Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zabezpečení osobních údajů podle nařízení GDPR na středních školách.

Bc. Petr Skipala

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Petr Skipala

Veřejná správa a regionální rozvoj

Název práce

Zabezpečení osobních údajů podle nařízení GDPR na středních školách.

Název anglicky

Securing personal data under GDPR regulations at secondary schools.

Cíle práce

Diplomová práce je zaměřena na problematiku ochrany osobních informací s možností využití cloudových technologií ve školství. Hlavní cíl práce je navrhnout procesní řešení využívající osobní údaje s využitím cloudových technologií na středních školách. Dílčími cíly práce dále jsou:
- zpracovat přehled současného stavu nakládání s osobními údaji v administraivní oblasti střední školy,
- zpracovat přehled technických možností přístupu k osobním údajům v rámci výuky,
- analyzovat zpracované přehledy v kontextu nařízení o ochraně osobních údajů,
- navrhnout nové procesní řešení odpovídající GDPR za využití cloudových technologií.

Metodika

Hlavní metodou teoretické části je studium odborných informačních zdrojů, zejména aktuálních znění Obecného nařízení na ochranu osobních údajů. Praktická část diplomové práce je zaměřena na zpracování přehledu aktuálního stavu vybrané střední školy v oblasti administrativní, technologické a výukové. Na základě syntézy informací z teoretické části a výsledků z praktické části bude formulován návrh řešení podle GDPR a závěry práce.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

GDPR, zabezpečení informací, cloudové technologie, Google Edu, Microsoft 365 office, střední školy

---

Doporučené zdroje informací

GDPR Portal. EU GDPR Portal. [online]. <http://www.eugdpr.org/>

JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Brno: Computer Press, 2011. ISBN 978-80-251-3458-0.

LACKO, Ľuboslav. Osobní cloud pro domácí podnikání a malé firmy. Brno: Computer Press, 2012. ISBN 978-80-251-3744-4.

Ravindran, A, & Prakash, E (eds) 2016, The ICT Age, Cambridge Scholars Publishing, Newcastle-upon-Tyne. Available from: ProQuest Ebook Central. [8 October 2017].

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Jan Jarolímek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 31. 10. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 04. 03. 2018

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zabezpečení osobních údajů podle nařízení GDPR na středních školách." jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.3.2018 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Janu Jarolímkovi, Ph.D. za odborné vedení, vstřícnost a trpělivost při psaní této Diplomové práce.

Zabezpečení osobních údajů podle nařízení GDPR na středních školách.

Abstrakt

Tato diplomová práce je zaměřena na zpracování osobních údajů na odborné střední škole. Hlavním cílem diplomové práce je analyzovat současný stav zpracování osobních údajů na vybrané střední škole a navrhnout takové procesní postupy, které zabezpečí soulad s GDPR. Pro tvorbu nových procesů při zpracování osobních údajů je předpokládáno využití cloudových technologií.

V teoretické části práce jsou definovány jednotlivé specifikace činností a oblastí podle Nařízení Evropského parlamentu a Rady (EU) 2016/679. Je zde definován postup zpracování GAP analýzy pro potřebu stanovení současného stavu zpracování a evidování osobních údajů. Součástí je obecná specifikace Cloud computingu a základy procesního řízení.

Praktická část je zaměřena na zpracování GAP analýzy stanovených oblastí, ve kterých dochází ke zpracování osobních údajů. Podle vyhodnocených údajů z GAP analýz jsou navrženy procesní diagramy tak, aby byly jednoznačně popsány a zaevidovány veškeré hlavní i podpůrné činnosti spojené s evidencí osobních údajů. Vyhodnocované oblasti a navržené procesní diagramy jsou definovány s důrazem na možnost využití cloudových technologií.

Klíčová slova: GDPR, zabezpečení informací, cloudové technologie, Google Edu, Microsoft 365 office, střední školy

Securing personal data under GDPR regulations at secondary schools.

Abstract

This thesis focuses on a personal data processing on the technical secondary school. The main aim of the thesis is analysing of the current condition of a personal data processing in a selected high school and suggesting of the procedural advancements which will be secure in conformity with GDPR. In order to create a new procedure of a personal data processing, a usage of the cloud´s technology is supposed.

In the theoretical part of the thesis, particular specifications of activities and fields, in according to the regulation of the European Parliament and the Council (EU) 2016/679 are defined.

The processing operations the GAP analysis for a need of determination of current condition of processing and keeping a record of personal data is also defined in the thesis. This part includes a general specification of the Cloud computing and the basis of process management.

The practical part is focused on processing of the GAP analysis in established areas where processing of personal data is carried out. According to evaluated data from the GAP analysis, the process diagrams are designed to clearly describe and revise all the main and support activities related to the personal data record. Evaluated areas and designed process diagrams are defined with emphasis on the possibility of using cloud technologies.

Keywords: GDPR, IA Security, cloud computing technology, Google Edu, Microsoft 365 office, high schools

Obsah

1 Úvod

V současné době je pojem GDPR velmi aktuální, ale zároveň kolem něj panuje mnoho různých informací. Oficiální informace jsou přímo z EU, potažmo jako pracovní materiály skupiny WP 29. Dalším pro prostředí ČR důležitým zdrojem oficiálních informací je Úřad pro ochranu osobních informací společně s aktualizovaným zněním zákona č. 101/2000 Sb., o ochraně osobních údajů, který je v ČR na relativně vysoké úrovni. Na druhou stranu je ve většině subjektů (státních, soukromých, školství, zdravotnictví a další) informační šum, kdy není zcela jasné, co přesně je od jednotlivých subjektů vyžadováno. V oblasti státní správy lze aktuálně použit metodické pokyny, které zpracovalo např. Ministerstvo školství nebo Ministerstvo zdravotnictví.

Současný stav nakládání s osobními údaji v ČR lze rozdělit na dvě skupiny, v první jsou subjekty, které z jakéhokoliv důvodu byly nuceny svou činnost podřídit zákonu č. 101/2000 Sb. a pro ty je splnění požadavků Obecného nařízení relativně snazší. Naproti tomu ve druhé skupině je skupina subjektů, nelze však říci, že například většina je ze soukromého sektoru, které o zmíněném zákonu věděly, ale z pohledu sankcí nebo jiných možných postihů pro ně náklady zásadně převažovaly nad hrozbami.

Tento stav je v této době mediálně zvýrazněn, a to především v rovině možných sankcí při nedodržení Obecného nařízení.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce si klade za cíl analyzovat současný stav na vybrané střední škole z pohledu zpracování osobních údajů a navrhnout takové procesní postupy, které zabezpečí soulad s Obecným nařízením. K dosažení souladu provádění veškerých operací s osobními údaji je navržen a vybrán jako jeden z hlavních prostředků v oblasti informačních technologií cloud computing.

Dílčí cíle byly stanoveny tak, aby jejich zpracování přineslo doplňující podklady pro hlavní cíl, tedy tak, aby došlo k vytvoření podkladů s výsledky GAP analýzy současného stavu, který je nutné zmapovat v určených oblastech. Protože se jedná o střední školu, je k dispozici velké množství různých informačních toků, a to jak s osobními, tak i s citlivými údaji.

Pro správné posouzení všech dostupných možností je nutné zajistit revizi stavu výpočetní techniky, kterou škola používá jak k řízení svých provozních agend, tak zároveň i pro výuku. V průběhu výuky může docházet k ukládání, případně distribuování osobních údajů studentů, proto je také nutné zjistit, jaký vliv a jaké skupiny těchto informací jsou přímo ve výuce využívány.

Dalším dílčím cílem je veškeré získané informace zpracovat a strukturalizovat tak, aby bylo možné je vyhodnotit z pohledu aktuálně daných pokynů Obecného nařízení a provést doplnění GAP analýzy o návrh cílového stavu, který splňuje tyto pokyny.

Protože v současnosti jsou cloudové technologie jedním z důležitých segmentů v oblasti zpracování informací, zároveň v kontextu GDPR se jejich využití jeví jako vhodné, tak ze získaných informací bude nutné navrhnout procesní diagramy pro maximálně efektivní řešení za využití vhodných cloudových technologií, které jsou k dispozici pro školní prostředí, tedy jejichž finanční parametry jsou navrženy tak, aby je školy mohly využít za co nejnižší ceny.

2.2 Metodika

Základní činností pro získání relevantních údajů pro další zpracování je vypracování GAP analýzy po jednotlivých logicko funkčních celcích.

Pro zajištění validních informací je nutná znalost zpracovávané organizace, což je zajištěno přímou účastí při zkoumání a analyzování informačních skupin. K vyšší kvalitě zpracování analýzy přispívá zkušenost jak s procesním řízením, tak s aktuální znalostí problematiky GDPR a činností externího vyučujícího a konzultanta v oboru informačních technologií. Díky uvedeným faktům lze získané informace považovat za objektivní a nezkreslené přímou závislostí na dané organizaci.

Podstatnou součástí metodiky pro zpracování práce je nutná soustavná aktualizace informací o vývoji dané problematiky. Protože se jedná o proces a činnosti, kterým nastane účinnost 25. 5. 2018, tak je nutné nově zjištěné metodiky do samotné práce zapracovat tak, aby tato obsahovala maximum změn podle nejnovějších aktualizací a metodik. Na druhou stranu nelze neustále zvolenou metodiku měnit, je nutné stanovit základní pravidla zpracování GAP analýzy a jejich výsledky následně hodnotit s co nejaktuálnějšími znalostmi. Do samotné práce byl jako poslední použit aktualizovaný postup vydaný MŠMT dne 15. 3. 2018.

3 Přehled řešené problematiky

Vstupním kritériem pro tuto práci je oblast ochrany osobních údajů, v současné době známé pod zkratkou GDPR a v této práci bude tato oblast využívat také často používaného názvu **Obecné nařízení**. Už ze samotného názvu plyne, že se jedná o nařízení, vydané EU a s tím souvisí povinnost plnit toto nařízení tak jak je nadefinováno.

3.1 Význam Obecného nařízení

Pojem Obecné nařízení tvoří novou právní oblast ochrany osobních údajů v Evropě. Toto Obecné nařízení bude od 25. května 2018 určovat pravidla ke zpracování osobních údajů zároveň s právy subjektu údajů (fyzická osoba). Zejména v českém právním prostředí toto Obecné nařízení bude nahrazovat zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, přesněji řečeno zákon o ochraně osobních údajů po jeho novelizaci bude pouze upravovat jen některé aspekty, které se týkají Úřadu pro ochranu osobních údajů (např. jeho organizaci, ustavení). Dále také některé jednotlivé záležitosti, které jsou nutné k dotvoření kompletního rámce ochrany osobních údajů. Ty nejsou upraveny Obecným nařízením nebo jim je umožněno či dokonce stanoveno upravení na vnitrostátní úrovni.

Univerzální použitelnost je charakteristická pro Obecné nařízení, a to ve všech státech Evropské unie (a Norska, Islandu a Lichtenštejnska) a zároveň má tedy i sjednocující účinek, protože jednotná pravidla pro získání osobních údajů budou platná v každém státě Evropské unie a také ve třech zmíněných státech. Jedním z cílů pro přijetí Obecného nařízení bylo zajištění větší jednotnosti předpisů ochrany osobních údajů.

Úplný název je Nařízení Evropského parlamentu a Rady (EU) 2016/679, který je ze dne 27. dubna 2016 o ochraně fyzických osob ve spojení se zpracováním osobních údajů a o volném oběhu těchto dat a o zrušení směrnice 95/46/ES .

V odborných textech či hovorech se lze setkat s anglickou zkratkou Obecného nařízení, a to GDPR (General Data Protection Regulation).

Protože Obecné nařízení stanovuje práva a povinnosti ve zpracování osobních údajů, tak v tomto rozsahu bude současný zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů nahrazován. V současném zákoně budou práva a povinnosti o ochraně osobních údajů nahrazena právy a povinnostmi, které vyplývají z Obecného nařízení. Mezi

aspekty, u kterých se předpokládá vnitrostátní úprava, patří zpracování osobních údajů s cílem výkonu svobody projevu, svobody umělecké tvorby a vědeckého bádání, práva na informace[1].

3.2 Povinnosti Obecného nařízení

Základní principy, zásady zůstávají neměnné, pouze byly detailněji rozpracovány a upřesněny (např. zabezpečení osobních údajů, nutnost disponovat pro zpracování právním důvodem, transparentnost vůči subjektu údajů). Obecné nařízení přináší nástavbu na těchto podkladech, která spočívá v doplňkových nových povinnostech, které budou pro české správce nové.

Jedná se především o tyto nové povinnosti:

- „povinnost vést záznamy o činnostech zpracování,
- posouzení vlivu na ochranu osobních údajů,
- předchozí konzultace,
- ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů,
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů,
- ustavení pověřence pro ochranu osobních údajů[2]".

Kromě povinného vedení záznamů o činnostech zpracování a ustanovení pověřence, tak ostatní nové povinnosti jsou zakládány na přístupu založeném na riziku, to znamená, že jejich uplatnění je vázáno na výskyt rizika nebo vysokého rizika pro svobody a práva subjektu údajů. Nicméně i když u povinnosti určit pověřence nejsou používané pojmy riziko či vysoké riziko, tak v této povinnosti se do určité míry odráží přístup založený na riziku, protože určitá zpracování, lépe řečeno určité subjekty, je povinností určit pověřence pro ochranu osobních údajů.

[1] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

[2] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

3.2.1 Posouzení vlivu na ochranu osobních údajů

Pokud je patrné, že určitý druh zpracování, zvláště při využívání nových technologií, s přihlédnutím k rozsahu, povaze, účelům a kontextu zpracování bude znamenat vysoké riziko pro svobody a práva fyzické osoby, musí správce provést posouzení vlivu na ochranu osobních údajů. To se však musí provést před zahájením předmětného zpracování. Správce si vyžádá posudek pověřence pro ochranu osobních údajů, pokud byl určen[3].

Posouzení vlivu na ochranu osobních údajů je důležité především:

- „u systematického a rozsáhlého 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,
- u rozsáhlého zpracování zvláštních kategorií údajů nebo rozsudků v trestních věcech,
- u rozsáhlého systematického monitorování veřejně přístupných prostorů[4]".

Konzultace ohledně zpracování osobních údajů je správce povinen s Úřadem pro ochranu osobních údajů, jestliže z posouzení vlivu na ochranu osobních údajů vyplývá, že by určené zpracování mělo za důsledek vysoké riziko, pokud by správce nepřijal opatření ke snížení tohoto rizika. Významem předchozí konzultace je opravovat hrozící vysoké riziko.

3.2.2 Důležité pojmy

3.2.2.1 Zpracování osobních údajů

Zpracováním se rozumí jakákoli operace či souhrn operací s osobními údaji, nebo také soubory osobních údajů, vykonávaným pomocí (či bez pomoci) automatizovaných postupů. Mezi tyto postupy patří například zaznamenání, shromáždění, uspořádání, uložení, strukturování, pozměnění nebo přizpůsobení, vyhledávání, použití, nahlédnutí, zpřístupnění přenosem, šíření, zkombinování či seřazení, omezení, zničení nebo výmaz.

[3] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

[4] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

V Obecném nařízení však nelze chápat zpracování jako jakékoli nakládání s osobními údaji. Jedná se spíše o sofistikovanější činnost, kterou provádí správce s osobními údaji za daným účelem a činí tak systematicky. Zmíněný pojem zpracování má tentýž význam, jaký měl v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů[5].

3.2.2.2 Osobní údaj

Pojem osobní údaj představuje jakoukoli informaci o identifikovatelné či identifikované fyzické osobě neboli subjektu údajů. Identifikovatelnou fyzickou osobou se rozumí fyzická osoba, kterou lze, ať už přímo či nepřímo identifikovat, a to odkazem na určitý identifikátor (číslo, jméno, síťový identifikátor) či na jeden nebo více určitých prvků fyzické, genetické, fyziologické, psychické, kulturní nebo společenské, ekonomické identity této fyzické osoby.

Tento pojem nebyl změněn oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

3.2.2.3 Subjekt údajů

Fyzická osoba, které se osobní údaje týkají, se nazývá subjektem údajů. Subjektem údajů však není právnická osoba, tudíž údaje, které se vztahují k právnické osobě, nejsou osobními údaji. Osobní údaje mohou být výhradně ve spojitosti s žijící fyzickou osobou, protože Obecné nařízení vyřazuje svoji účinnost na údaje o zesnulé osobě.

Tento pojem má totožnou definici jako v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů[6].

3.2.2.4 Profilování

Pod pojmem profilování se rozumí forma či tvar automatizovaného zpracování osobních údajů, které spočívají v jejich použití ke klasifikaci některých osobních aspektů, které se vztahují k fyzické osobě, a to zejména k odhadu či rozboru aspektů, které se týkají jejího pracovního výkonu, zdravotního stavu, ekonomické situace, osobních preferencí, spolehlivosti, zájmů, chování, pohybu či místa, kde se nachází.

---

[5] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

[6] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

Tento pojem je nově definován, nicméně se nejedná o žádnou novinku, protože v současné době dochází také k profilování. Profilování není zakázáno zákonem o ochraně osobních údajů nebo Obecným nařízením. Je ale důležité, aby se uskutečnilo na základě stanovených pravidel a v předvídaných případech. Tento pojem je častý například ve finančních službách, kde klient, který žádá o hypotéku je profilován finančními subjekty, které hodnotí jeho schopnost splácet.

3.2.2.5 Správce

Správcem se rozumí subjekt, u kterého nerozhoduje právní forma, který určuje prostředky a účely zpracování osobních údajů a odpovídá primárně za zpracování. Osobní údaje správce zpracovává pro účely, které vyplývají z jeho činnosti (ze smluv, zákonem stanovené povinnosti), ale musí je zpracovávat i pro svoje určené účely (pro vlastní oprávněné zájmy, jestliže tyto zájmy nepřesahují zájem na ochraně základních práv a svobod fyzické osoby.

Jakýkoli subjekt může být správcem. Fyzická osoba, která zpracovává osobní údaje takovým způsobem, který vyřazuje uplatnění výjimky domácí či osobní činnosti, může být správcem. Respektive pokud nedochází k nakládání s osobními údaji, nesplňující definici jejich zpracování.

Zmíněný pojem nebyl změněn oproti zákonu č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů[7].

3.2.2.6 Zpracovatel

Subjekt, kterého si správce najímá proto, aby prováděl pro něj zpracovatelské operace s osobními údaji, se nazývá zpracovatel. Jednodušeji řečeno, zpracovatel vypracovává osobní údaje pro správce. Zpracovatel může provádět pouze takové operace, kterými ho správce pověří či vyplývají z činnosti, kterou byl zpracovatel pověřen správcem. Tím se zpracovatel odlišuje od správce. O zpracovatele se jedná pouze ve vztahu k osobním údajům, které jsou poskytnuté správcem, ne však osobních údajů, které zpracovatel zpracovává pro účely,

[7] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

dotýkajícího se ho přímo (např. zpracováním osobních údajů pro vlastní zaměstnance). U zpracovatele stejně jako u správce není rozhodující jeho právní forma.

Daný pojem zpracovatel nebyl změněn oproti zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů[8].

