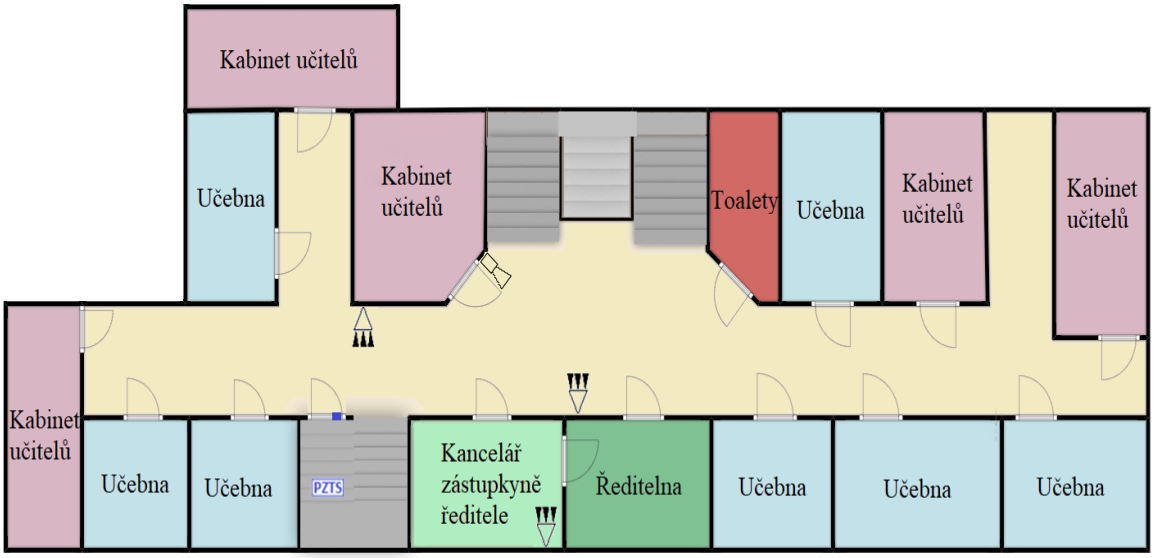
Škola využívá zabezpečení „https“ na stránkách, kde se musí zadat osobní údaje žáků či zaměstnanců. Protokol https zajišťuje bezpečnou komunikaci webového prohlížeče s webovým serverem za pomocí SSL protokolu, který zaručuje autentizaci, důvěrnost a integritu přenášených dat. Do aplikací, souvisejících se zpracováním osobních údajů, mají přístup pouze zaměstnanci, jenž pracují s osobními údaji za účelem vyplývající z jejich pracovní činnosti. Dále má do těchto aplikací přístup správce IT a odpovědné osoby pověřené dodavatelem softwaru. Veškeré počítače jsou vybaveny licencovanými a pravidelně aktualizovanými antivirovými programy. Tyto softwary dokáží zachytit veškeré typy malwarů. Ovšem hackeři se vyvíjí rapidní rychlostí, a proto je škola pojištěna proti případným kybernetickým útokům.

7.3 Identifikovatelné problémy

Hlavní problém v případě zabezpečení osobních údajů na SPŠ v Bystřici pod Hostýnem je absolutní absence poplachového zabezpečovacího a tísňového systému (dále jen PZTS). Tento typ zabezpečení je důležitý zejména k detekci případného pachatele a následnému předání této informace na dohledové a poplachové přijímací centrum (dále jen DPPC).

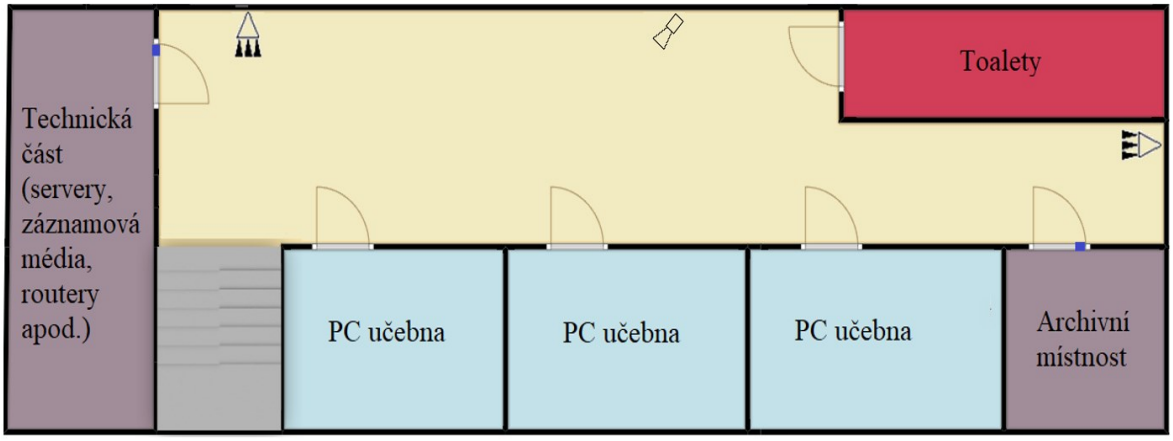
7.4 Zhodnocení zabezpečení a případný návrh zlepšení

Přístupový systém do objektu je řešen pomocí čipového systému u hlavního vchodu, který jako jediný slouží k přímému vstupu do budovy. Prostor u hlavního vchodu je monitorován kamerovým systémem, který ovšem slouží pouze k vedení záznamu několika dní. V případě přístupu do objektu bych zde přidal magnetické kontakty na hlavní dveře a detektory tříštění skla poblíž skleněného hlavního vchodu a oken. Tyto komponenty by komunikovaly přes ústřednu PZTS, která by umožňovala další komunikaci na DPPC. DPPC by případné detekce vyhodnotilo a vyslalo na místo zásahové vozidlo určité bezpečnostní agentury či předalo informaci státním orgánům.



Obrázek 8 - návrh zabezpečení osobních údajů a ústředny PZTS 1. patra

Ústředna PZTS je umístěna v prvním patře v odkládací místnosti pod schody. Tato místnost je pro případné návštěvníky nezajímavá a nachází se ve středu budovy. Dále bych zvážil umístění pasivních infračervených detektorů (dále jen PIR detektor) na chodbu před kancelář zástupkyně ředitele a přímo do kanceláře, která obsahuje složky zaměstnanců. Další PIR detektor je umístěn také na chodbě, určený pro zabezpečení samotné ústředny. Na dveřích ke vstupu do místnosti s ústřednou je umístěn magnetický kontakt pro maximální zabezpečení samotné ústředny. Kamera určená k zaznamenávání dění na chodbě před ředitelnou, je součástí dosavadního zabezpečení školy.



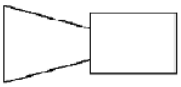
Obrázek 9 - návrh zabezpečení osobních údajů ve 2. patře

Ve druhém patře se nachází nejdůležitější dvě místnosti, související se zpracováním osobních údajů. Tyto dvě místnosti by se v první řadě měly zabezpečit magnetickými kontakty a PIR detektory k detekování případného pachatele. Kamerový systém je součástí dosavadního zabezpečení budovy.

Veškeré zmíněné komponenty detekují pachatele pouze mimo provozní dobu objektu, neboť během této doby se nachází v budově několik desítek či stovek žáků nebo zaměstnanců. Komponenty bych doporučil spojit s ústřednou PZTS bezdrátově z důvodu staré budovy, do jejíž konstrukce by se nemělo zasahovat. Ústředna umožňuje komunikaci s DPPC.

Požární ochrana je v objektu řešena pomocí ústředny EPS, ke které jsou připojeny samočinné i tlačítkové hlásiče požáru. V případě detekce požáru či zmáčknutí hlásiče požáru ústředna detekci zaznamená a pošle informaci pomocí zařízení dálkového přenosu (dále jen ZDP) na příslušné DPPC. Tento subjekt tuhle informaci vyhodnotí a vyšle na místo hasičský záchranný sbor.

Tabulka 7 – použité schématické značky

PZTS	Ústředna
	Kamera pevná vnitřní
	PIR detektor
	Magnetický kontakt

ZÁVĚR

Ve své bakalářské práci jsem se zabýval ochranou zpracování osobních údajů v organizaci. Jako cílový objekt byla zvolena Střední průmyslová škola v Bystřici pod Hostýnem. Z toho vyplývá že se zde řeší veškeré zpracování osobních údajů ve školství a s ním spojeny dokumenty jako například školní matrika, přihlášky ke stravování nebo dokonce i účetnictví, kde se musí vést jednotlivé složky všech zaměstnanců.