3.2.3 Zvláštní kategorie osobních údajů (citlivé údaje)

Existují osobní údaje takové povahy, které mohou subjekt údajů poškodit samy o sobě např. v zaměstnání, ve společnosti či ve škole, a mohou tak způsobit jeho diskriminaci. Právě proto je úplným výčtem stanovena skupina údajů, které jsou pokládány za citlivé vůči subjektu údajů, a kterým je umožněna zvýšená ochrana při zpracování. Ochrana se projevuje zvláště v uvedených zvláštních právních důvodech. Na základě těchto zvláštních právních důvodů je lze zpracovávat. Je zde vázanost určitých institutů na jejich zpracování, při hlavní činnosti (ustavení pověřence, posouzení vlivu), hlavní důraz je kladen na mnohem vyšší bezpečnost.

Do této kategorie osobních údajů spadají takové údaje, vypovídající o etnickém či rasovém původu, náboženském vyznání, politických názorech, zdravotním stavu nebo sexuálním životě či orientaci a členství v odborech. Dále zde lze zahrnout i biometrické a genetické údaje, zpracovávající se za účelem identifikace fyzické osoby. Tyto osobní údaje jsou totožné s výčtem citlivých údajů, uvedené v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Do zvláštní skupiny osobních údajů již nelze zahrnout záznam o odsouzení za trestný čin. Tyto záznamy týkající se rozsudků v trestních činech a trestních věcech jsou zahrnuty do zvláštního režimu v článku 10 Obecného nařízení[9].

Zvláštní skupina osobních údajů, které je možné zpracovávat, za předpokladu:

- „subjekt údajů udělil výslovný souhlas,
- zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany,

[8] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

[9] Tamtéž

- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas,
- zpracování provádí v rámci svých oprávněných činností nadace, sdružení či jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy nebo na osoby, které s tímto subjektem udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt,
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů,
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo při jednání soudů,
- zpracování je nezbytné z důvodu významného veřejného zájmu,
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče atd.,
- zpracování je nezbytné z důvodu veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění bezpečnosti zdravotní péče, léčivých přípravků nebo zdravotnických prostředků,
- zpracování je nezbytné pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely[10]".

3.2.3.1 Správce, zpracovatel

Za dodržování povinností stanovených Obecným nařízením je odpovědný správce. Nejdůležitější je zachování zásad zpracování, které správce musí být schopen doložit. Základním nutným předpokladem pro existenci spolehlivého právního důvodu vyhotovení osobních údajů, kterými správce musí disponovat tak, aby byl schopen zpracovat osobní údaje. Důležité je zabezpečení osobních údajů. Nezbytné musí být také dodržování ostatních povinností kladených Obecným nařízením.

V závislosti na aspektech zpracování se určitého správce Obecné nařízení dotkne jinými způsoby. Tomu však odpovídají i přípravy správce. Přístup zakládající se na riziku váže určité

[10] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

povinnosti jen na riziková nebo vysoce riziková zpracování. To znamená, že některé povinnosti nebude mnoho správců muset plnit, a naopak na jiné správce dopadnou všechny stanovené povinnosti. Důležité je zpracování vlastní analýzy, která zjistí, jaké povinnosti se na daného správce vztahují. V analýze může být zahrnuta specifikace slabých míst správce (v provedení či zabezpečení právních důvodů, které jsou v souladu s podmínkami Obecného nařízení). Pro správce, který řádně plní stanovené povinnosti, které vyplývají z aktuálního zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů by Obecné nařízení nemělo představovat významný problém. Důležité je nezapomenout na informovanost zaměstnanců[11].

3.2.3.2 Vztah správce - zpracovatel

Správce má možnost přibrat jiný subjekt ke zpracování osobních údajů. Ten pro něj bude zpracovávat osobní údaje. Zpracovatel by měl být takový, který poskytne dostatečné záruky organizačních a technických opatření tak, aby toto zpracování splňovalo požadavky Obecného nařízení a současně tak byla zajištěna subjektu údajů ochrana práv. Mezi správcem a zpracovatelem musí být uzavřena smlouva, ve které je stanovena doba trvání, předmět, účel a povaha zpracování, kategorie subjektů údajů a typ osobních údajů, práva a povinnosti správce. Další povinností je, aby smlouva byla zpracována na základě článku 28. odst. 3 Obecného nařízení.

Smlouva nemusí být vždy uzavřena samostatně, ale může být součástí i jiných smluv, které jsou uzavřeny mezi správcem a zpracovatelem v rámci obchodního vztahu. Správce se nezbavuje odpovědnosti za vypracování osobních údajů přizváním zpracovatele.

Pojem řetězení zpracovatelů nastává v situaci, kdy zpracovatel se může zapojit do vyhotovení jiného zpracovatele. Toto řetězení zpracovatelů není předem zakázáno, nicméně je důležité, aby správce dal zpracovateli písemné svolení. Svolení může být obecné, nebo určeno konkrétnímu zpracovateli. Cílem je, aby správce odpovídající primárně za zpracování osobních údajů věděl, jaké subjekty zpracovávají pro něj osobní údaje[12].

---

[11] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

[12] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

3.2.4 Pověřenec pro ochranu osobních údajů

Správce a zpracovatel musí jmenovat pověřence, pokud:

- „zpracování provádí orgán veřejné moci či veřejný subjekt s výjimkou soudů jednajících v rámci svých soudních pravomocí,
- hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů,
- hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů a osobních údajů týkajících se rozsudků v trestních věcech[13]".

Je možnost jmenovat jediného pověřence pro skupinu podniků, nicméně pro každý podnik musí být snadno pověřenec dosažitelný.

Podle článku 37 odst. 1 písm. a) Obecného nařízení je povinností obce jmenovat pověřence. Avšak úřad nezastává názor, aby každá obec měla svého vlastního pověřence. Je však možné, aby pověřenec vykonával činnost pro určitý počet obcí (např. pověřenec vyššího územně samosprávného celku nebo dohodnutí několika obcí o najmutí si vlastního pověřence). Obecné nařízení také umožňuje jmenovat jednoho pověřence pro více správců. Ti mohou být veřejným subjektem nebo orgánem veřejné moci.

Je důležité, aby pověřenec byl podřízen pracovníkům vrcholového řízení správce nebo zpracovatele. Nejedná se však o organizační podmínku, ale spíše o podmínku, která umožňuje pověřenci mít přímý přístup k vedení společnosti. Je důležité, aby nebyl žádný mezičlánek mezi pověřencem a vedení dané společnosti při předávání informací.

Hlavním úkolem pověřence je poskytování poradenství a informací správci nebo zpracovateli, a také zaměstnancům podílejících se na zpracování. Pověřenec musí monitorovat zpracování tak, aby bylo v souladu s Obecným nařízením a ostatními předpisy. Pokud se jedná o posouzení vlivu k ochraně osobních údajů, tak pověřenec může poskytnout své poradenství. Nezbytnou součástí je také spolupráce s Úřadem pro ochranu osobních údajů.

[13] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

Podle Obecného nařízení pro pověřence nejsou stanoveny požadavky týkající se vzdělání a akademických titulů. Musí se jednat o osobu, která disponuje odbornou znalostí práva a profesními kvalitami a praxí v oblasti ochrany osobních údajů. Je nutné, aby také ovládal Obecné nařízení. Pro každého správce může být důležitý pověřenec s jiným vzděláním (např. technické či právní vzdělání).

Obecným nařízením není stanovena certifikace pověřence pro výkon funkce. Správce může vybrat osobu, která má či nemá certifikát.

Obecné nařízení nevylučuje možnost, že by pověřence poskytla právnická osoba např. jako službu. Je však podstatné, aby byla určena fyzická osoba, která bude vykonávat pověřence. Správce by měl vzít v úvahu při využití služby pověřence, že pověřencem musí být osoba, která detailně pozná u správce zpracování osobních údajů. Pouze tak dále dokáže identifikovat možná rizika, která nemusí být u najatého pověřence. Z hlediska konkurence je vhodné zvážení situace, kdy poskytovatel může poskytnout stejného pověřence konkurenci. V tomto případě však hrozí prozrazení know-how[14].

3.2.5 Práva subjektů osobních údajů podle GDPR

Tento článek se zabývá druhou stranou vztahů v oblasti ochrany osobních údajů, a to právy subjektů osobních údajů. Subjektem se standardně rozumí fyzická osoba, které osobní údaje zpracovává správce nebo zpracovatel osobních údajů.

3.2.6 Zásada transparentnosti a právo na informace

Nařízení je založeno na mnoha základních zásadách. Každá zásada obsahuje určité povinnosti správce osobních údajů a práva subjektu osobních údajů tomu odpovídající. Subjekt má tedy právo, aby jeho osobní údaje byly vypracovány pouze na bázi některého z titulů - zákonných důvodů - vymezených v Obecném nařízení (např. založeném na jejich souhlasu (zásada zákonnosti), aby byly vypracovány jen pro konkrétní, vyjádřené a legitimní účely (zásada účelového omezení). Dále aby zpracování bylo přiměřené, omezené na potřebný rozsah se zřetelem na účel zpracování, relevantní (zásada minimalizace údajů)[15].

[14] Dostupné z: *Základní příručka* <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744> [online 2018-01-11]

[15] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

Zásada transparentnosti patří mezi jednu z nejvýznamnějších. Podle odst. 58 preambule tato zásada Obecného nařízení vyžaduje „aby všechny informace určené veřejnosti nebo subjektu údajů byly stručné, snadno přístupné a srozumitelné, podávané za použití jasných a jednoduchých jazykových prostředků a ve vhodných případech navíc i vizualizace. Pokud budou tyto informace určeny veřejnosti, mohly by být poskytovány v elektronické podobě, například prostřednictvím internetových stránek."[16] Účelem této zásady je upravení formy a pochopitelnost informací, které jsou poskytovány subjektům údajů vzhledem ke zpracování.

Hlavním právem každého subjektu údajů oproti správci je tedy právo na určitý obnos informací poskytnutých stručným, srozumitelným způsobem, který je uvedený výše. Právo na informace není novinkou, i současná právní úprava, která vychází ze Směrnice č.95/46/ES o ochraně osobních údajů nařizovala správcům povinnost poskytovat subjektům určité informace. Obecné nařízení však rozšiřuje okruh těchto informací. [17]

Podle Obecného nařízení mají subjekty právo, aby správci jim sdělili výše uvedeným způsobem informace o:

- „identifikačních údajích správce, případně jeho zástupce v EU a kontakty na případného Pověřence pro ochranu osobních údajů, pokud jej má správce mít;
- účelech zpracování, pro které jsou osobní údaje určeny, a právním základu pro zpracování;
- kategoriích zpracovávaných osobních údajů;
- případných příjemcích osobních údajů;
- detailech případného předávání osobních údajů mimo EU (zahrnující identifikaci konkrétních zemí, způsobech zajištění ochrany osobních údajů a zárukách ochrany)
- době zpracování osobních údajů, nebo kritériích použitých pro stanovené této doby;
- je-li titulem zpracování ochrana oprávněných zájmů správce nebo třetí osoby, identifikace těchto oprávněných zájmů;
- právech subjektu údajů v užším slova smyslu – právu požadovat od správce přístup ke zpracovávaným osobním údajům, právu na jejich opravu nebo výmaz, na omezení zpracování, právu vznést námitku proti zpracování, právu na přenositelnost údajů, právu na podání stížnosti k dozorovému úřadu;

[16] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[17] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

- dochází-li ke zpracování na základě souhlasu subjektu údajů, o právu na odvolání tohoto souhlasu, aniž by tím byla dotčena zákonnost zpracování, k němuž docházelo před odvoláním tohoto souhlasu;
- skutečnosti, zda je poskytnutí osobních údajů založeno na zákonném nebo smluvním základě a o následcích neposkytnutí údajů;
- o tom, zda ve vztahu k osobním údajům má docházet k automatizovanému rozhodování, s informací o použitých postupech a následcích tohoto zpracování pro jednotlivce[18]".

Zmíněné informace jsou základním právem subjektu údajů, nicméně standardně je subjekt má obdržet v odpovídající lhůtě po získání osobních údajů, to však pouze do jednoho měsíce, vzhledem na konkrétní okolnosti, za které jsou zpracovány osobní údaje.

Za podmínky, že osobní údaje mají sloužit ke komunikaci se subjektem, tak informace musí být poskytnuty nejpozději do té doby, kdy dojde poprvé ke komunikaci s daným subjektem.

Je nutné si však uvědomit, že výše uvedené informace se vztahují k určitému účelu, který vyplývá z náležitého právního důvodu zpracování. Pokud však dojde ke zpracování k novému účelu, tak je nutné poskytnou tyto informace subjektu znovu, a získat souhlas od subjektu k tomuto novému účelu. Výše určené informace není nutné poskytovat subjektům v případě, že už dané informace mají, nebo v případě, že není možné poskytnout takové informace či vyžaduje nepřiměřené úsilí. Dalším případem, kdy informace nemusí být poskytnuty, je jejich zpřístupnění a získání stanoveno právem Unie či jsou předmětem služebního tajemství[19].

3.2.6.1 Práva subjektů v užším slova smyslu

V užším slova smyslu, jsou práva subjektů považována za možnosti uskutečnění určitých přímých nároků subjektu oproti správci podle žádosti subjektu. Tento výčet je stanoven

[18] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[19] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

Obecným nařízením v č. 15 až 22. Správce má povinnost informovat subjekt o těchto nárocích, které jsou v rámci informační povinnosti.

3.2.6.2 Právo na přístup k osobním údajům

Subjekt může požádat správce o informaci, zda jsou jeho osobní údaje zpracovávány. V případě, že jsou zpracovávány, tak může subjekt požádat správce o přístup k těmto údajům. Tento přístup je poskytován pomocí kopie osobních údajů. První kopie je vždy poskytnuta zdarma, až případné další kopie jsou zpoplatněny přiměřeným poplatkem.

Pokud je žádost podána pomocí elektronické komunikace, tak i kopie osobních údajů musí být poskytnuta v elektronické formě a to v běžném formátu. Je to z toho důvodu, že správci pracují se specifickými software a musí být schopni exportovat data v čitelném formátu pro běžného uživatele. Konkrétní případ, kdy subjekt uplatní právo na přístup k osobním údajům uvedený v bodě 63 preambule Obecného nařízení, podle kterého zahrnuje právo na přístup […] „přístup k údajům o svém zdravotním stavu, například k údajům ve své lékařské dokumentaci, která obsahuje například informace o diagnóze, výsledky vyšetření, posudky ošetřujících lékařů a údaje o veškeré léčbě a provedených ošetřeních nebo zákrocích[20]“.

Nebude možné, aby lékař odmítl dát pacientovi výpis zdravotnické dokumentace, kterou by pacient předal jinému lékaři. Na informace o vyhotovení osobních údajů, na které má subjekt právo na základě žádosti, jsou podobná, co se týče obsahu těm, které automaticky správce poskytuje subjektu v souvislosti s informační povinností. Subjekt na základě své žádosti získá informace o tom, z jakého důvodu se osobní údaje zpracovávají, dobu po kterou budou uchovány, kdo je příjemce osobních údajů, jaká je logika automatizovaného zpracování osobních údajů a v neposlední řadě také jaké mohou být důsledky. Preambule Obecného nařízení doporučuje správcům, aby poskytli subjektům dálkový přístup, který umožní přímý přístup k osobním údajům. Toto ustanovení lze chápat jako doporučení, avšak pro správce toto doporučení přestavuje možnost doložení dodržení zásady odpovědnosti. Ve všech případech uvedená práva subjektů údajů představují důvod k tomu, aby se zanalyzoval stav a možnosti daných informačních systémů.

[20] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

Preambule Obecného nařízení obsahuje změkčení povinnosti správce v situaci, že subjekt zpracovává množství informací, které se týkají subjektu údajů. V takovém případě správce má mít možnost požádání subjektu údajů o informaci o jakou činnost nebo informaci se týká jeho žádost. Z toho vyplývá, že v této situaci správce nemusí poskytnout subjektu informace o všech zpracovaných údajích. V textu Obecného nařízení se již žádné změkčení neobjevuje. S ohledem na funkci preambulí komunitárních předpisů můžeme očekávat, že správci, kteří zpracovávají velké množství informací, by si obhájili upřesňující požadavek[21].

Zároveň ale v této oblasti není nijak definován pojem **velké množství informací.**

3.2.6.3 Právo na opravu zpracovávaných údajů

Článek 16 Obecného nařízení předepisuje právo subjektu žádat vůči správci opravu nesprávně zpracovávaných údajů, a doplnění údajů neúplných.

3.2.6.4 Právo na výmaz - tzv. právo být zapomenut

Na základě současné právní úpravy existuje právo požádat správce o výmaz a ukončení osobních údajů. Obecné nařízení však toto ukončení více rozvádí. Právo subjektu nastupuje obecně v případě výmazu jeho osobních údajů, kdy nesplňuje zpracování stanovené požadavky Obecného nařízení. V článku 17 je obsažen úplný výčet situací, kdy subjekt může zažádat o výmaz údajů[22].

Obvykle mezi nimi nalezneme případy:

„(1) osobní údaje přestaly být potřebné pro účely, pro které byly shromážděny,

(2) kdy subjekt údajů odvolal svůj souhlas se zpracováním a pro zpracování neexistuje žádný jiný důvod, anebo

---

[21] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[22] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

(3) subjekt údajů vznesl námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování[23]“.

Speciální režim dopadá na správce při přijímání požadavku o výmaz údajů, který zveřejnil osobní údaje subjektu. V této situaci je povinen přijmout „s ohledem na dostupnou technologii a náklady na provedení[24]“ kroky, které budou informovat ostatní správce o tom, že subjekt požádal o výmaz. Toto směřuje k ochraně uživatelů, kteří působí v on-line prostředí. Přiměřené kroky směřují pouze na straně správce k informovanosti ostatních správců nikoliv k odstranění[25].

3.2.6.5 Právo na omezení zpracování

Tento pojem představuje uvedení osobních údajů do tzv. izolace, kdy údaje mohou být jen uloženy, ale nemohou být jakkoli jinak zpracovávány bez souhlasu subjektu údajů. K požadavku na omezení zpracování může subjekt přistoupit v těchto případech:

- „popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit,
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů, a žádá místo toho o omezení jejich použití,
- nebo správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků (zejména např. v případě spotřebitelského sporu mezi správcem a subjektem)[26]”.

Pokud je zpracování provedeno automatizovanými prostředky, tak informační systém musí umožnit omezení, které podle charakteru poskytované služby může představovat

---

[23] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[24] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[25] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[26] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

přesunutí dat na samostatné úložiště, přijetí jiných opatření či blokaci osobních údajů na internetu.

3.2.6.6 Právo na přenositelnost údajů

Na rozdíl od stávající úpravy je toto právo zcela nové. Subjekt od správce může požadovat uveřejnění osobních údajů, které poskytl správci v běžném strojově používaném formátu, tak aby údaje mohly být uchovány pro vlastní potřebu anebo aby správce předal tyto údaje jinému správci. Je tedy důležité, aby správce komunikoval napřímo s ostatními správci za účelem předávání osobních údajů. Nový správce zcela odpovídá samostatně za právní titul zpracování a taktéž za celkový soulad zpracování s Obecným nařízením[27].

Neomezené není právo na přenositelnost údajů. Obecné nařízení jej stanovuje ve dvou případech a to:

„(1) zpracování je založeno na souhlasu subjektu nebo na smlouvě, jejíž je subjekt údajů smluvní stranou, anebo

(2) zpracování se provádí automatizovaně[28]".

Mezi nejčastější tituly patří souhlas subjektů a plnění smluvních povinností, proto v oblasti zpracování osobních údajů bude toto množství zpracovávaných údajů veliké. Je důležitá také podmínka, podle které se přenositelnost týká údajů, které jsou poskytnuty subjektem správci. Právo se nemusí vztahovat pouze na údaje, které jsou správci aktivně poskytnuty. Na základě pracovní skupiny WP 29, tato podmínka dopadá i na data, která aktivně subjekt správci neposkytne, ale naopak která dostane správce pomocí sledování chování subjektu.

Výslovně je uvedeno, že výkonem tohoto práva není omezeno právo na vymazání osobních údajů. Na zpracování, které je nezbytné pro plnění úkolu při výkonu veřejné moci nebo ve veřejném zájmu se právo na přenositelnost nevztahuje[29].

---

[27] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[28] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

3.2.6.7 Právo vznést námitku proti zpracování

Další novinkou, kterou Obecné nařízení zavádí, je právo na vznesení námitky proti zpracování. To je stanoveno ve třech situacích:

- „jsou jeho osobní údaje subjektu zpracovávány pro účely přímého marketingu – na základě vznesení námitky musí správce okamžitě takového zpracovávání zanechat; v tomto případě není právo na vznesení námitky čímkoli dalším omezeno a má absolutní povahu (bude se zajisté doplňovat s úpravou odhlášení od zasílání obchodních sdělení, u nás obsaženou v zák. 480/2004 Sb. o některých službách informační společnosti);
- při zpracování údajů pro účely vědeckého či historického výzkumu nebo pro statistické účely je subjekt oprávněn vznést námitku z důvodů, které se týkají jeho konkrétní situace, ledaže je zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu; toto právo je tedy méně absolutní, když v samotné námitce budou subjekty muset specifikovat důvody, týkající se jejich situace (na rozdíl od námitky podané v případě přímého marketingu, kdy nemusí být uváděn žádný důvod).
- při zpracování z důvodu veřejného zájmu nebo při výkonu veřejné moci, nebo pro účely oprávněných zájmů příslušného správce či třetí strany, musí správce na základě námitky zanechat zpracování, ledaže prokáže oprávněné důvody zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo nezbytnost zpracování údajů pro určení, výkon nebo obhajobu právních nároků; i v tomto případě je podání námitky podmíněno důvody, týkajícími se konkrétní situace subjektu[30]“.

---

[29] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

[30] Dostupné z: *Díl třetí: Práva subjektů osobních údajů podle GDPR* <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm> [online 2018-01-11]

3.3 DPIA - Posouzení vlivu na ochranu osobních údajů

Jedná se o proces, jehož podstata vychází přímo z definice zodpovědnosti správce v kontextu GDPR. Jeho hlavním cílem v problematice zpracování osobních údajů je:

- popis zpracování dat;
- posouzení nezbytnosti a přiměřenosti zpracování;
- podpora při zvládání rizik práv a svobod fyzických osob[31].

Zpracování DPIA pro operace s osobními údaji v rámci Obecného nařízení není povinné, ale její zpracování je požadováno, pokud lze stanovit, že [...] „je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení[32]“.

Pro jednoznačné posouzení, zda je pro daný okruh získávaných informací vhodné provést zpracování DPIA ilustruje schéma na obrázku 1.

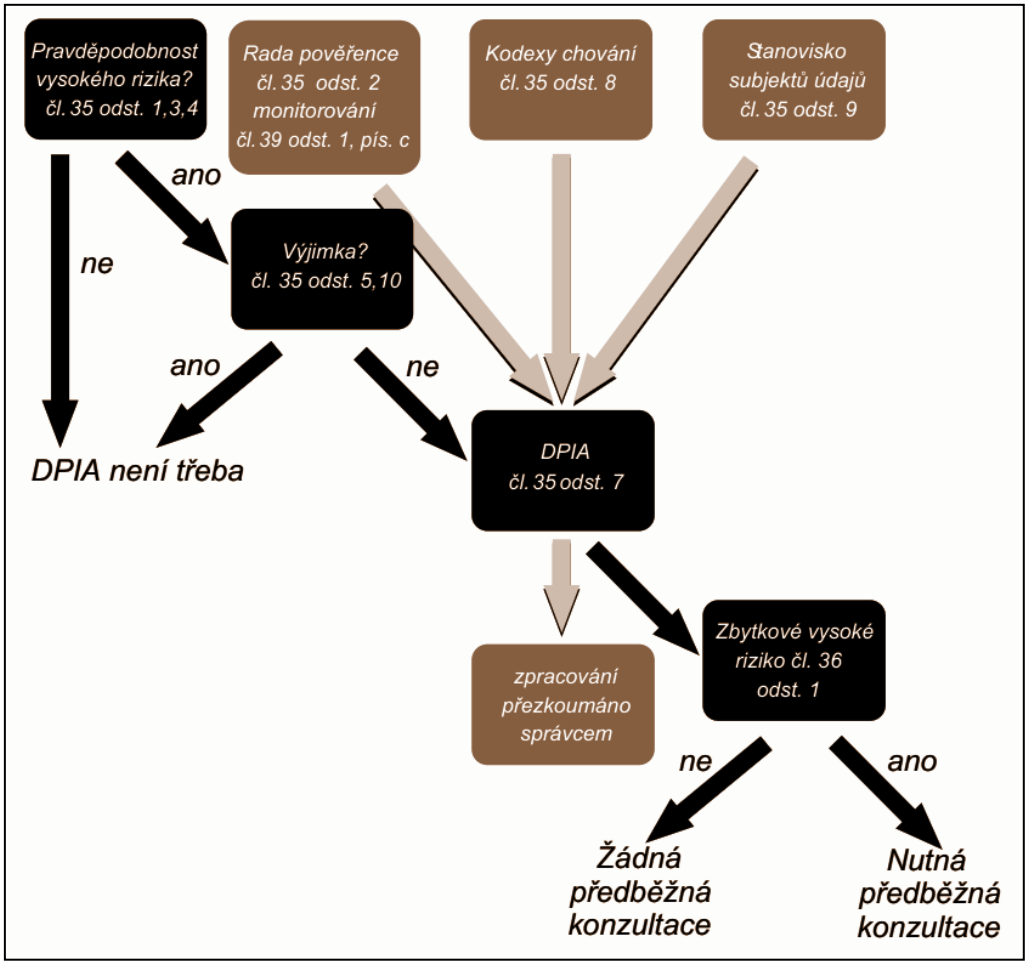
Zároveň je nutné konstatovat, že zpracování DPIA je plně v kompetenci správce. Při rozhodnutí, že bude DPIA zpracováno, je doporučeno se zvláště precizně zaměřit na následující oblasti dat, tedy oblasti, ze kterých jsou osobní údaje zpracovány:

- datové toky,
- příchozí data,
- odchozí data,
- rizika,
- pseudonymizace.

[31] Srov. NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. s. 98-99.

[32] Dostupné z: *EU obecné nařízení o ochraně osobních údajů "Posouzení vlivu na ochranu osobních údajů"* <http://www.privacy-regulation.eu/cs/35.htm> [online 2018-01-12]

Obrázek 1 - Zpracování DPIA v souvislosti s výskytem rizika[33]



3.4 GAP analýza

Jedná se v zásadě o první a základní krok v rámci implementace požadavků GDPR do firemních procesů a postupů. GAP analýza (doslova analýza mezery) je technika, která se používá k definování rozdílu mezi současným stavem a stavem požadovaným.

Pro základní popis současného stavu a navržení nového stavu byla použita GAP analýza. Tato metoda bývá používána při potřebě definice rozdílu, který vzniká při popsání současného a nově požadovaného stavu. V souvislosti s GDPR právě GAP analýza může napomoci správně specifikovat požadovaný stav tak, aby byl v souladu s Obecným nařízením. Zpracování analýzy má za cíl popsat tyto oblasti:

- „kde jsou v organizaci sběrné uzly osobních dat (místa sběru);

[33] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. s. 101.

- jaká je struktura shromažďovaných dat;
- pomocí jakých nástrojů;
- zjistit formální obsah nástrojů (formát formulářů apod.);
- jak byl získán souhlas ke zpracování osobních dat;
- kdo má přístup k datům;
- na základě jakého oprávnění;
- jak jsou data uchovávána a chráněna;
- v jakých systémech a aplikacích se s daty pracuje;
- v jakých procesech data figurují a jak probíhá jejich zpracování;
- zda jsou formy a procesy v souladu s nařízením GDPR;
- kontrola smluvních závazků týkajících se osobních dat;
- vazby a smlouvy třetích stran;
- přístup k hodnocení dopadů na soukromí;
- proces řízení incidentů a schopnost reagovat;
- jaké jsou návrhy a doporučení v případě nesouladu s nařízením[34]".

3.5 Cloud computing

V dnešní době je pojem cloud, nebo cloud computing, již poměrně známý. Většina běžných uživatelů moderní výpočetní techniky jej využívá, a to nejen cíleně nebo vědomě, ale v mnoha případech si ani neuvědomí, že většina činností se děje právě v cloudu.

3.5.1 Definice Cloud computingu

Aby bylo možné Cloud computing definovat, je potřeba zmínit základní části, na kterých je tento model postaven. Primární princip je založen na virtualizaci sdílených ICT zdrojů, kterými jsou hardware, paměť, konektivita nebo i služby jako např. databáze. Další hlavní vlastností cloudu je vysoká abstraktnost zdrojů, díky tomu lze jednotlivé zdroje v krátkém čase lehce škálovat[35].

Jedna z možných definic Cloud computingu, kterou specifikoval Národní ústav pro normalizaci a technologie USA (NIST) je, že je to model, který umožní na vyžádání z jakéhokoliv místa síťový přístup k výpočetním zdrojům. Mezi tyto zdroje patří servery,

[34] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. s. 97.
[35] Dostupné z: *Cloud Computing: Benefits, risks and recommendations for information security* <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment> [online 2018-01-20].

datová úložiště, samotné sítě a v neposlední řadě také služby a aplikace. Podstatou tohoto modelu je, že zdroje jsou poskytovány nebo odebírány podle požadavku na ně, a to bez zásahu uživatele. Struktura cloudového modelu je definována pomocí 5 základních vlastností, 3 servisních modelů a 4 metod zapojení[36].

Mezi základní znaky cloudu patří:

- On-demand služby, tedy takové služby, které jsou k dispozici na vyžádání. Jejich výhodou je možnost využívat vyžádané zdroje prakticky okamžitě podle dohodnutých pravidel.
- Druhým znakem je širokopásmový přístup k síti, který pomocí z kteréhokoli zařízení s webovým prohlížečem (tablet, mobil, stacionární či přenosné počítače) zajistí přístup ke cloudovým službám.
- Dalším znakem je sdílení výpočetních zdrojů poskytovatele. V jednom okamžiku tak mohou poskytovat služby více zákazníkům.

Dalším znakem jsou měřené služby, které automaticky kontrolují a optimalizují využití zdrojů v závislosti na požadovaném výkonu poskytovaných služeb. Děje se tak při měření využití funkcionality za určité míry abstrakce podle typu poskytovaného zdroje, která odpovídá poskytovanému druhu služby[37].

3.5.2 Náklady na Cloud computing

Hlavní výhodou Cloud computingu jsou [...] „snížené náklady na vlastnictví IT infrastruktury a rozložení investic do delšího období"[38], kdy při používání cloudových služeb odpadá většina nákladů spojených s vlastnictvím, správou a údržbou vlastních ICT zařízení. Další neméně podstatnou výhodou je relativně snadné a bez zásadního investičního zásahu rozšíření kapacit nebo výkonu využívaných služeb.

Fixní náklady bývají nahrazovány stálými odměnami za služby, kde využití služeb je rozloženo na delší období. Vnitrofiremní komunikace a mobilita je cloudem podpořena tak, že jak zaměstnanci, tak i externí pobočky mohou provozované aplikace kdykoli použít

---

[36] Dostupné z: *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology* <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [online 2018-01-20].

[37] Dostupné z: *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology* <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf> [online 2018-01-20].

[38] JANSA, Lukáš a Petr OTEVŘEL. *Softwarové právo: praktický průvodce právní problematikou v IT.* s. 311.

pomocí přístupu přes Internet. Ztrátu důvěry uživatelů si poskytovatelé cloudových služeb nemohou dovolit, proto mají velice propracovanou IT infrastrukturu, obrovská zálohovací centra a také vyškolené techniky. Proto také bezpečnost dat v cloudu je v současné době na vyšší úrovni než u běžné lokální IT struktury. Další podstatnou výhodou cloudového řešení je zajištění používání pouze legálního software[39].

O použití Cloud computingu z pohledu GDPR je vhodné zmínit stanovisko skupiny WP 29, která stanovuje, že zákazník cloudových služeb je správcem. Zároveň uvádí, že poskytovatel cloudových služeb je z tohoto pohledu zpracovatelem. Dále je také zdůrazněno, že poskytovatel cloudových služeb musí zajistit důvěrnost, přímo je stanoveno, že […] „jakákoli osoba, která jedná z pověření správce nebo zpracovatele, jakož i samotný zpracovatel, který má přístup k osobním údajům, je může zpracovávat pouze podle pokynů správce, ledaže právo stanoví jinak[40]“.

3.6 Procesní řízení

V organizacích všech typů je vhodné definovat organizační strukturu. Bez ohledu na danou strukturu zároveň v každé organizaci existují činnosti, které se opakují. Právě těmto činnostem je vhodné definovat procesy, a následně pomoci nich tyto činnosti, potažmo celou organizaci, řídit. Tento způsob vedení organizace je nazýván procesní řízení.

3.6.1 Proces

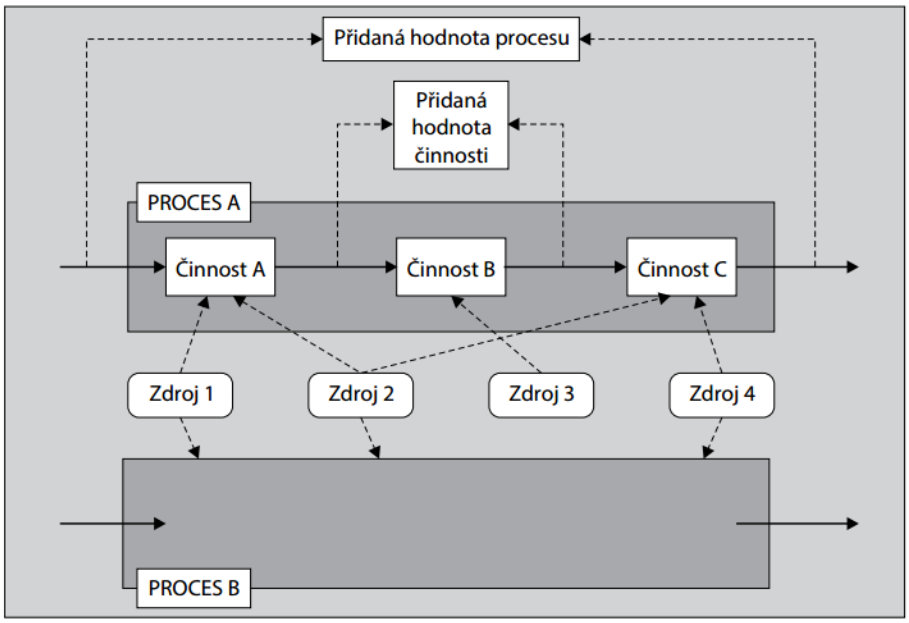
Proces je definován takto: jedná se o [...] „uspořádaný sled činností (aktivit), které transformují vstupy na výstupy a spotřebovávají přitom zdroje[41]“. Pro názornost je na obrázku 2 ukázáno, jak probíhá transformace v rámci procesu, jakým způsobem každá činnost provádí svou transformaci a při tom spotřebovávají zdroje. Ty se však během transformace nemění.

[39] Srov. JANSA, Lukáš a Petr OTEVŘEL. *Softwarové právo: praktický průvodce právní problematikou v IT*. s. 311.

[40] Dostupné z: *Úřad pro ochranu osobních údajů* <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=16706>[online 2018-01-02]

[41] FIŠER, Roman. *Procesní řízení pro manažery: jak zařídit, aby lidé věděli, chtěli, uměli i mohli*. s. 55.

Obrázek 2 - Přidaná hodnota a zdroje procesu[42]



3.6.2 Workflow

Nejen pro grafické zobrazení procesů se používá workflow. Jeho hlavním smyslem je co nejvíce automatizovaně zajistit provádění jednotlivých činností definovaných v procesu. Velkou výhodou, kterou workflow přináší, je jednoznačná identifikace právě probíhající části procesu, zodpovědné nebo výkonné osoby a v neposlední řadě také informace o časové náročnosti jednotlivých částí procesu. Většinou je workflow v informačních systémech realizováno pomocí delegování jednotlivých úkolů na konkrétní pozici nebo osobu, je sledován stav zpracování daného úkolu, jsou vyhodnocovány jednotlivé reakce nebo údaje a při dokončení konkrétního úkolu je tento vyhodnocen a zpracován další krok podle nadefinovaného procesu.

[42] FIŠER, Roman. *Procesní řízení pro manažery: jak zařídit, aby lidé věděli, chtěli, uměli i mohli*. s. 55.

4 Vlastní práce

Praktická část diplomové práce je zaměřena na analýzu aktuálního stavu vybrané střední školy v městě Jeseník v souvislosti s GDPR. Zároveň lze konstatovat, že obdobný stav je i na dalších středních školách v regionu, přičemž žádná z těchto škol není svým zaměřením úzce specializovaná na oblast informačních technologií, tedy lze předpokládat, že podle zpracovaného stavu by bylo možné postupovat u většiny středních škol v ČR.

Základem vstupní analýzy celého projektu je jednoznačné identifikování veškerých oblastí, ve kterých se instituce setkává s pojmy, vymezenými v článku 4 odst. 1 Obecného nařízení[43]. Tyto oblasti jsou rozděleny na skupiny podle druhu informací, které jsou zpracovávány a evidovány.

Jako základní celky pro zpracování analýzy současného stavu byly navrženy dvě hlavní oblasti. První z nich se soustředí na veškerou evidenci osobních údajů evidovanou v rámci chodu školy. Jsou rozděleny do těchto částí:

- současní studenti,
- bývalí studenti,
- zákonní zástupci,
- zaměstnanci,
- externí subjekty – dodavatelé.

Druhou oblastí jsou veškeré technologické systémy, které škola pro svůj chod využívá, případně jsou v prostorách školy použity. Jsou to tyto celky:

- školní veřejná síť,
- školní síť pro výuku,
- školní síť pro provoz školy,
- školní informační systém,
- ekonomický IS,
- docházkový systém,
- systém pro evidenci obědů,
- kamerový systém,
- webový portál školy.

[43] Dostupné z: *EU obecné nařízení o ochraně osobních údajů "Posouzení vlivu na ochranu osobních údajů"* <http://www.privacy-regulation.eu/cs/35.htm> [online 2018-01-12]

4.1 Návod na zabezpečení procesů vydaný MŠMT

V průběhu března 2018 [...] „MŠMT připravilo Stručný návod na zabezpečení procesů souvisejících s GDPR ve školách (nástin pracovního postupu). Záměrem materiálu je pomoci zorientovat se prakticky v povinnostech, které s GDPR souvisí[44]".