V prvních částech bakalářské práce jsem veškerou pozornost věnoval novému obecnému nařízení GDPR, a především jeho legislativním požadavkům na všechny organizace, které zpracovávají osobní údaje v rámci celé Evropské unie. Dle mého názoru bych nařízení GDPR nepovažoval za „revoluční změnu“ v této problematice zpracování osobních údajů. Můj názor je takový, že ten, kdo se do doby nabytí platnosti nařízení GDPR řídil zákonem č. 101/2000 Sb., o ochraně osobních údajů, tak do určité míry splňoval práva a povinnosti nařízení.

Cílem této práce je prozkoumání veškeré administrativy nebo elektronických databází, která zaznamenávají osobní údaje. Tyto veškeré dokumentace se musí archivovat po určitou dobu, nejčastěji se jedná o dobu desíti let. Z toho důvodu tato bakalářská práce také řeší konkrétní zabezpečení jednotlivých dokumentů v cílovém objektu. Tohle zabezpečení je detailně rozebráno a následně je vykonstruován návrh řešení identifikovaných problémů.

Dle mého názoru dosavadní zabezpečení dokumentů souvisejících se zpracováním osobních údajů na střední průmyslové školy v Bystřici pod Hostýnem je dostačující, avšak pouze na minimální úrovni této klasifikace. V objektu není ústředna PZTS, která by v případě detekce pachatele v objektu předávala informace na DPPC, jenž by informaci vyhodnotilo a vyslalo na místo zásahové vozidlo. Ovšem pachatel může být detekován na kamerovém záznamu, kterým tato škola disponuje.

Práce byla vytvořena za pomocí znalostí subjektů vybraného objektu, především tedy správce IT, ředitele a školníka. Poskytli mi veškeré potřebné informace k vytvoření praktické části této bakalářské práce.

SEZNAM POUŽITÉ LITERATURY

[1] OSOBNÍ ÚDAJ. UOOU [online]. [cit. 2019-05-13]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=1627

[2] SOUKROMÍ. Wikipedia [online]. [cit. 2019-05-13]. Dostupné z: https://cs.wikipedia.org/wiki/Soukrom%C3%AD

[3] ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ. 22HLAV[online]. [cit. 2019-05-13]. Dostupné z: https://www.22hlav.cz/gdpr-zpracovani-osobnich-udaju

[4] SPRÁVCE. Managementmania [online]. [cit. 2019-05-13]. Dostupné z: https://managementmania.com/cs/gdpr-spravce-osobnich-udaju-data-controller

[5] ZPRACOVATEL. MVČR [online]. [cit. 2019-05-13]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zakladni-pojmy-v-gdpr.aspx

[6] CITLIVÝ ÚDAJ. GDPR [online]. [cit. 2019-05-13]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/citlive-osobni-udaje/

[7] FOJTÍK, Petr. Návrh implementace nařízení GDPR v podmínkách obcí do tisíce obyvatel. Zlín: Univerzita Tomáše Bati ve Zlíně, 2017, 59 s. (79 240 znaků). Dostupné také z: http://hdl.handle.net/10563/41936. Univerzita Tomáše Bati ve Zlíně. Fakulta managementu a ekonomiky, Ústav regionálního rozvoje, veřejné správy a práva. Vedoucí práce Kolumber, David.

[8] GDPR. EUR-lex [online]. [cit. 2019-05-13]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016R0679

[9] MVČR: Legislativa [online]. [cit. 2019-05-13]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/gdpr-web-legislativa-legislativa.aspx

[10] GDPR: Implementace v ČR [online]. [cit. 2019-05-13]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

[11] OBECNÉ NAŘÍZENÍ. JSNS [online]. [cit. 2019-05-13]. Dostupné z: https://www.jsns.cz/gdpr/gdpr

[12] ZMĚNY. MVČR [online]. [cit. 2019-05-13]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/gdpr-web-legislativa-legislativa.aspx]%20[https://www.gdpr.cz/gdpr/zmeny/

[13] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[14] ŽŮREK, Jiří. Praktický průvodce GDPR. 1. vydání. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3.