Současně s tímto návodem byly připraveny pracovní vzory záznamů o činnostech a také vzorová struktura směrnice o ochraně osobních údajů. V souvislosti s koncepcí této práce bylo konstatováno, že pro analyzovanou střední školu je tento materiál vhodným doplněním provedených analýz. Zároveň přináší metodickou podporu v návrhu interních směrnic. Co se týká zpracování GAP analýz jednotlivých stanovených oblastí, tak se tyto dvě oblasti vzájemně doplňují, protože zvolené oblasti byly stanoveny převážně z pohledu procesních zpracování pomocí informačních technologií. Pro širší využitelnost této práce je jako příloha doplněn materiál, který byl vytvořen na MŠMT. Jedná se o přílohu 1 - Vzor struktury směrnice, týkající se ochrany osobních údajů. Dále je pro potřebu zpracování doplněna adresa pro stažení pracovního sešitu „Příloha Záznamy o činnostech zpracování-2.xlsx[45]".

4.2 Analýza aktuálního stavu

Analýza současného stavu ve vazbě na Obecné nařízení je první a základní metoda, kterou je nutné použít pro zmapování situace v instituci. Musí být provedena podle důkladně nastaveného plánu a nesmí opomenout žádnou oblast, ve které by bylo možné nezmapovat činnosti v oblasti zpracování osobních údajů nebo jejich evidenci.

Jak bylo zmíněno v teoretické části, pro oblast zmapování jednotlivých oblastí pro splnění požadavků GDPR byla zvolena GAP analýza.

Plán analýzy je složen z bodů, které jednoznačně definují kritické oblasti, ve kterých je zmapován a vyhodnocen aktuální stav. V návaznosti na zjištěné výsledky jsou následně definována řešení, které při jejich dodržování uvedou řízení konkrétní činnosti do souladu s Obecným nařízením.

Pro analýzu byl stanoven seznam kontrolovaných činností, z kterých byl vytvořen formulář pro zaznamenání aktuálního stavu, následně při zpracování bude doplněn cílový stav a z těchto dvou identifikací bude stanoven GAP. Jedná se tedy o popsání rozdílu mezi

[44] Dostupné z: *Stručný návod na zabezpečení procesů souvisejících s GDPR* <http://www.msmt.cz/dokumenty-3/strucny-navod-na-zabezpeceni-procesu-souvisejicich-s-gdpr> [online 2018-01-02]

[45] Dostupné z: *Záznamy o činnostech zpracování* <http://www.msmt.cz/file/46280_1_1/> [online 2018-01-02]

současným stavem a stavem požadovaným neboli cílovým, včetně stanovení řešení nebo procesů, které k tomuto povedou.

Jednotlivé skupiny informací jsou vyhodnoceny pro každou dále zmíněnou oblast a jsou zaevidovány do tabulky. Tato slouží jako základní podklad pro návrh nebo aktualizaci procesního řešení pro danou oblast. Každá specifikovaná oblast je dále popsána z pohledu aktuálního stavu v informační rovině, a zároveň je doplněna vyhodnoceným formulářem s aktuálním stavem.

Pro správné vyhodnocení formuláře GAP analýzy je stanovena legenda symbolů popsaných v tabulce 1:

Tabulka 1 - Legenda symbolů GAP analýzy

SLOUPEC	**ZNA**	**VÝZNAM**
SOUHLAS (S)	--	požadavek není vyhodnocen nebo není aktuálně evidován
	N	nezavedeno žádné opatření
	C	částečně zavedeno opatření
	Z	opatření již zavedeno
	NA	nelze opatření aplikovat
ŘEŠENÍ (Ř)		uveden krátký a výstižný popis řešení v souvislosti s hodnotou uvedenou ve sloupci SOUHLAS, nezaměňovat s cílovým řešením
POZNÁMKA (P)		výstižná poznámka, případně doplňující informace
	ZD	zákonný důvod
	OZ	oprávněný zájem

Zdroj: vlastní zpracování, 2018

4.3 Stav ICT

Střední škola je z pohledu informačních technologií vybavena spíše průměrně. Především díky velké různorodosti a stáří jednotlivých zařízení. Z pohledu softwareového vybavení je situace na lepší úrovni, a to zejména díky licenční politice firmy Microsoft vůči školním zařízením. Na všech počítačích, stolních nebo přenosných je instalován operační systém Microsoft Windows minimálně ve verzi 7. Jiný operační systém na žádném uživatelsky přístupném počítači není instalován.

Aktuálně by se dalo ICT vybavení rozdělit do čtyř logických oblastí. První popisuje hlavní síťovou infrastrukturu. Druhý zahrnuje školní systém pro výuku. Třetí pak pokrytí bezdrátovým signálem v prostředí školy nejbližšího okolí. Poslední oblast zahrnuje jednotlivé informační systémy potřebné pro chod školy.

4.3.1 Síťová a hardwareová infrastruktura

Jednou z prvních oblastí, kterou je nutno specifikovat je samotná datová infrastruktura, jak sítí, serveru tak i ostatních periferií. Z pohledu bezpečnosti jsou zde tři oblasti, které mohou představovat potencionální hrozbu. Samotná topologie vnitřní sítě pro **nestudentské využití** je tvořena optickými a metalickými kabely, soustavou menežovatelných switchů a rozdělení do virtuálních podsítí. Softwarová správa je postavena na serverovém řešení od firmy Microsoft s využitím AD a s nastavenou politikou pro tvorbu a vytváření hesel. Aktuálně je povoleno pro připojení do pevné interní sítě pouze autorizovaným zařízením, přičemž vše je zajištěno za využití AD. Povolená zařízení mají svůj jednoznačný účet v AD, a každý tento účet má pevně přidělenu IP adresu. V této virtuální síti není povoleno přiřazení IP adresy z DHCP serveru.

Pro zajištění udržování aktualizovaných operačních systémů a dalších softwarových produktů má škola definován aktualizační proces, který je plně v kompetenci interního správce ICT. Součásti ochrany a bezpečnosti je také antivirové řešení pro každé jednotlivé zařízení včetně serverů.

4.3.1.1 Emailová komunikace

Každý uživatel má při založení svého uživatelského účtu v lokální síti přiřazen emailový účet, který je provozován pomocí platformy Microsoft Office 365. Zároveň je povolen antispamový filtr pro daný účet. Antivirová kontrola poštovních zpráv je aktuálně řešena přímo na jednotlivých stanicích pomocí lokálně instalované antivirové ochrany.

4.3.1.2 Přístup do internetu

V přístupu k webovým stránkám je ve škole nastaveno relativně benevolentní prostředí. Lze používat aktuálně dostupné prohlížeče, pouze jsou nastaveny pravidla tak, aby docházelo k pravidelným aktualizacím a tím se mírně snížilo riziko zanesení škodlivého kódu do PC. Na vstupním firewallu je zapnut NAT, tedy systém překladu adres. Zároveň je zakázán vzdálený přístup pomocí přímého nebo routovaného připojení.

4.3.1.3 Vzdálená podpora a správa

V lokální síti v jednotlivých virtualizovaných podsítích má správce umožněn vzdálený přístup na jednotlivá PC. Pokud vznikne požadavek na vzdálený přístup z vnějšího prostředí, tak jsou aktuálně nastavena pravidla, na které vybrané stanice lze pomocí služby TeamViewer[46] přistoupit a zároveň komu je tento vzdálený přístup povolen. Jedná se primárně o přístup dodavatelů jednotlivých informačních systémů.

4.3.2 Výuka ICT

Tato skupina je z pohledu zabezpečení, evidence ukládání informací a omezení přístupu vytvořena pomocí terminálové sítě, kdy jednotlivé učebny umožňují přístup pomocí terminálového připojení na jednotlivé uživatelské účty. Vše je řízeno pomocí AD, ve které má každý student nebo jiný uživatel nastavená konkrétní práva podle definovaných pravidel. Zároveň je do jednotlivých učeben umožněn přístup pouze s pověřenou osobou, tedy vyučujícím případně jiným zodpovědným pracovníkem školy.

Pozitivním přínosem je, že pro výuku předmětu Informační a komunikační technologie byl již před více než rokem stanoven přístup a ukládání dat pomocí systému Office365. Zároveň je v bezpečnostní politice AD nastaveno, aby veškeré nově vytvořené, stažené nebo jinak potřebné soubory byly z uživatelského profilu po odhlášení odstraněny.

Tabulka 2 - GAP Analýza - Výuka ICT

GAP ANALÝZA	Výuka s ICT		Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1	server s AD	serverovna v uzamčené místnosti	--	netýká se	ZD
1.2	portál office365	cloudové řešení Microsoft pro školy	N	nutné zajistit	
2	STRUKTURA EVIDOVANÝCH DAT			Nástroje	Formát
2.1	Osobní	bod 1.2	N	portál	struktur.data
2.2	Citlivé	--	N		
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		N		ZD
3.2	Elektronicky		N		ZD

[46] Dostupné z: *TeamViewer* <https://www.teamviewer.com/cs/> [online 2018-01-20]

3.3	Jinak		N		ZD
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			Oprávnění	
4.1	PPV		N	dodatek pr.sml.	
4.2	Smluvní vztah		C		
4.3	Jiný vztah				studenti
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		C	mapa sítě	router a firewall
5.2	Listinná evidence		N		
5.3	Jiná evidence		N		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C	uživatelské jméno a heslo	aktuálně slabé heslo
6.2	Šifrování dat na paměťových médiích		N	studenti bez oprávnění připojit	
6.3	Pravidelná aktualizace operačního a antivirového systému		Z	interní metodika	
6.4	Antivirová ochrana v reálném čase		Z		
6.5	Zálohování dat		C	office365, moodle	
6.5.1		Umístění	C	osobní data studentů v Office365 moodle na lokální NAS	
6.5.2		Šifrování	C		moodle není šifrován
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				Ochrana
7.1	Vlastní server		N	Ano	
7.1.1		Zabezpečení	C	MS AD	
7.1.2		Šifrování	N		
7.2	Cloudové řešení		Z		
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	N		
7.3	Listinná forma		--		
7.3.1		Archiv	--		
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		N	bez evidence přístupu	
7.5	Vlastní úložný prostor		N	bez evidence přístupu	
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		--		
8.2	Informační aplikace		--		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			Typ	
10.1			C		

11	KONTROLA SMLUV SE ZPRACOVATELI OÚ		Typ	Perioda
11.1		--		
12	SOUČASNÉ PROCESY - GDPR		Typ	Ověřitelnost
12.1		--		

Zdroj: vlastní zpracování, 2018

4.3.2.1 Výukový systém moodle

Ve všech aktuálně vyučovaných předmětech je studentům i vyučujícím přístupný LMS systém moodle[47]. Jedná se v ČR o jeden z nejrozšířenějších systémů pro podporu výuky, především ve školách, ale je samozřejmě použitelný i v jiných oblastech.

Je umístěn na jednom z virtuálních serverů ve školní serverovně, je plně ve správě určených vyučujících a správce ICT. V současné době není stanoven žádný jednotný a závazný postup, jak s evidovanými údaji pracovat, především jakým způsobem jsou informace o studentech evidovány a jaké mají nastaveno zabezpečení.

Další výhodou respektive nevýhodou je jeho zpřístupnění z externího prostředí. Je možné se do tohoto systému přihlásit pomocí odkazu z webového portálu školy.

Shrnutí provedené GAP analýzy následuje v tabulce 3.

Tabulka 3 - GAP analýza - Výukový systém moodle

GAP ANALÝZA		Výukový systém moodle	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1	Moodle	lokální server	N		
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní	Jméno a příjmení	N		ZD
		heslo	N		ZD
2.2	Citlivé	--	--		
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		--		
3.2	Elektronicky		--		
3.3	Jinak				ZD
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		N	dodatek pr.sml.	
4.2	Smluvní vztah		C		
4.3	Jiný vztah		--		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		N	webový portál	
5.2	Listinná evidence		--		

[47] Dostupné z: *Moodle* <https://moodle.org/> [online 2018-01-20]

5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C	jméno a heslo	bez https
6.2	Šifrování dat na paměťových médiích		--		
6.3	Pravidelná aktualizace operačního a antivirového systému		Z		
6.4	Antivirová ochrana v reálném čase		--		
6.5	Zálohování dat		C		
6.5.1		Umístění	C	lokální, NAS	
6.5.2		Šifrování	N		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		Z	Ano	virtuální server
7.1.1		Zabezpečení	Z	MS AD	Ano
7.1.2		Šifrování	Z		Ano
7.2	Cloudové řešení		--		
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	--		
7.3	Listinná forma		--		
7.3.1		Archiv			
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		--		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		--		
8.2	Informační aplikace		--		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1	--		N	vlastní správa	
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1	Licence GNU, vydávaná Free Software Foundation		N		1 x ročně
12	SOUČASNÉ PROCESY - GDPR			TYP	OVĚŘITELNOST
12.1	--		N		

Zdroj: vlastní zpracování, 2018

Jak je možné v uvedené analýze zjistit, pro výuku pomocí systému moodle je kritické nezabezpečené a nešifrované připojení k studijním informacím, které obsahují osobní údaje.

4.3.3 Školní veřejná síť

V současné době je pro zjednodušení přístupu do internetu umožněno připojení pomocí bezdrátového pokrytí prostor školy a nejbližšího okolí. Tento způsob je dán historicky a pravděpodobně je jedním z benefitů pro studenty. Aktuálně je nastaveno přihlašování do této bezdrátové sítě pomocí jedinečných uživatelských jmen a hesel a zároveň je tato

bezdrátová síť vyčleněna z ostatních provozních datových sítí, je vytvořena speciální VLAN, která umožní pouze přístup k internetu. Toto je postaveno na technologických zařízeních pořízených a konfigurovaných před více než 6 lety. Dalším bezpečnostním prvkem je časové omezení přihlášeného uživatele na stanovenou dobu. Po jejím uplynutí je daný uživatel odhlášen.

Aktuálně není žádným systematickým způsobem evidován přístup jednotlivých zařízení do této bezdrátové sítě. Taktéž není žádným systémem nastaven způsob omezení připojení jakéhokoliv zařízení do bezdrátové sítě, a omezení je, jak bylo uvedeno výše, pouze znalost přihlašovacích údajů.

Tabulka 4 - Gap analýza - Školní veřejná síť

GAP ANALÝZA	Školní veřejná síť		Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1	WIFI účty	serverovna	N		
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní	jméno a heslo	N	router, wifi	strukturovaná data
2.2	Citlivé	--			
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		N		
3.2	Elektronicky		N		
3.3	Jinak		--		
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		C	dodatek pr.sml.	
4.2	Smluvní vztah		C		
4.3	Jiný vztah		--		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		C	router, firewall	
5.2	Listinná evidence		--		
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C	virtuální LAN	
6.2	Šifrování dat na paměťových médiích		N		
6.3	Pravidelná aktualizace operačního a antivirového systému		--		
6.4	Antivirová ochrana v reálném čase		--		
6.5	Zálohování dat		--		
6.5.1		Umístění	--		
6.5.2		Šifrování	--		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		--		
7.1.1		Zabezpečení	--		
7.1.2		Šifrování	--		
7.2	Cloudové řešení		--		

7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	--		
7.3	Listinná forma		--		
7.3.1		Archiv	---		
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		--		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		--		
8.2	Informační aplikace		--		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1			--		
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			--		
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1			--		

Zdroj: vlastní zpracování, 2018

Z uvedené analýzy se veřejně přístupná bezdrátová síť jeví jako velmi zásadní riziko, a to nejen z pohledu GDPR, ale i z bezpečnosti elektronických informací v prostředí školy. Jak bylo zmíněno výše, jediné 2 bezpečnostní opatření jsou postavena na relativně starých síťových prvcích.

4.3.4 Informační systémy

Oblast informačních systémů pro evidenci provozních i školních agend se skládá z několika od sebe absolutně odlišných systémů.

4.3.4.1 ERP

Ekonomický informační systém je umístěn v lokální síti s daty uloženými na lokálním úložišti. Pro veškerou činnost spojenou s ekonomickými agendami je určeno přímo ekonomické oddělení. Protože se jedná o zaměstnance, je z pohledu Obecného nařízení situace jednodušší, protože se na ně vztahují jednotně nastavené pravidla a procesy. Z pohledu Obecného nařízení se toto oddělení přímo účastní zpracování osobních údajů, a to jak studentů, absolventů školy, zaměstnanců i externích subjektů. Navíc zde do zpracování

osobních údajů vstupuje skupina zákonných zástupců současných, případně potencionálních studentů.

Výsledky získané GAP analýzou v prostředí školy, ke kterým v běžném režimu dochází, jsou přehledně shrnuty v tabulce 5.

Tabulka 5 - GAP analýza ERP

GAP ANALÝZA		ERP	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1	ERP ALEF		N		ZD
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní	STUDENTI, ZÁKONNÍ ZÁSTUPCI	C		
		KONTAKTY NA AKCÍCH	N		
2.2	Citlivé	STUDENTI	C		
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		C		
3.2	Elektronicky		C		
3.3	Jinak		--		
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		N	dodatek pr.sml.	
4.2	Smluvní vztah		C		
4.3	Jiný vztah		--		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		C	SERVER	
5.2	Listinná evidence		C	ARCHIV	
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C		
6.2	Šifrování dat na paměťových médiích		C		
6.3	Pravidelná aktualizace operačního a antivirového systému		C	SMĚRNICE NOVÁ VERZE	
6.4	Antivirová ochrana v reálném čase		A		
6.5	Zálohování dat		A		
6.5.1		Umístění	C		
6.5.2		Šifrování	C		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		C		
7.1.1		Zabezpečení	C		
7.1.2		Šifrování	N		
7.2	Cloudové řešení		--		
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	--		
7.3	Listinná forma		C		
7.3.1		Archiv	C		

7.3.2		Bezpečnost a evidence přístupu	N	BEZ SMĚRNICE O EVIDENCI, BEZ ZABEZPEČENÍ	
7.4	Šanon v kanceláři		C		
7.5	Vlastní úložný prostor		C		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		--		
8.2	Informační aplikace		--		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		C		
9.1.1		Způsob odhlášení z evidence	N		
9.2	Elektronická forma akcí		C		
9.2.1		Způsob odhlášení z evidence	N		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1			C	DODAVATEL ERP	
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			C	PPV	
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1			N		

Zdroj: vlastní zpracování, 2018

4.3.4.2 Evidence studia

Pro sledování informací o studentech, výuce a známkách je provozován hybridní systém Bakalář. Aktuálně je tento systém instalován na vyhrazeném serveru. Data jsou plně pod správou školního správce. Zároveň však k tomuto systému existuje externí přístup pomocí rozhraní poskytovatele tohoto systému a tím je v současné době umožněno přistupovat k datům a informacím o studentech a výuce i z prostředí mimo školní síť, respektive přímo z internetu. Základní správu systému Bakaláři má v gesci vyčleněný člen učitelského sboru, který zajišťuje pořízení základních dat, konfiguraci a případné řešení problémů. Také je pověřen kontrolou aktualizací systému a archivací dat. Samotnou hlavní evidenční činnost mají jednotliví učitelé, kteří v systému evidují veškeré studijní informace.

GAP analýzou byly zjištěny parametry aktuálního stavu zpracování, ty jsou uvedeny v tabulce 6.

Tabulka 6 - GAP analýza evidence studia Bakaláři

GAP ANALÝZA		Evidence studia Bakaláři	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1	Bakaláři	lokální server	N	ZD	
1.2	Bakaláři web	datové úložiště poskytovatele služby	C	smluvní ošetření zpracování dat	
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní	veškeré osobní údaje studentů	C	písemný souhlas + ZD	
		základní osobní údaje učitelů	C	písemný souhlas + ZD	
2.2	Citlivé	údaje studentů se speciálními vzdělávacími potřebami	C	písemný souhlas + ZD	
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		C	formulář při žádosti o přijetí, změny údajů	
3.2	Elektronicky		--		
3.3	Jinak		--		
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		C	dodatek pr.sml.	
4.2	Smluvní vztah		C		
4.3	Jiný vztah		N		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		C	standardní zabezpečení	
5.2	Listinná evidence		C	zamykatelná místnost	
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C	2 úrovně přístupových údajů	
6.2	Šifrování dat na paměťových médiích		N		
6.3	Pravidelná aktualizace operačního a antivirového systému		C	SMĚRNICE NOVÁ VERZE	
6.4	Antivirová ochrana v reálném čase		C		
6.5	Zálohování dat		C	centrální	
6.5.1		Umístění	C	server	
6.5.2		Šifrování	N		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		C		MS AD
7.1.1		Zabezpečení	C		jméno a heslo, bezpečnostní politika
7.1.2		Šifrování	NA		
7.2	Cloudové řešení		C	Smluvní vztah	
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	C	Smluvní vztah	

7.3	Listinná forma		C		
7.3.1		Archiv	C		
7.3.2		Bezpečnost a evidence přístupu	N		
7.4	Šanon v kanceláři		N		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		N	nutná změna obsahu webu	
8.2	Informační aplikace		--		
8.3	Tiskoviny		N	doplnit informace	
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1	Smlouva o podpoře IS Bakaláři, zajištění webového přístupu		C	roční	zajistit revizi
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			--		
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1	evidence osobních a citlivých údajů		N	není procesní diagram	doplnit procesní diagram včetně logování informací

Zdroj: vlastní zpracování, 2018

4.3.4.3 Docházkový systém

Docházkový systém ve škole slouží jak pro evidenci příchodů, tak také jako zařízení pro řízení vstupu. Je využíván všemi pracovníky školy a zároveň i všemi studenty. Systém pomocí elektronického čipu jednoznačně identifikuje danou osobu, samozřejmě za předpokladu, že tyto čipy nejsou mezi osobami vyměňovány. Tento systém je další, ve kterém jsou evidovány osobní údaje. Agenda docházky je propojena s uživatelskými účty v AD a zároveň jsou pro jeho činnost vytvářeny záznamy v databázi, umístěné na serveru v lokální síti a spravované školním správcem. GAP analýzu docházkového systému zobrazuje tabulka 7.

Tabulka 7 - GAP analýza docházkového systému

GAP ANALÝZA		Docházkový systém	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1		Z-WARE	C	AKTUALIZACE SW, REVIZE SMLUV	
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní		N		
2.2	Citlivé		NA		
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		C	aktualizace při platbě zálohy	
3.2	Elektronicky		N		
3.3	Jinak		NA		
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		C	dodatek pr.sml.	
4.2	Smluvní vztah		C		
4.3	Jiný vztah		--		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		C		
5.2	Listinná evidence		NA		
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C		
6.2	Šifrování dat na paměťových médiích		N		
6.3	Pravidelná aktualizace operačního a antivirového systému		--		
6.4	Antivirová ochrana v reálném čase		--		
6.5	Zálohování dat		N		
6.5.1		Umístění	N		
6.5.2		Šifrování	N		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		C		
7.1.1		Zabezpečení	C		
7.1.2		Šifrování	N		
7.2	Cloudové řešení		--		
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	--		
7.3	Listinná forma		--		
7.3.1		Archiv	--		
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		--		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		N	přístup z portálu, není ošetřeno	
8.2	Informační aplikace		NA		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				

9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1			N	správce portálu	správce možných OU
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			C	doplnit a aktualizovat	
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1			--		

Zdroj: vlastní zpracování, 2018

4.3.4.4 Stravovací systém

S docházkovým systémem je plně provázán i stravovací systém, který umožní vést na úrovni školy veškerou evidenci o stravování. Zároveň slouží pro jednotlivé uživatele jako systém pro volbu a odhlašování jídla. Samotná datová evidence využívá i agendu pro evidenci zaplacených obědů, plateb nebo vracení nevyčerpaných záloh na stravování. Tak jako docházkový systém základní identifikační údaje čerpá z AD na školním serveru. Získané údaje z GAP analýzy zobrazuje tabulka 8.

Tabulka 8 - GAP analýza stravovacího systému

GAP ANALÝZA	Stravovací systém	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT			
1.1	SYSTÉM Z-WARE	C	AKTUALIZACE SW, REVIZE SMLUV	
2	STRUKTURA EVIDOVANÝCH DAT		NÁSTROJE	FORMÁT
2.1	Osobní	N		
2.2	Citlivé	NA		
3	FORMA ZÍSKÁNÍ SOUHLASU			
3.1	Písemně	C	aktualizace při platbě zálohy	
3.2	Elektronicky	N		
3.3	Jinak	NA		
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM		OPRÁVNĚNÍ	
4.1	PPV	C	dodatek pr.sml.	
4.2	Smluvní vztah	C		
4.3	Jiný vztah	--		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT			
5.1	Elektronická evidence	C		

5.2	Listinná evidence		NA		
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C		
6.2	Šifrování dat na paměťových médiích		N		
6.3	Pravidelná aktualizace operačního a antivirového systému		--		
6.4	Antivirová ochrana v reálném čase		--		
6.5	Zálohování dat		N		
6.5.1		Umístění	N		
6.5.2		Šifrování	N		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		C		
7.1.1		Zabezpečení	C		
7.1.2		Šifrování	N		
7.2	Cloudové řešení		--		
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	--		
7.3	Listinná forma		--		
7.3.1		Archiv	--		
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		--		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		N	přístup z portálu, není ošetřeno	
8.2	Informační aplikace		NA		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1			N	správce portálu	správce možných OU
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			C	doplnit a aktualizovat	
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1			--		

Zdroj: vlastní zpracování, 2018

4.3.4.5 Kamerový systém

V prostředí školy je v současné době z bezpečnostního hlediska instalován kamerový systémem. Ten je však určen pouze pro identifikace příchozích osob bez archivace video záznamu. Zároveň není video signál připojen na specializovaný dohledový pult, ale pouze na

monitor spojený se vstupním systémem. Z tohoto pohledu tedy nejsou zásadní požadavky v souvislosti s Obecným nařízením. Přesto pro tento systém byla zpracována GAP analýza současného stavu. Z pohledu budoucích možných využití je důležité mít tento systém zmapován, tak aby jej bylo v případě potřeby možné nastavit i do režimu ukládání obrazového záznamu. Aktuální stav popisuje tabulka 9.

Tabulka 9 - GAP analýza kamerového systému

GAP ANALÝZA		Kamerový systém	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1	--	obrazový záznam není pořizován	--		
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní	obrazový záznam není pořizován	--		
2.2	Citlivé	obrazový záznam není pořizován	--		
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		N	informační cedule	doplnit do školního řádu
3.2	Elektronicky		--		
3.3	Jinak		--		
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		--	dodatek pr.sml.	
4.2	Smluvní vztah		--		
4.3	Jiný vztah		--		
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		C	Firewall, přístupová práva	
5.2	Listinná evidence		--		
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C	2 úrovně přihlašování	
6.2	Šifrování dat na paměťových médiích		N	--	
6.3	Pravidelná aktualizace operačního a antivirového systému		Z	automatické	
6.4	Antivirová ochrana v reálném čase		Z	automatické	
6.5	Zálohování dat		--		
6.5.1		Umístění	--		
6.5.2		Šifrování	--		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		--		
7.1.1		Zabezpečení	--		
7.1.2		Šifrování	--		
7.2	Cloudové řešení		--		
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	--		

7.3	Listinná forma		--		
7.3.1		Archiv	--		
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		--		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		C	nutné doplnit informace	
8.2	Informační aplikace		--		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		
9.2	Elektronická forma akcí		--		
9.2.1		Způsob odhlášení z evidence	--		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1			C	dodavatel kamer. systému	
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			--		
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1			--		

Zdroj: vlastní zpracování, 2018

4.3.5 Webový portál školy

Školní webový portál je umístěn v hostingovém centru, a smluvně se o hlavní kostru a funkcionalitu portálu stará externí organizace. Portál je definován tak, aby bylo možné do jednotlivých tematických částí doplňovat data přímo pověřenými pracovníky školy, dále umožňuje propojení s webovým rozhraním interních školních systémů, konkrétně s Bakaláři, stravovacím systémem a výukovým systémem Moodle.

Vzhledem k stavu, že tento portál je jedním z hlavních informačních zdrojů o škole, zároveň slouží jako centralizované prostředí pro přístup studentů i pedagogů k jednotlivým subagendám, byl také analyzován a získané údaje zobrazuje tabulka 10.

Tabulka 10 - GAP analýza webového portálu

GAP ANALÝZA		Webový portál školy	Souhlas	Řešení	Pozn.
1	UMÍSTĚNÍ SBĚRNÝCH UZLŮ OSOBNÍCH DAT				
1.1		portál www.hotelovkajes.cz	NA	není nástroj pro sběr OÚ	
2	STRUKTURA EVIDOVANÝCH DAT			NÁSTROJE	FORMÁT
2.1	Osobní		--		
2.2	Citlivé		--		
3	FORMA ZÍSKÁNÍ SOUHLASU				
3.1	Písemně		--		
3.2	Elektronicky		N	doplnit souhlas	
3.3	Jinak		N	vyžádání email	
4	OSOBY S PŘÍSTUPEM K OSOBNÍM ÚDAJŮM			OPRÁVNĚNÍ	
4.1	PPV		N	správce	
4.2	Smluvní vztah		C	zpracovatel	
4.3	Jiný vztah		--	--	
5	EVIDENCE MÍST S HROZÍCÍM RIZIKEM ÚNIKU DAT				
5.1	Elektronická evidence		N	webhosting a portál	
5.2	Listinná evidence		--		
5.3	Jiná evidence		--		
6	STAV ZABEZPEČENÍ ICT				
6.1	Ochrana přístupu do PC		C		
6.2	Šifrování dat na paměťových médiích		N		
6.3	Pravidelná aktualizace operačního a antivirového systému		Z		
6.4	Antivirová ochrana v reálném čase		N		
6.5	Zálohování dat		C		
6.5.1		Umístění	--		
6.5.2		Šifrování	N		
7	ULOŽENÍ DAT OBSAHUJÍCÍ OÚ A CÚ				OCHRANA
7.1	Vlastní server		N		
7.1.1		Zabezpečení	C	MS AD	
7.1.2		Šifrování	N		
7.2	Cloudové řešení		N	Ne	
7.2.1		Smluvní ošetření vztahu s poskytovatelem cloudu	N	Neověřeno	
7.3	Listinná forma		--		
7.3.1		Archiv	--		
7.3.2		Bezpečnost a evidence přístupu	--		
7.4	Šanon v kanceláři		--		
7.5	Vlastní úložný prostor		--		
8	ZVEŘEJNĚNÍ INFORMACÍ O GDPR				
8.1	Webové stránky		N		
8.2	Informační aplikace		N		
8.3	Tiskoviny		--		
9	EVIDENCE POTENCIÁLNÍ KLIENTŮ				
9.1	Písemná forma akcí		--		
9.1.1		Způsob odhlášení z evidence	--		

9.2	Elektronická forma akcí		C	webportál	anketa, dotazník
9.2.1		Způsob odhlášení z evidence	N		
10	VAZBY A SMLOUVY NA 3 STRANY			TYP	
10.1			C	správce portálu	správce možných OU
11	KONTROLA SMLUV SE ZPRACOVATELI OÚ			TYP	PERIODA
11.1			C		
12	SOUČASNÉ PROCESY – GDPR			TYP	OVĚŘITELNOST
12.1			N	nezpracovány	

Zdroj: vlastní zpracování, 2018

4.4 Vyhodnocení vstupní analýzy

Již na začátku provedení GAP analýzy bylo zřejmé, že uvedená střední škola bude muset zavést opatření, vyplývající z Obecného nařízení. Bylo stanoveno, že „Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů"[48] podle článku 37 Obecného nařízení. K tomuto rozhodnutí vedla také různorodost zjištěných dat, které v sobě nesou osobní údaje respektive citlivé údaje. Zvláště v oblasti citlivých údajů je v prostředí jakékoliv školy nutné zajistit jednoznačné a precizně evidované nakládání s těmito údaji, dále pak další v Obecném nařízení specifikované činnosti z pohledu správce i zpracovatele.

Ze získaných informací dále lze konstatovat, že cloudové technologie v současném prostředí střední školy jsou využívány spíše méně. Jejich vyššímu využití zvláště v oblasti informačních systému, jak ERP, tak i systémů pro evidenci stravy a docházky brání jejich technologické parametry, případně stav vybavenosti aktuálními verzemi uvedených informačních systémů. Jednou z hlavních příčin nevyužívání nových verzí těchto systémů jsou omezené finanční prostředky, které jsou převážně využívány na potřeby výuky a na provozní činnosti jsou spíše omezené.

Důležitou skupinou informací získaných analýzou je oblast fyzického zabezpečení veškerých informačních toků v prostředí střední školy. Jednak se jedná o zpřístupněné bezdrátové pokrytí prostor a blízkého okolí školy, dále pak o nezabezpečené a nešifrované přístupy do LMS systému moodle. Tyto fakta jsou velmi zásadní pro celkové posouzení stavu školy a jejich správné nastavení vede k celkové schopnosti školy být v souladu s Obecným nařízením.

[48] Dostupné z: *EU obecné nařízení o ochraně osobních údajů "Posouzení vlivu na ochranu osobních údajů"* <http://www.privacy-regulation.eu/cs/35.htm> [online 2018-01-12]

4.5 Nastavení procesního přístupu

Jednou z hlavních a podstatných částí analýzy aktuálního stavu v uchovávání, přístupu a poskytování osobních informací, jakožto i informací o jednotlivých činnostech studentů bylo vyspecifikovat takové procesy, ve kterých data s osobními údaji v tomto prostředí vznikají, jakým způsobem jsou ukládány, jak jsou zabezpečeny a jaké existují postupy pro jejich získání, modifikaci nebo odstranění.

Vzhledem k faktu, že střední škola není firma, tak zde procesní řízení není nastaveno na takové úrovni, že by byly jednotlivé procesy nastaveny, průběžně revidovány a aktualizovány. Dle mého názoru ale identifikování činností a jejich následné zpracování do procesních postupů může požadavky stanovené Obecným nařízením lépe dodržovat a mít nad nimi i potřebnou kontrolu.

Oblast analýzy byla rozdělena obdobně jako při popisu stavu ICT na tři oblasti, a to na oblast výuky, oblast informační a evidenční a poslední oblast se zaměřuje na přístup do internetu z neautorizovaných zařízení (mobilní telefony, tablety, notebooky).

Pro tvorbu procesních schémat, jejich validaci a modifikaci byl použit softwareový nástroj Bizagi Modeler[49] verze 3.1. Jeho výhodou je velmi intuitivní tvorba procesních schémat, dále možnost validace procesu pomocí simulace a v případě pořízení nástroje Bizagi Studio i spuštění procesu jako workflow.

4.5.1 Únik osobních dat

Protože jedna z hlavních oblastí problematiky GDPR je řešení úniku osobních dat ze **systému**, považuji proto jako jeden z prvních procesních modelů uvést právě ten, který řeší činnosti při zjištění takového incidentu. Obecně lze konstatovat, že tento proces je součástí všech dále uvedených procesních diagramů, a to buď jako jejich součást, nebo jako nadřízený proces při zjištění možného úniku informací.

Jednou z důležitých částí tohoto procesu je jednoznačná identifikace síly rizika. Tuto lze rozdělit do následujících skupin s uvedením charakteristiky pro subjekt údajů:

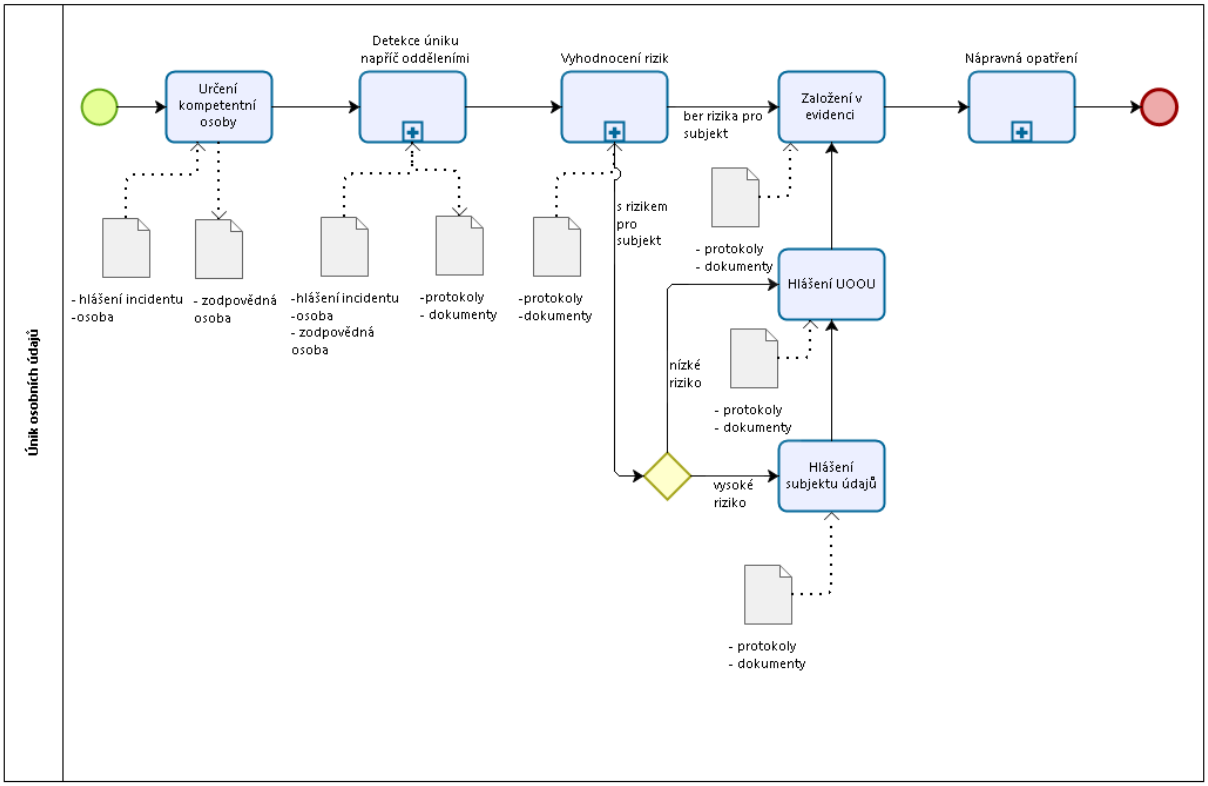
- **zanedbatelné**
    - nebude postižen vůbec či pouze minimálně s drobnými nepříjemnostmi, překonatelnými v krátkém čase a s minimální námahou,

[49] Dostupné z: *Bizagi* <https://www.bizagi.com/en/products/bpm-suite/modeler> [online 2018-01-20]

    - není nutné hlášení dozorovému orgánu,
- **nízké**
    - může se setkat s významnými nepříjemnostmi, ale ty bude schopen překonat, i za cenu mírných obtíží, například dodatečné náklady, strach, zamezení přístupu k obchodním službám,
    - je nutné hlášení dozorovému orgánu
- **střední**
    - může být postižen významnými důsledky, které je schopen překonat za zvýšeného úsilí, lze očekávat zneužití finančních prostředků, škody na majetku, umístění na černé listiny bank,
    - nutné hlásit dozorovému orgánu i subjektu údajů,
- **vysoké**
    - lze se setkat s významnými důsledky, je možné očekávat jejich dlouhodobé odstraňování,
    - nutné hlásit dozorovému orgánu i subjektu údajů,
- **kritické**
    - může se setkat s významnými nebo nezvratnými důsledky, ty nemusí být i přes veškerou snahu překonatelné,
    - nutné hlásit dozorovému orgánu i subjektu údajů.