[15] GDPR: Právní důvody pro zpracování osobních údajů. GDPR[online]. [cit. 2019-05-13]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pravni-duvody-zpracovani-ou/

[16] GDPR: Pověřenec pro ochranu osobních údajů [online]. [cit. 2019-05-13]. Dostupné z: https://www.gdpr.cz/gdpr/dpo/

[17] EPRAVO: Posouzení vlivu na ochranu osobních údajů. EPRAVO [online]. [cit. 2019-05-13]. Dostupné z: https://www.epravo.cz/top/clanky/posouzeni-vlivu-na-ochranu-osobnich-udaju-podle-gdpr-105892.html

[18] OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ: Předchozí konzultace. [online]. [cit. 2019-05-13]. Dostupné z: http://www.privacy-regulation.eu/cs/36.htm

[19] MŠMT: Metodická pomůcka k aplikaci GDPR ve školství [online]. [cit. 2019-05-13]. Dostupné z: http://www.msmt.cz/dokumenty-3/metodicka-pomucka-k-aplikaci-obecneho-narizeni-o-ochrane?highlightWords=gdpr

[20] HAMPLOVÁ, Hana. Implementace nařízení GDPR ve školské organizaci[online]. Ostrava, 2018 [cit. 2019-05-13]. Dostupné z: http://hdl.handle.net/10084/130140. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava.

[21] GDPR: Prohlášení o ochraně osobních údajů [online]. [cit. 2019-05-13]. Dostupné z: http://sps-prerov.cz/provoz-skoly/

[22] OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ: Článek 32 [online]. [cit. 2019-05-13]. Dostupné z: http://www.privacy-regulation.eu/cs/32.htm

[23] SPŠ PŘEROV: O škole [online]. [cit. 2019-05-13]. Dostupné z: http://sps-prerov.cz/o-nasi-skole/

[24] SPŠ PŘEROV: Výroční zpráva 2017/2018 [online]. [cit. 2019-05-13]. Dostupné z: http://sps-prerov.cz/provoz-skoly/

[25] ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ: Citlivé údaje [online]. [cit. 2019-05-13]. Dostupné z: https://www.uoou.cz/5-zvlastni-kategorie-osobnich-udaj-citlive-udaje/d-27274

[26] GDPR: Prohlášení o ochraně osobních údajů [online]. [cit. 2019-05-13]. Dostupné z: http://sps-prerov.cz/provoz-skoly/

[27] BAKALÁŘI: Evidence osobních údajů [online]. [cit. 2019-05-13]. Dostupné z: https://www.bakalari.cz/

[28] FOTOGALERIE: SPŠ Přerov [online]. [cit. 2019-05-13]. Dostupné z: http://sps-prerov.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GDPR	General Data Protection Regulaton
EU	Evropská unie
SPŠ	Střední průmyslová škola
PC	Personal computer
IT	Informační technologie
PZTS	Poplachové zabezpečovací a tísňové systémy
EPS	Elektrická požární signalizace
DPPC	Dohledové a poplachové přijímací centrum
ČR	Česká republika
MŠMT	Ministerstvo školství, mládeže a tělovýchovy

SEZNAM OBRÁZKŮ

Obrázek 1 - Hlavní úkony, které se musely provést před nabytím platnosti obecného nařízení [19] 23
Obrázek 2 - Střední průmyslová škola v Bystřici pod Hostýnem [28] 27
Obrázek 3 - půdorys přízemí na SPŠ v Bystřici pod Hostýnem 28
Obrázek 4 - půdorys 1. patra na SPŠ v Bystřici pod Hostýnem 28
Obrázek 5 - půdorys 2. patra na SPŠ v Bystřici pod Hostýnem 29
Obrázek 6 - Organizační struktura na SPŠ v Bystřici pod Hostýnem 31
Obrázek 7 - Evidence žáků školního systému Bakaláři [27] 43
Obrázek 8 - návrh zabezpečení osobních údajů a ústředny PZTS 1. patra 50
Obrázek 9 - návrh zabezpečení osobních údajů ve 2. patře 50

SEZNAM TABULEK

Tabulka 1 – Přehled oborů na SPŠ v Bystřici pod Hostýnem [24] 30
Tabulka 2 – Přehled počtu učitelů na SPŠ v Bystřici pod Hostýnem [24] 30
Tabulka 3 – Určení míry pravděpodobností 33
Tabulka 4 – Určení závažnosti hrozeb 34
Tabulka 5 – Hodnocení rizik 35
Tabulka 6 – Klasifikace rizika 36
Tabulka 7 – použité schématické značky 51