Procesní diagram je na rozdíl od ostatních umístěn pouze v jedné oblasti, protože ta celá spadá do problematiky GDPR. Diagram je zobrazen na obrázku 3.

Obrázek 3 - Únik osobních údajů



Zdroj: vlastní zpracování, 2018

Tento procesní diagram s uvedenými riziky je vždy nutné dodržet včetně všech vstupních i výstupních činností. Při jakémkoli porušení zabezpečení osobních údajů správce ohlásí prostřednictvím DPO bez zbytečného odkladu a nejlépe do 72 hodin od zjištění úniku informací dozorovému úřadu. Jestliže nedojde k ohlášení o incidentu dozorovému úřadu do 72 hodin, tak samotné ohlášení už musí obsahovat i uvedení důvodů tohoto zpoždění.

4.5.2 Síťová infrastruktura

Samotná infrastruktura lokální počítačové sítě je v relativně akceptovatelném stavu. Z analýzy provedené na aktivních síťových zařízení je nutné zajistit pravidelnou a bezchybnou aktualizaci. Jedná se především o zařízení, uvedená v tabulce 11.

Tabulka 11 - Stav síťové infrastruktury

ZAŘÍZENÍ	STAV	DOPORUČENÍ
Firewall • PfSense	• Neaktuální verze • Chybí VPN modul	• Aktualizace systému podle nadefinovaných pravidel

ZAŘÍZENÍ	STAV	DOPORUČENÍ
	• Chybí nastavení a reportování logů	• Přidělování VPN přístupů podle nadefinovaných pravidel • Nastavení permanentního logování včetně přesunu logovacích souborů do archivu
Windows Server s DC	• Správa prováděna učiteli • Nesystematičnost v aplikacích aktualizací • Nejednotnost zálohování • Nemožnost obnovy při havárii	• Zpracovat pracovní postupy pro uvedený stav • Outsourcovat správu ICT
Aktivní síťové prvky	• Neexistující plán kontrol a revizí stavu • Neexistující strategie testování funkčnosti • Neexistuje sledování funkčnosti prvků	• Nasazení monitorovacího systému, např. Zabbix[50] • Outsourcovat správu ICT

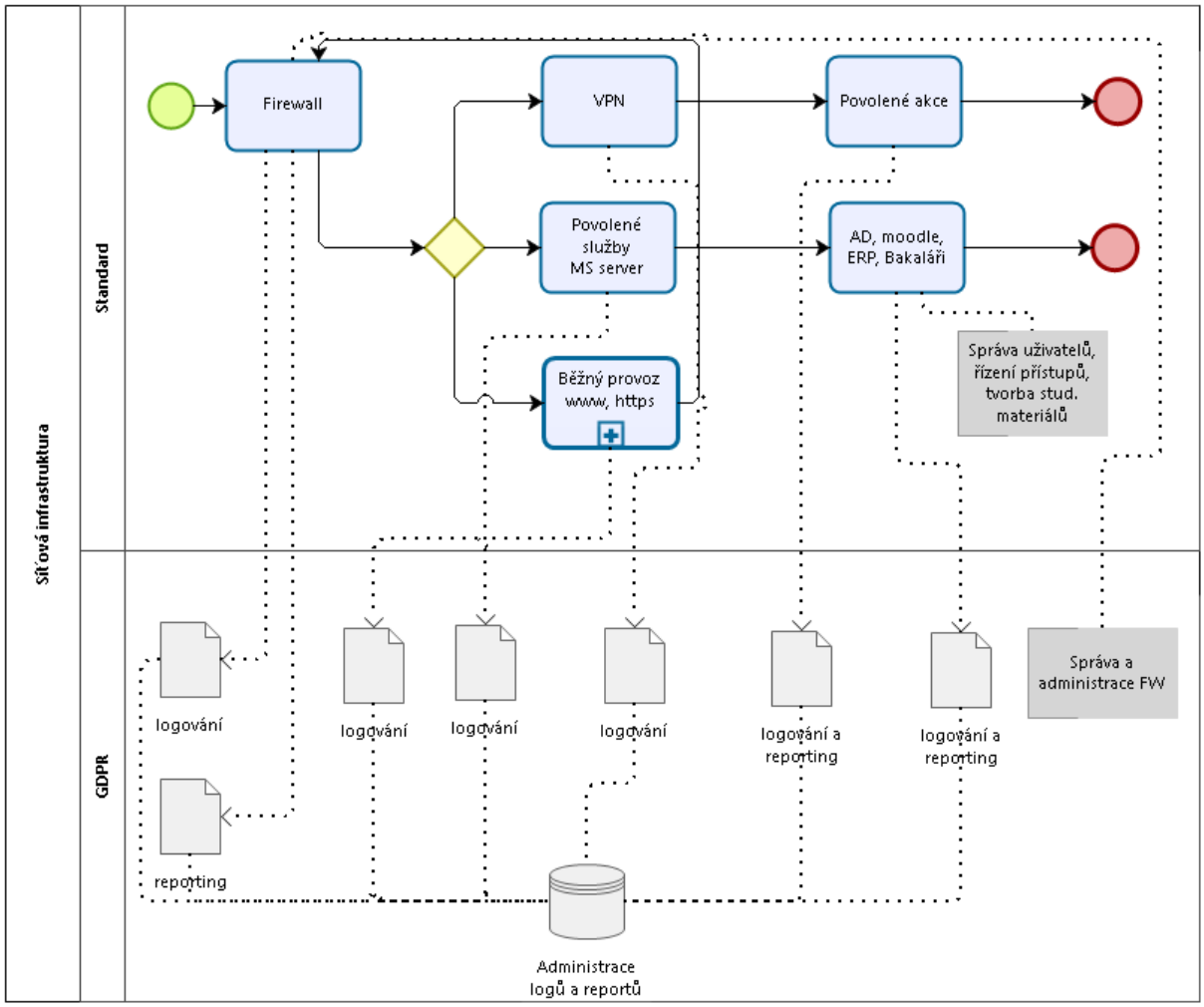
Zdroj: vlastní zpracování, 2018

Technologické vybavení odpovídá stavu a době pořízení, je však vhodné vypracovat strategii obnovy klíčových komponent nutných pro zabezpečení chodu celé lokální počítačové sítě. Procesní diagram pro správu LAN je na obrázku 4.

Podstatná činnost pro zajištění co nejvyšší spolehlivosti lokální počítačové sítě je také kromě dodržování procesního diagramu pravidelná profilaxe samotných hardwareových prvků. Pro tuto činnost je vhodné a vedení školy bylo doporučené outsourceovat správu podle definovaných pravidel a kritérií. Zároveň má vedení školy jako správce i zpracovatel osobních údajů zajištěnu odpovědnost za uvedenou oblast.

[50] Dostupné z: *Zabbix* <https://www.zabbix.com/> [online 2018-01-20]

Obrázek 4 - Procesní schéma síťové infrastruktury



Zdroj: vlastní zpracování, 2018

4.5.2.1 Emailová komunikace

V prostředí školy je aktuálně aktivně využíván systém Microsoft Office 365, který v licenci pro školní zařízení umožňuje využití emailových služeb spojených s doménovým jménem, ale v cloudovém prostředí.

Jednotliví uživatelé, ať už se jedná o personál školy, tak i o jednotlivé studenty, mají vždy při vytvoření přístupových údajů zřízen také emailový účet ve formátu prijmeni@domenaskoly.cz. Jelikož se jedná o osobní údaj uživatele, je zaevidován souhlas se zpracování osobních údajů.

Pro práci s emailovými zprávami není nastavena jednotná strategie a tak každý z uživatelů používá takového poštovního klienta, kterého je schopen si nainstalovat, případně ve formě webmailu používat.

4.5.2.2 Přístup do internetu

Pro zajištění bezpečnosti osobních údajů na jednotlivých pracovních stanicích je nutné zcela změnit přístup k nastavení práv uživatelů. Řešení je navrženo tak, aby zcela využilo vlastností doménové politiky, konkrétně nadefinování přesných pravidel přístupu, stanovení ověřených rozsahů adres a v neposlední řadě bylo nastaveno logování podezřelých činností z antivirového systému do centrální evidence incidentů.

4.5.2.3 Vzdálená podpora a správa

Vzhledem k faktu, že současný trend podpory uživatelů komerčních softwareových produktů je postaven na vzdáleném připojení, bylo zvoleno a v doménové politice pro specifikované uživatele povoleno použít tento způsob podpory. Důležitým faktorem z pohledu GDPR je jednoznačná evidence těchto vzdálených přístupů, jakož i smluvní ošetření stavu, kdy externí instituce má možnost pracovat s osobními daty.

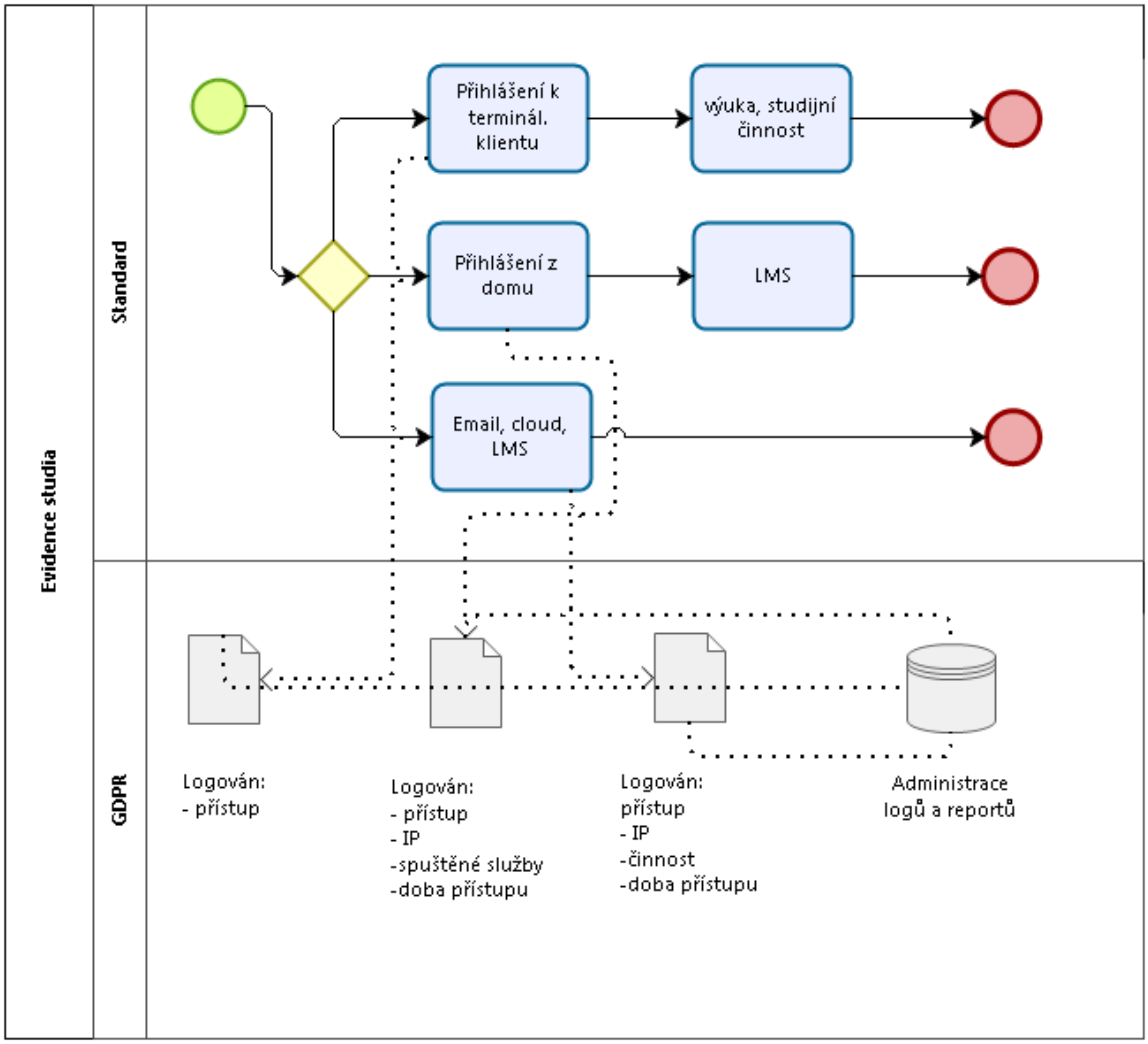
4.5.3 Výuka s ICT

Oblast výuky využívající informační technologie v sobě nese mnoho možností, jak během běžných vyučovacích hodin získat, zaevidovat případně odstranit osobní údaje. Jak bylo uvedeno v teoretické části práce, osobním údajem v oblasti výuky jsou například tyto oblasti:

- vytváření a ukládání datových souborů s nestrukturalizovanými osobními informacemi,
- informace o studijních postupech spojených s uživatelem (studentem),
- využití osobních údajů pro potřeby výuky jako např. seznamy adres, klasifikačních informací a podobně.

Pro potřeby výuky ICT byly specifikovány procesy, které využívají aktuálně zprovozněné služby v oblasti LMS – moodle, portálu Microsoft Office 365 pro školy a terminálového přístupu na lokální server ve školní počítačové síti. Procesní diagram evidence studia je na obrázku 5.

Obrázek 5 - Procesní diagram evidence studia



Zdroj: vlastní zpracování, 2018

4.5.3.1 Výuka v cloudovém prostředí

Při GAP analýze byla tato oblast vyhodnocena jako hlavní pro prozkoumání, jaký cloudový systém bude pro výuku vhodnější. Ke srovnání byly vybrány dva komplexní systémy, a to Microsoft Office 365[51] a Google Aps pro vzdělávání[52]. Oba systémy dokládají prohlášení o tom, že splňují požadavky dané nařízením GDPR.

[51]Dostupné z: *Office 365* <https://resources.office.com/ww-thankyou-GDPR-comply-infographic.html?LCID=EN> [online 2018-01-02]

[52] Dostupné z: *Google apps pro vzdělání* <https://www.google.cz/apps/intl/cs/edu/> [online 2018-01-20]

Bohužel z pohledu využitelnosti v dané střední škole jsou důležité především nákladové parametry, dále pak jednoduchost a nízká náročnost na správu. V neposlední řadě bylo kritériem také rozšířenost, respektive snaha o výuku v systému, který je ve školství v ČR **nejrozšířenější**.

Z tohoto pohledu v rozhodnutí o používání vyhrál systém společnosti Microsoft. Rozhodnutí pro jeho další užívání bylo podpořeno následujícími argumenty:

„1. Vyhledání informací s osobními údaji,

2. Zabezpečení dokumentů a e-mailů s osobními údaji,

3. Minimalizace výskytu stejných dokumentů s osobními údaji a jejich nesprávného použití,

4. Vytváření agend spojených se zajištěním výkonu práv subjektů,

5. Zajištění zařízení, ze kterého se přistupuje k osobním údajům,

6. Bezpečné ověření oprávněného uživatele[53]“.

4.5.4 Školní veřejná síť

Provedenou analýzou byly identifikovány aktuální slabá místa, která by mohla být v důsledku případné kontroly v souvislosti s Obecným nařízením rizikovým prvkem. Proto byl navržen komplexní proces pro zajištění a evidenci přístupů do dané infrastruktury.

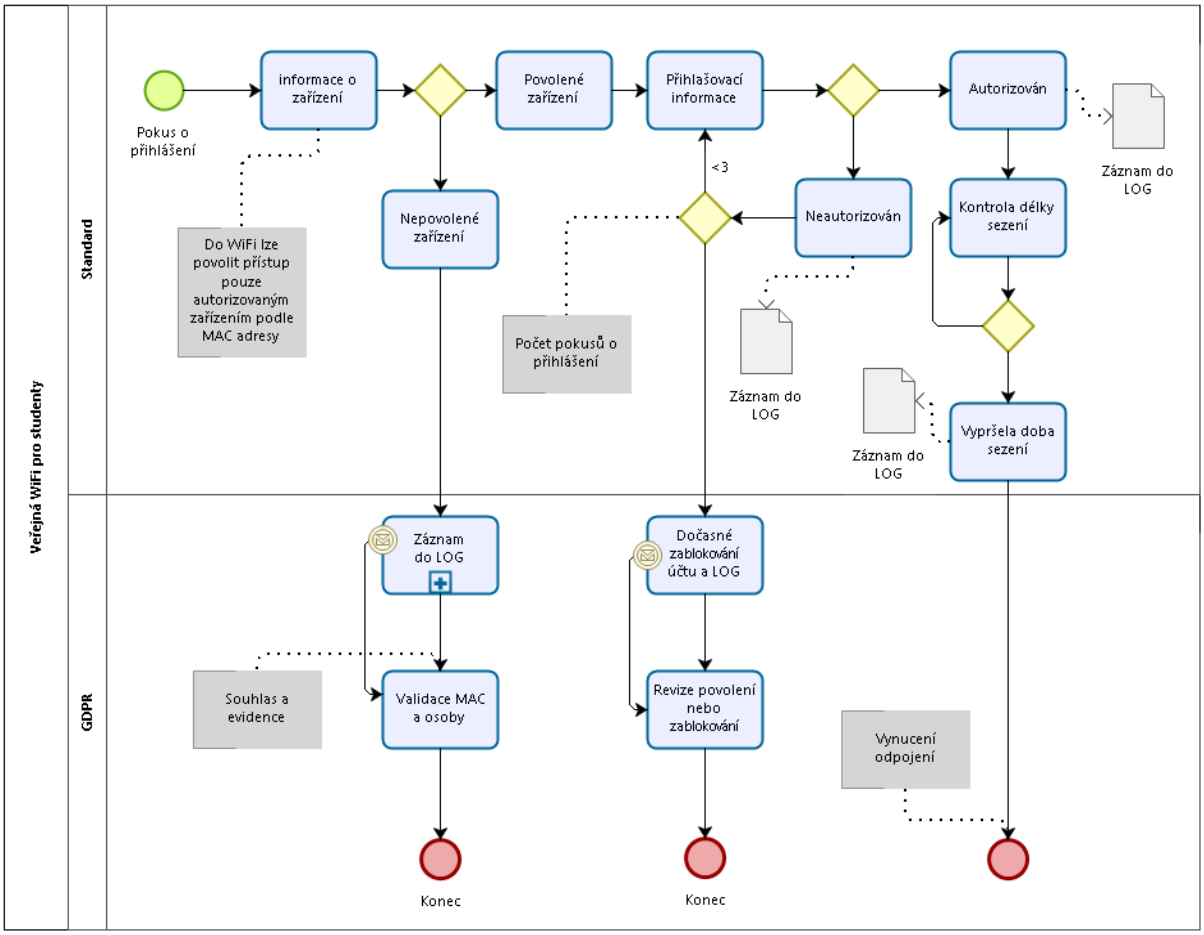
Oproti původnímu stavu došlo v procesním modelu k zásadnímu posunu v jednoznačné identifikaci připojitelných technických klientů s vazbou přímo na jednotlivé osoby. Dále bylo značně posíleno logování nutných stavů, a to tak, aby jednotlivé stavy bylo možné na vyžádání reportovat. Nově navržené procesní schéma je na obrázku 6, který zobrazuje procesy rozložené do 2 rovin. První standardní rovina zobrazuje běžně používané procesní stavy, které jsou v novém systému nastaveny. Druhá část zahrnuje oblast přímo závislou na oblasti GDPR.

Při srovnání aktuálního procesního modelu se stavem plynoucím z GAP analýzy pro Školní veřejnou síť, tak došlo k vytvoření procesní podpory k zajištění souladu s Obecným nařízením.

---

[53] Dostupné z: *S jakými požadavky GDPR pomůže Microsoft Office 365* <https://www.autocont.cz/aktuality/open space/gdpr-microsoft/office-365> [online 2018-01-20]

Obrázek 6 - Školní veřejná síť



Zdroj: vlastní zpracování, 2018

4.5.5 Pracovní postupy v oblasti informačních systémů

4.5.5.1 Ekonomický informační systém

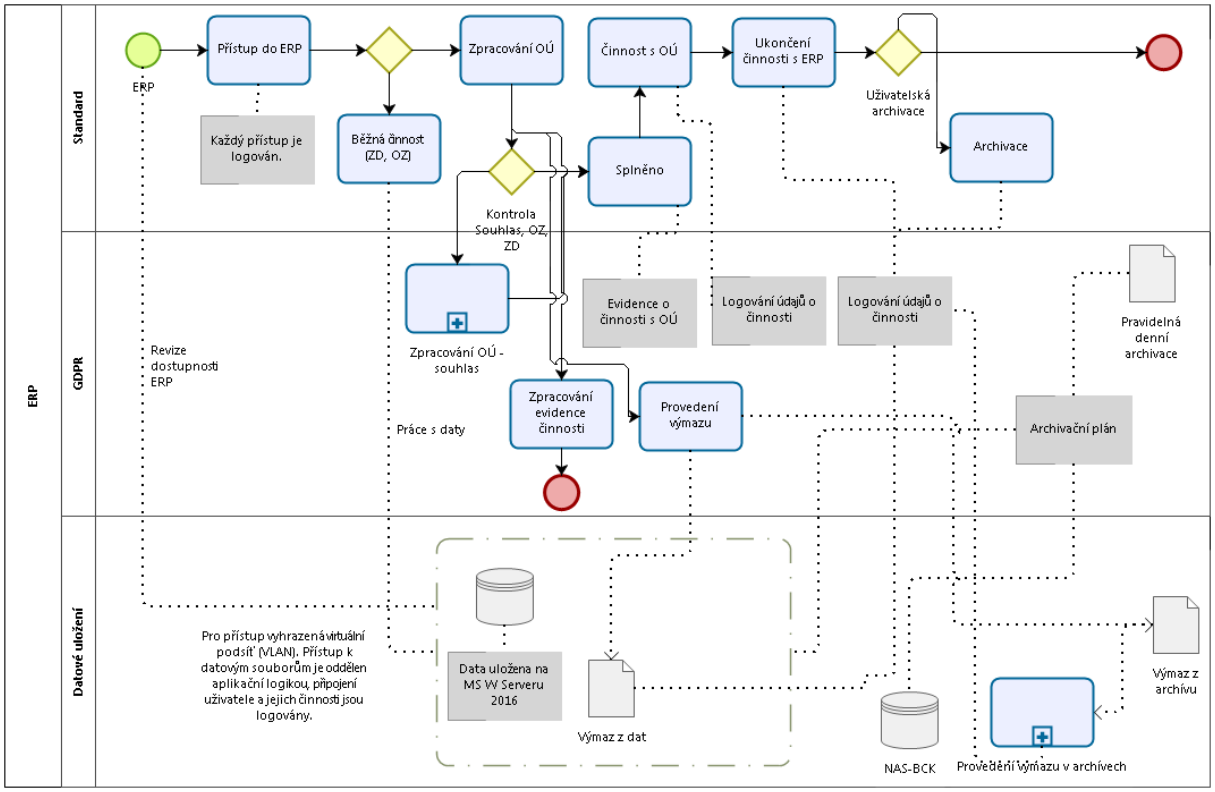
Ekonomický informační systém používaný nepedagogickými pracovníky školy aktuálně nevyužívá žádné cloudové zdroje, je to systém, který je navržen pro využití v lokálních sítích a vzdálený přístup k datům přímo pomocí klientské aplikace není umožněn. Z tohoto důvodu lze konstatovat, že pro zajištění požadavků daných Obecným nařízením bude nutné využít pouze interní procesy a systémy pro evidenci a zabezpečení.

Protože škola je v oblasti ERP systému zároveň zpracovatel OÚ, je nutné na získané výsledky nastavit procesní řešení, které popisuje nutné činnosti, a jeho základní schéma je na obrázku 7.

ERP systém je konfigurován tak, že pro přihlášení do něj je využita autentizace pomocí AD v systému Windows Server. Tím jsou zajištěny jednotné pravidla pro složitost i obměnu přístupových údajů.

Jelikož dodavatele ERP neumožňuje datové soubory v reálném čase na disku šifrovat, bylo připojení informačnímu systému zajištěno pomocí vyhrazeních virtuálních podsítí, které mají povoleno přistoupit k datovým souborů. Šifrování na tomto připojení není, vzhledem k dalším pasivním bezpečnostním pravidlům lze považovat zabezpečení za dostatečné.

Obrázek 7 - ERP procesní diagram



Zdroj: vlastní zpracování, 2018

4.5.5.2 Evidence studia - IS Bakaláři

Aktuálně je systém Bakaláři využíván pro všechny pro střední školu potřebné evidenční oblasti. Z toho důvodu je nutné tento systém brát jako klíčový a v něm zavedené postupy a probíhající procesy budou nejvíce postiženy dopadem Obecného nařízení. Zároveň z tohoto důvodu plyne nutnost maximální pečlivosti při zjištění stavu a návrhu nových procesů.

Vedení školy se rozhodlo data ukládat na úložiště v rámci interní počítačové sítě, ale zároveň zajistilo vytvoření přístupu pro připojení uživatelů pomocí webového rozhraní z internetu. Externí přístup je realizován pomocí zabezpečeného protokolu funkcionalitou dodávanou přímo výrobcem tohoto IS, a tedy v tomto režimu je škola přímo závislá na způsobu a realizaci daném výrobcem. Jedná se zprostředkování dat pomocí webové služby

umístěné na serveru v lokální síti školy. Tento způsob zprostředkování dat z pohledu bezpečnosti vyžaduje zvýšené požadavky na technické vybavení.

Proto se GDPR týkají procesy, které mají vliv na data uložená lokálně. Jedná se o tyto agendy:

- evidence osobních údajů studentů,
- evidence zodpovědných zástupců studentů,
- evidence studijních výsledků studentů,
- evidence výuky,
- evidence docházky, třídní kniha,
- rozvrhy a evidence učitelů.

Aby bylo možné detailně zpracovávat jednotlivé agendy v roli správce i zpracovatele osobních údajů, je nutné zajistit plně aktualizovanou verzi informačního systému. Z GAP analýzy vyplynulo, že v této činnosti je nutno získat plnou podporu výrobce, včetně deklarace splnění požadavků GDPR. Aktuální stav podle informací webového portálu www.bakalari.cz je takový, že výrobce intenzivně zpracovává známé požadavky z Obecného nařízení, zároveň ale stále očekává stav, kdy bude […] „doplněno českým adaptačním zákonem o zpracování osobních údajů, který je aktuálně v legislativním procesu[54]“.

Zároveň je nutné tyto aktualizace podpořit zajištěním doporučených konfiguračních parametrů, zejména pak zavedení využívání komunikačního šifrované protokolu HTTPS společně s platným certifikátem. Tuto realizaci musí škola zavést.

Pozitivním stavem je již využívání SQL serveru pro datové úložiště, kdy tento databázový nástroj je na instalován na jednom ze serverů ve škole. Dle GAP analýzy ještě plynou úkoly pro komplexní soulad s GDPR, a to v rámci šifrování dat, archivace dat a zabezpečení samotného serveru.

4.5.5.3 Docházkový a stravovací systém

Vzhledem ke stavu, že výrobce a dodavatel obou těchto systémů je jedna společnost, pak lze jednoznačně stanovit nutné požadavky na zajištění souladu s GDPR. Výhodou se také jeví fakt, že systémy jsou navrženy tak, aby přímo přebíraly údaje o jednotlivých osobách přímo z AD serveru, který je plně pod správou školy.

[54] Dostupné z: *Základní informace* <http://bakalari.cz/Static/GDPR/informace> [online 2018-01-20]

Zásadní požadavek na změnu, která je z pohledu zabezpečení nutná, je zajistit pro modul objednávání stravy komunikaci pomocí protokolu HTTPS, který prozatím nebyl implementován. Po splnění tohoto požadavku již oba systémy budou v souladu s GDPR a pouze bude nutné zajistit dodržování pravidel bezpečnosti uživateli, kteří k osobním údajům v těchto evidencích mají přístup.

4.5.5.4 Kamerový systém

Jak plyne z GAP analýzy kamerového systému, je tento v případě, že nebude využit k záznamu obrazového signálu, po splnění bodů z části řešení schopný provozu. Nutné je doplnění veškerých informačních povinností. Neméně důležité je nastavení takové doménové politiky, aby bylo jednoznačně prokazatelné, že k záznamu obrazového signálu nedochází.

4.5.5.5 Webový portál školy

Webový portál školy je specifikován tak, aby nebyl nástrojem pro sběr ani evidenci osobních údajů. Přesto ale podle návrhu řešení z provedené GAP analýzy plyne, že pro určité specifické akce je nutné doplnění informací o souladu s GDPR. Jedná se především o samotnou informaci o stavu GDPR, dále pak o doplnění možnosti zadat osobní údaje pouze se specifikovaným souhlasem vyjádřeným elektronickou formou.

Další část, kterou je nutné zajistit, jsou smluvní podmínky organizací, které webový portál administrují nebo u kterých jsou umístěny datové soubory[55].

4.6 Workflow

Pro zjednodušení a zkvalitnění průběžné práce s procesy bylo ve škole zahájeno poptávkové řízení na výběr elektronického systému pro realizaci workflow nad nově definovanými procesy. V současné době je interně testován cloudový systém Procesoid[56], vytvořený pro potřeby evidence a sledování realizace procesů.

---

[55] Dostupné z: *How To Prepare Your School For The GDPR* <https://www.finalsite.com/blog/p/~post/how-to-prepare-your-school-for-the-gdpr-8112017> [online 2018-01-20]

[56] Dostupné z: *Procesoid* <https://procesoid.com/cesko/> [online 2018-01-02]

Podle aktuálních možností dané školy je také možné zvolit řízení workflow přímo v informačním systému, pokud jej jako součást obsahuje, ale to pro uvedenou střední školu aktuálně není realizovatelné, protože používaný informační systém tuto funkcionalitu zatím nenabízí.

5 Výsledky a diskuze

V této práci bylo pomocí GAP analýzy zmapováno prostředí střední školy v kontextu jejího připravení na zajištění evidence osobních údajů v souladu s Obecným nařízením. Byly stanoveny jednotlivé klíčové oblasti, v jejich evidenční náplni byly zjištěny aktuální možnosti a stavy evidence osobních a citlivých údajů. Zároveň na tuto školu bylo nahlíženo v součinnosti s platnou legislativou, metodickým pokynem Ministerstva školství, mládeže a tělovýchovy k problematice GDPR, dále pak porovnáním známých skutečností z informačních zdrojů Úřadu pro ochranu osobních údajů. Velmi důležitou informační databází je pro jakékoliv realizace GDPR skupina WP 29, která je zřízena jako poradní orgán Evropské komise pro otázky ochrany osobních údajů.

Při jednotlivých GAP analýzách bylo možné často evidovat stav, který není zcela nepoužitelný. Tato skutečnost plyne z existence zákona č. 101/2000 Sb., o ochraně osobních údajů, který je ve svém platném znění na vysoké úrovni a protože zkoumaná střední škola je zřízena Olomouckým krajem, tak je možné konstatovat, že zde nejsou jednoznačně prokazatelné porušení uvedeného zákona.

Na druhou stranu je nutné konstatovat, že zvláště ve vybavenosti informačními technologiemi v souvislosti s potřebou důkladné evidence získaných potřebných dat, nově vzniklými definicemi pojmů, činností a procesů v souvislosti s GDPR je nutné v co nejkratší možné době zajistit aktualizace využívaných informačních systémů. Další nutnou činností je zavést jednoznačný a prokazatelný evidenční režim, ve kterém budou ukládány potřebné údaje, které budou v co nejvíce možné míře generovány navrženými procesy.

Při samotném vyhodnocování zpracovaných GAP analýz bylo vyvinuto zvýšené úsilí na jasnou identifikaci možných rizikových činností. Z tohoto pohledu je nutné věnovat pozornost pravidelně se opakujícím činnostem, zvláště v oblasti aktualizací operačních systémů, antivirových systémů a také jednotlivých informačních a evidenčních systémů.

Protože jedním z aktuálně možných řešení je využití cloud computingu, bylo prověřeno u všech zkoumaných systémů jejich možné kooperování s takovýmto systémem. Informační systémy používané v této škole v současné konfiguraci a verzi je potřeba uvést do souladu s GDPR, zajistit jednoznačné potvrzení výrobce a splnit doporučené postupy nastavení. Je ale nutné zmínit, že aktuální využití cloudových úložišť pro data těchto systému jsou v současné situaci neaplikovatelné. Hlavním důvodem je u ERP systému jeho nemožnost takto data uchovávat. A jelikož by se jednalo o více různých úložišť a s tím spojené vyšší nároky na správu, je vhodnější netříštit síly a soustředit se na jeden systém. Zároveň je ale potřeba

konstatovat, že v případě uvolnění nových verzí podporujících uložení dat v cloudových úložištích lze dané oblasti reanalyzovat a zvážit možné změny.

Proto se Cloud computing aktuálně využívá pouze pro výukové účely a také pro umístění poštovních účtů.

6 Závěr

Hlavním cílem této diplomové práce bylo analyzovat aktuální stav v oblasti zpracování osobních a citlivých údajů na vybrané střední škole podle oblastí definovaných aktuálním Nařízením Evropského parlamentu a Rady (EU) 2016/679. Zároveň bylo stanoveno na zpracovaných GAP analýzách vypracovat nové procesní postupy a ty uvést do reálného stavu ve školním prostředí.

Pro zpracování dílčích cílů bylo nutné nadefinovat základní kritéria, podle kterých byla pomocí GAP analýzy stanovena současná situace v předem určených logických oblastech. Jedná se o okruhy činností, ve kterých dochází k základním operacím s osobními údaji nebo o okruhy, které mohou zapříčinit únik osobních údajů.

Dalším dílčím cílem bylo vyhodnotit vhodnost cloudového prostředí pro zajištění souladu ve zpracování osobních údajů podle GDPR. Zároveň bylo také nutné zvolit cloudový systém, který by byl vhodný jako podpůrný nástroj pro výuku, případně pro uložení datových struktur v jednotlivých informačních systémech školy. Výsledek zjištěných informací zcela nenaplnil úvodní očekávání, ve kterém byla snaha cloudové uložiště využít i pro data z ERP systému, případně i o veškeré informace o studiu studentů na střední škole. Vzhledem k omezeným finančním možnostem zkoumané střední školy není možné aktuálně změnit informační systém za takový, který by byl schopen své datové soubory ukládat v cloudu, čímž by došlo k přenesení určitých odpovědností na zpracovatele. Proto byl Cloud computing použit pouze pro studijní potřeby a pro poštovní služby. Pro vybraný systém hovoří jeho dlouhodobé používání ve škole a zároveň i vstřícná prodejní politika pomocí systému Microsoft Select.

Na základě zpracovaných GAP analýz byly pro určené oblasti vypracovány zcela nové procesní diagramy. Vzhledem k faktu, že střední škola procesní řízení jako takové zatím nepoužívala, bylo nutné tyto procesy definovat jako komplexní řešení a zároveň k němu bylo zahájeno výběrové řízení pro softwareovou podporu workflow, tedy pro nástroj, který je schopen jednoznačně přidělovat, sledovat, vyhodnocovat, logovat a připomínat postupně vynikající úkoly jednotlivým oprávněným osobám.

Důležitou součástí celého zpracování bylo nastavení pravidel pro průběžné evidování činností, které mohou ovlivňovat osobní údaje.

Takto nastavené procesní řízení včetně zpracované analýzy lze považovat za model, podle kterého je možné zpracovat obdobné školy, případně jiné organizace s podobným charakterem činností.

7 Seznam použitých zdrojů

7.1 Internetové zdroje

Autocont. S jakými požadavky GDPR pomůže Microsoft Office 365 [online]. 2018 [cit. 2018-01-20]. Dostupné z: <https://www.autocont.cz/aktuality/openspace/gdpr-microsoft/office-365>

Bakaláři. *Základní informace* [online]. 2018 [cit. 2018-01-20]. Dostupné z: <http://bakalari.cz/Static/GDPR/informace>

Bizagi. *Bizagi* [online]. 2018 [cit. 2018-01-20]. Dostupné z: <https://www.bizagi.com/en/products/bpm-suite/modeler>

European Union Agency for Network and Information Security. *Cloud Computing: Benefits, risks and recommendations for information security* [online]. 2018 [cit. 2018-01-20]. Dostupné z: <https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment>

Finalsite. *How To Prepare Your School For The GDPR* [online]. 2018 [cit. 2018-01-20]. Dostupné z:<https://www.finalsite.com/blog/p/~post/how-to-prepare-your-school-for-the-gdpr-8112017> [online 2018-01-20]

Google. *Google apps pro vzdělání* [online]. 2018 [cit. 2018-01-20]. Dostupné z: <https://www.google.cz/apps/intl/cs/edu/>

Google Cloud. *Google Cloud* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <https://www.google.com/cloud/security/gdpr/

Ministerstvo školství, mládeže a tělovýchovy. *Stručný návod na zabezpečení procesů souvisejících s GDPR* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <http://www.msmt.cz/dokumenty-3/strucny-navod-na-zabezpeceni-procesu-souvisejicich-s-gdpr>

Ministerstvo školství, mládeže a tělovýchovy. *Záznamy o činnostech zpracování* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <http://www.msmt.cz/file/46280_1_1/>

National Institute of Standards and Technology. *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology* [online]. 2018 [cit. 2018-01-20]. Dostupné z: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Nová citační norma ČSN ISO 690. *2011 - Bibliografické citace* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <https://sites.google.com/site/novaiso690/>

Office 365. *Office 365* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <https://resources.office.com/ww-thankyou-GDPR-comply-infographic.html?LCID=EN>

Privazy Plan. *EU obecné nařízení o ochraně osobních údajů "Posouzení vlivu na ochranu osobních údajů*"[online]. 2018 [cit. 2018-01-12]. Dostupné z: <http://www.privacy-regulation.eu/cs/35.htm>

Procesoid. *Procesoid* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <https://procesoid.com/cesko/>

TeamViewer. *TeamViewer* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <https://www.teamviewer.com/cs/>

Úřad pro ochranu osobních údajů. *Stanovisko č. 05/2012 ke cloud computingu* [online]. 2018 [cit. 2018-01-02]. Dostupné z: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=16706>

Úřad pro ochranu osobních údajů. *Základní příručka* [online]. 2018 [cit. 2018-01-11]. Dostupné z: <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744>

Zabbix. *Zabbix* [online]. 2018 [cit. 2018-01-20]. Dostupné z: <https://www.zabbix.com/>

Systém online. *Díl třetí: Práva subjektů osobních údajů podle GDPR* [online]. 2018 [cit. 2018-01-11]. Dostupné z: <https://www.systemonline.cz/it-pravo/gdpr-od-a-do-z-2.htm>

7.2 Literární zdroje

FIŠER, Roman. Procesní řízení pro manažery: jak zařídit, aby lidé věděli, chtěli, uměli i mohli. Praha: Grada, 2014. Manažer. ISBN 978-80-247-5038-5.

JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Brno: Computer Press, 2011. ISBN 9788025134580.

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

8 Seznam použitých zkratek

AD	Active Directory je systém adresářových služeb LDAP využívaných v serverových systémech společnosti Microsoft.
DC	Domain Controler, doménový řadič je součást Microsoft serveru pro bezpečné ověřování požadavků
DPIA	Data Protection Impact Assessment
ERP	Enterprise resource planning, informační systém pro plánování a řízení podnikových zdrojů
GDPR	General Data Protection Regulation, je to nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
HTTPS	HyperText Transfer Protocol – Secure
ICT	informační a komunikační technologie
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
VLAN	Virtuální datová síť, zřízena pomocí aktivního síťového prvku
VPN	Virtuální privátní síť

9 Seznam tabulek, obrázků a příloh

9.1 Seznam obrázků

9.2 Seznam tabulek

9.3 Seznam příloh

10 Přílohy

Příloha 1 - Vzor struktury směrnice

„Směrnice školy … pro ochranu osobních údajů

Platnost směrnice: od 1. 5. 2018

1. Působnost

1.1 Tato směrnice upravuje postupy školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji, pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů. Směrnice rovněž upravuje některé povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji.

1.2 Tato směrnice je závazná pro všechny zaměstnance školy. Směrnice je závazná i pro další osoby, které mají se školou jiný právní vztah (smlouva o dílo, nájemní smlouva) a které se zavázaly postupovat podle této směrnice.

2. Zásady nakládání s osobními údaji

Při nakládání s osobními údaji se škola, její zaměstnanci a další osoby řídí těmito zásadami:

- *Postupovat při nakládání s osobními údaji v souladu s právními předpisy,*
- *S osobními údaji nakládat uvážlivě, souhlas se zpracováním osobních údajů nenadužívat,*
- *Zpracovávat osobní údaje ke stanovenému účelu a ve stanoveném rozsahu a dbát na to, aby tyto byly pravdivé a přesné,*
- *Zpracovávat osobní údaje v souladu se zásadou zákonnosti – na základě právních předpisů, při plnění ze smlouvy, při plnění právní povinnosti správce, při ochraně životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (zejména děti požívají vyšší ochrany), při ochraně oprávněných zájmů školy, při ochraně veřejného zájmu, a zpracování osobních údajů na základě souhlasu,*
- *Respektovat práva člověka, který je subjektem údajů, zejména práva dát a odvolat souhlas se zpracováním, práva na výmaz, namítat rozsah zpracování apod.,*
- *Poskytovat při zpracování osobních údajů zvláštní ochranu dětem,*
- *Poskytovat informace o zpracování osobních údajů, komunikovat,*
- *Při uzavírání smluv a právním jednání postupovat se zřetelem na povinnost chránit osobní údaje před zneužitím,*
- *Spolupracovat s pověřencem pro ochranu osobních údajů.*

3. Postupy školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji

3.1 Škola všechny osobní údaje, se kterými nakládá a které zpracovává, chrání vhodnými a dostupnými prostředky před zneužitím. Přitom škola především uchovává osobní údaje

v prostorách, na místech, v prostředí nebo v systému, do kterého má přístup omezený, předem stanovený a v každý okamžik alespoň řediteli školy známý okruh osob; jiné osoby mohou získat přístup k osobním údajům pouze se svolením ředitele školy nebo jím pověřené osoby.

3.2 Škola zavede taková opatření, aby o nakládání a zpracování osobních údajů měl přehled alespoň ředitel školy nebo jím pověřená osoba a pověřenec pro ochranu osobních údajů. Mezi tato opatření patří např. ústní nebo písemná informace, písemná komunikace, stanovení povinností v pracovní smlouvě, v dohodě o provedení práce, v dohodě o pracovní činnosti, ve smlouvě, kterou škola uzavírá se třetí osobou (nájemní smlouva, smlouva o dílo, smlouva o poskytování služeb).

3.3 Škola alespoň jednou za rok provede zhodnocení postupů při nakládání a zpracování osobních údajů. Zhodnocení může být provedeno dle zvyklostí školy, zpravidla se učiní stručný záznam např. v zápisu z porady. Zjistí-li se, že některé postupy školy jsou zastaralé, zbytečné nebo se neosvědčily, učiní škola bezodkladně nápravu.

3.4 Každý zaměstnanec školy při nakládání s osobními údaji respektuje jejich povahu, tedy že jde o součást soukromí člověka jako subjektu údajů, a tomu přizpůsobí úkony s tím spojené. Zaměstnanec zejména osobní údaje nezveřejňuje bez ověření, že takový postup je možný, nezpřístupňuje osobní údaje osobám, které neprokáží právo s nimi nakládat. Zaměstnanec, vyplývá-li taková povinnost z jiných dokumentů, informuje subjekt údajů o jeho právech na ochranu osobních údajů; jinak odkáže na ředitele školy nebo jím určenou osobu nebo na pověřence pro ochranu osobních údajů.

3.5 Škola při nakládání a zpracovávání osobních údajů aktivně spolupracuje s pověřencem pro ochranu osobních údajů.

3.6 Škola ihned řeší každý bezpečnostní incident týkající se osobních údajů, a to v součinnosti s pověřencem pro ochranu osobních údajů. V případě, že je pravděpodobné, že incident bude mít za následek vysoké riziko pro práva a svobody fyzických osob, především konkrétního žáka, studenta, zaměstnance, zákonného zástupce atd., škola tuto osobu vždy informuje a sdělí, jaká opatření k nápravě přijala. O každém incidentu se sepíše záznam. O každém závažném incidentu škola informuje Úřad pro ochranu osobních údajů.

3.7 Vzhledem k tomu, že škola eviduje v podstatě údaje o žácích a zaměstnancích, které stanovují právní předpisy (zejména školský zákon a pracovněprávní předpisy), nemá oznamovací povinnost vůči Úřadu pro ochranu osobních údajů podle ustanovení 3.6 věty první.

3.8 Organizační opatření k ochraně osobních údajů ve škole

3.8.1 Třídní výkazy, katalogové listy a další materiály ze školní matriky, které obsahují osobní údaje žáků, jsou trvale uloženy v uzamykatelných skříních v kanceláři školy, a to v kanceláři ředitele nebo zástupce ředitele školy). Třídním učitelům jsou zapůjčeny na nezbytně dlouhou dobu k provedení zápisů. Vyučující jednotlivých předmětů zapisují jen klasifikaci dle úvazku a výhradně v kanceláři ředitele nebo zástupce ředitele. Třídní výkazy, katalogové listy, další materiály ze školní matriky či jejich části nelze vynášet ze školy, předávat cizím osobám nebo kopírovat a kopie poskytovat neoprávněným osobám.

3.8.2 Elektronická školní matrika je vedena v zabezpečeném informačním systému „Jedničkáři a propadlíci". Do tohoto systému mají přístup jednotliví pedagogové školy a další osoby výslovně a písemně pověřené ředitelem školy, a to jen na základě jedinečného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením. Při práci s elektronickou evidencí oprávnění nesmí oprávněné osoby opouštět počítač bez odhlášení se, nemohou nechat nahlížet žádnou jinou osobu a musí chránit utajení přihlašovacího hesla; a v případě nebezpečí jeho vyzrazení jej ihned (ve spolupráci se správcem sítě) změnit. Přístupy nastavuje pověřený zaměstnanec školy – správce počítačové sítě, který nastavuje potřebné zabezpečení dat a školní počítačové sítě (dle pokynů ředitele a zástupce ředitele). Zákonní zástupci žáků a žáci mají zajištěn zabezpečený dálkový přístup výhradně k vlastním údajům o klasifikaci na základě přihlašovacího kódu a hesla předaného správcem počítačové sítě přísně individuálně prostřednictvím třídních učitelů.

3.8.3 Osobní spisy zaměstnanců jsou uloženy v uzamykatelných skříních v kanceláři ředitele školy, přístup k nim má ředitel školy nebo zástupce ředitele, zastupuje-li ředitele, případně, je-li to nutné též sekretářka školy nebo mzdová účetní.

3.8.4 Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu. O tomto právu jsou zaměstnanci poučeni, zpravidla na poradě.

3.8.5 Zaměstnanci školy neposkytují bez právního důvodu žádnou formou osobní údaje zaměstnanců školy a žáků cizím osobám a institucím, tedy ani telefonicky ani mailem ani při osobním jednání.

3.8.6 Písemná hodnocení a posudky, která se odesílají mimo školu, např. pro potřeby soudního řízení, přijímacího řízení, zpracovávají zaměstnanci určení ředitelem školy. Nejsou však oprávněni samostatně tato hodnocení podepisovat, poskytovat a odesílat jménem školy a mají povinnost zachovávat mlčenlivost o dané věci.

3.8.7 Seznamy žáků se nezveřejňují, neposkytují bez vědomého souhlasu žáků či zákonných zástupců žáků jiným fyzickým či právnickým osobám nebo orgánům, které neplní funkci orgánu nadřízeného škole nebo nevyplývá-li to ze zákona.

3.8.8 V propagačních materiálech školy, ve výroční zprávě či ročence školy, na školním webu či na nástěnkách ve škole apod. lze s obecným souhlasem žáků nebo zákonných zástupců žáků uveřejňovat výhradně textové či obrazové informace o jejich úspěších (např. u soutěží umístění na předních místech) s uvedením pouze jména (případně ročníku či třídy). Při publikování v tisku se autor dotazuje na souhlas příslušného žáka. Žák nebo zákonný zástupce má právo požadovat bezodkladné zablokování či odstranění informace či fotografie či záznamu týkající se jeho osoby, který zveřejňovat nechce. Platí to i o fotografiích či záznamech žáka bez uvedení jména v rámci obecné dokumentace školních akcí a úspěchů.

3.8.9 Psychologické, lékařské a jiné průzkumy a testování mezi žáky, jejichž součástí by bylo uvedení osobních údajů žáka, lze provádět jen se souhlasem žáka nebo zákonného zástupce žáka. To se netýká anonymních průzkumů, které však musí souviset se vzděláváním na dané škole a musí s nim předem písemně souhlasit ředitel či zástupce ředitele; to platí zvláště v případě, že výsledky jsou poskytovány mimo školu.

3.8.10 Pokud jsou pro vedení dokumentace využívány formuláře a software, je nutné provést kontrolu, zda nepožadují či nenabízejí evidenci nadbytečných údajů a tyto údaje nezpracovávat.

3.8.11 Ve škole se neprovozují kamerové systémy sledující prostory používané žáky a zaměstnanci školy v době, kdy jsou žáci přítomni ve škole.

3.8.12 Uzavírá-li škola jakoukoli smlouvu (nájemní smlouvu, smlouvu o dílo, smlouvu o poskytnutí služeb, nepojmenovanou smlouvu apod.), k jejímuž plnění je zapotřebí druhé smluvní straně poskytnout osobní údaje, škola vždy a bezpodmínečně bude trvat na tom, aby ve smlouvě byla druhé smluvní straně uložena povinnost:

- *přijmout všechna bezpečnostní, technická, organizační a jiná opatření s přihlédnutím ke stavu techniky, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování k zabránění jakéhokoli narušení poskytnutých osobních údajů,*
- *nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu školy,*
- *zpracovávat osobní údaje pouze pro plnění smlouvy (vč. předání údajů do třetích zemí a mezinárodním organizacím); výjimkou jsou pouze případy, kdy jsou určité povinnosti uloženy přímo právním předpisem,*
- *zajistit, aby se osoby oprávněné zpracovávat osobní údaje u dodavatele byly zavázány k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti,*

- *zajistit, že dodavatel bude škole bez zbytečného odkladu nápomocen při plnění povinností školy, zejména povinnosti reagovat na žádosti o výkon práv subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 nařízení a povinnosti provádět předchozí konzultace dle čl. 36 nařízení, a že za tímto účelem zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje školu,*
- *po ukončení smlouvy řádně naložit se zpracovávanými osobními údaji, např. že všechny osobní údaje vymaže, nebo je vrátí škole a vymaže existující kopie apod.,*
- *poskytnout škole veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené škole právními předpisy,*
- *umožnit kontrolu, audit či inspekci prováděné školou nebo příslušným orgánem dle právních předpisů,*
- *poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví škola, součinnost potřebnou pro plnění zákonných povinností školy spojených s ochranou osobních údajů, jejich zpracováním,*
- *poskytnuté osobní údaje chránit v souladu s právními předpisy,*
- *přiměřeně postupovat podle této směrnice, která je přílohou smlouvy.*

4. Pravidla pro získávání, shromažďování, ukládání, použití, šíření a uchovávání osobních údajů.

4.1 Škola nakládá a zpracovává pouze osobní údaje, které

- *souvisejí s pracovním a mzdovým zařazením zaměstnanců či smluvních pracovníků, se sociálním, a zdravotním pojištěním (např. dosažené vzdělání, délka praxe, funkční zařazení apod.),*
- *souvisejí s jednoznačnou identifikací zákonných zástupců žáků v souladu se zákonem (jméno, příjmení, bydliště, kontakt, např. telefonní číslo pro případ nutného kontaktu školy se zákonným zástupcem v rámci ochrany zdraví, bezpečnosti a práv žáka, další údaje nezbytné např. pro vydání správního rozhodnutí apod.),*
- *související s identifikací žáka ze zákona (datum narození, místo narození, rodné číslo, státní příslušnost, bydliště, údaj o zákonném zástupci, soudní rozhodnutí vztahující se k přidělení dítěte do výchovy, nutný zdravotní údaj apod.),*
- *jsou nezbytné pro plnění právní povinnosti, ochranu oprávněných zájmů školy nebo ve veřejném zájmu,*
- *k jejichž zpracování získala souhlas subjektu údajů.*

4.2 Osobní údaje se uchovávají pouze po dobu, která je nezbytná k dosažení účelu jejich zpracování, včetně archivace.

4.4 K osobním údajům mají přístup osoby k tomu oprávněné zákonem nebo na základě zákona. Do jednotlivých dokumentů školy, které obsahují osobní údaje, mohou nahlížet

- *do osobního spisu zaměstnance* vedoucí zaměstnanci, kteří jsou zaměstnanci nadřízeni. Právo nahlížet do osobního spisu má orgán inspekce práce, úřad práce, soud, státní zástupce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad a zpravodajské služby. Zaměstnanec má právo nahlížet do svého osobního spisu, činit si z něho výpisky a pořizovat si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele (§ 312 zákoníku práce),
- *do údajů žáka ve školní matrice pedagogičtí pracovníci školy (v rozsahu daném pedagogickou funkcí), sekretářka,*
- *do údajů o zdravotním stavu žáka, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv - výchovný poradce, vedoucí pedagogičtí pracovníci, třídní učitel,*
- *do spisu, vedeném ve správním řízení účastníci správního řízení, sekretářka, vedoucí pedagogičtí pracovníci (ředitel, zástupce ředitele, vedoucí vychovatel), osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.*

5. Souhlas k zpracováním osobních údajů

5.1 Ke zpracování osobních údajů nad rozsah vyplývající ze zákonů (ze zákona vyplývá i oprávněný zájem, plnění právní povinnosti, plnění smlouvy, veřejný zájem) je nezbytný souhlas osoby, o jejíž osobní údaje se jedná. Souhlas musí být poučený, informovaný a konkrétní, nejlépe v písemné podobě. Souhlas se získává pouze pro konkrétní údaje (určené např. druhově), na konkrétní dobu a pro konkrétní účel.

5.2 Souhlas se získává pro zpracování osobních údajů jen tehdy, pokud je jejich zpracování nezbytně nutné a právní předpisy jiný důvod pro toto zpracování nestanoví.

5.3 Souhlas se poskytuje podle účelu např. na celé období školní docházky na škole, na školní rok, na dobu školy v přírodě apod. Udělený souhlas může být v souladu s právními předpisy odvolán.

6. Některé povinnosti školy, jejích zaměstnanců, případně dalších osob při nakládání s osobními údaji.

6.1 Každý zaměstnanec školy je povinen počínat si tak, aby neohrozil ochranu osobních údajů zpracovávaných školou.

6.2 Dále je každý zaměstnanec školy povinen

- *zamezit nahodilému a neoprávněnému přístupu k osobním údajům zaměstnanců, žáků, zákonných zástupců a dalších osob, které škola zpracovává,*
- *, pokud zjistí porušení ochrany osobních údajů, neoprávněné použití osobních údajů, zneužití osobních nebo jiné neoprávněné jednání související s ochranou osobních údajů, bezodkladně zabránit dalšímu neoprávněnému nakládání, zejména zajistit znepřístupnění, a ohlásit tuto skutečnost řediteli školy či jinému příslušnému zaměstnanci.*

6.3 Ředitel školy je povinen

- *informovat zaměstnance o všech významných skutečnostech, postupech nebo událostech souvisejících s nakládáním s osobními údaji ve škole, a to bez zbytečného odkladu,*
- *zajistit, aby zaměstnanci školy byli řádně poučeni o právech a povinnostech při ochraně osobních údajů,*
- *zajišťovat, aby zaměstnanci školy byli podle možností a potřeb školy vzděláváni nebo proškolováni o ochraně osobních údajů*
- *zajistit, aby škola byla schopna řádně doložit plnění povinností školy při ochraně osobních údajů, které vyplývají z právních předpisů.*

S touto směrnicí byli seznámeni dne …:

1. *Jméno a příjmení* *podpis*
2. *Jméno a příjmení* *podpis.*