Řízení rizik a procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů

Marcela Králová

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2018/2019

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

Jméno a příjmení:	**Marcela Králová**
Osobní číslo:	**L16037**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**

Zásady pro vypracování:

1. **Zpracujte průzkum literárních pramenů a zhodnoťte teoretické a zákonné důvody týkající se zpracování osobních údajů v rozsahu nařízení GDPR.**
2. **Analyzujte a zhodnoťte aplikaci teorie do praxe ve vybrané organizaci.**
3. **Navrhněte a formulujte opatření pro efektivní řízení procesů v souvislosti s nařízením GDPR.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] NULÍČEK, Michal. GDPR – obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

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

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

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Slavomíra Vargová, PhD.**
Ústav krizového řízení

Datum zadání bakalářské práce: **30. listopadu 2018**

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

V Uherském Hradišti dne 30. listopadu 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.
②

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti, dne: 15. 5. 2019

Jméno a příjmení studenta: Marcela Králová

.....
podpis studenta

ABSTRAKT

Práce se zabývá řízením rizik a procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů. Pro správné řízení rizik je nezbytné identifikovat jednotlivá rizika, provést jejich analýzu a výsledky zhodnotit. Na základě zjištěných údajů provést řízení rizik jednotlivých procesů ku prospěchu organizace a tím zabránit sankcím, které by organizaci postihly v případě porušení ochrany osobních údajů. Výsledky této práce mohou posloužit jako návrh k řízení rizik, která jsou v této organizaci prokazatelná.

Klíčová slova: Ochrana osobních údajů, Analýza procesů, Identifikace rizik, Analýza rizik, Hodnocení rizik, Řízení rizik

ABSTRACT

The bachelor thesis deals with risk management of processes in kindergarten. It is also good to think about new personal data protection legislation. It is needed to identify each risk, analyze and evaluate the results. According to the evaluated results is it necessary to make a risk management of each process for organization's benefit. On the other hand there are sanctions which could affect organization in case of personal protection violation. The results could have influence on risk management in this organization which are provable for next progress.

Keywords: Personal data protection, Process analysis, Identification of risks, Risk analysis, Risk avaluation, Risk management

Velké poděkování patří paní Ing. Slavomíře Vargové, Ph.D., za odborné a profesionální vedení při vypracování bakalářské práce, za její podnětné rady, připomínky, vstřícnost a lidský přístup.

Dále bych chtěla poděkovat ředitelce mateřské školy XY, za ochotu a čas, který mi věnovala při poskytování informací.

Nemalý dík patří i mé rodině za trpělivost a podporu při mém studiu.

OBSAH

ÚVOD

Obecné nařízení o ochraně osobních údajů neboli GDPR (General Data Protection Regulation) je nařízení Evropské unie, které vešlo v platnost 25. května 2018. Organizace v České republice se musely na toto nařízení připravit. Probíhaly analýzy spojené s ochranou osobních údajů. Hledala se riziková místa a docházelo k vyhodnocování skutečného stavu. Po zjištění slabých míst se navrhovala vhodná opatření, aby mohl proběhnout proces ochrany osobních údajů v souvislosti s obecným nařízením. V současné době je nařízení již v platnosti a dá se posuzovat, jak která organizace implementaci zvládla a jak chrání osobní údaje. Tato práce je zaměřena na řízení rizik a procesů v mateřské škole právě s ohledem na novou právní úpravu ochrany osobních údajů. V první řadě je vhodné připomenout obecné údaje související s historií vzniku ochrany osobních údajů a postupný přechod na obecné nařízení Evropské unie, dále pak oblasti působnosti obecného nařízení a pojmy, se kterými obecné nařízení pracuje. Nesmí se zapomenout na zabezpečení osobních údajů a sankce, které vyplývají z porušení tohoto nařízení. Vzhledem k tomu, že předmětem práce je řízení rizik a procesů dané organizace, je nezbytné se seznámit i s pojmy využívanými managementem rizik, a to především analýzou rizik a řízením rizik, aby bylo zřejmé, co je cílem této práce. Samotná mateřská škola XY, která je zde zmiňována, nepatří mezi velké organizace. Nachází se na malé obci, která má zhruba 400 obyvatel. Má pouze jednu třídu. Technická vybavenost organizace je na základní úrovni. Ale i pro tuto organizaci platí obecné nařízení o ochraně osobních údajů, tudíž se tímto nařízením musí řídit, aby došlo ke zjištění skutečnosti. Zda organizace neporušuje zásady obecného nařízení o ochraně osobních údajů, provede se analýza rizik současného stavu organizace v souvislosti s tímto nařízením. Pro správné provedení analýzy rizik je důležité seznámení se samotnou organizací a také pochopit účel, ke kterému byla zřízena, a to je předškolní vzdělávání. Již zde je zřejmé, že organizace bude pracovat nejen s osobními údaji svých zaměstnanců, ale i dětí a jejich zákonných zástupců. Okrajově je třeba se zmínit i o hospodaření organizace, aby bylo možné posoudit, s jakými finančními prostředky disponuje a zda by v případě porušení obecného nařízení měla prostředky na úhradu případné sankce. Rozčleníme jednotlivé procesy, které v organizaci probíhají a zanalyzujeme současný stav ochrany osobních údajů. Budou se identifikovat rizikové oblasti a provede se za pomocí metody FMEA analýza rizik. Následně se zjištěné údaje zhodnotí. Výsledky této analýzy slouží pro samotné řízení rizik a procesů. Zjištěná rizika je nutné zvládnout. Pokud nepůjdou zcela odstranit, tak je minimalizovat, aby organizace splnila obecné nařízení a zbytečně se nevystavila sankcím.

I. TEORETICKÁ ČÁST

1 HISTORIE VZNIKU OCHRANY OSOBNÍCH ÚDAJŮ

Prvním celosvětově významným mezinárodním dokumentem zaručujícím právo na soukromí byla Všeobecná deklarace lidských práv, přijatá v San Francisku v roce 1948 Valným shromážděním Organizace spojených národů. Tato deklarace v čl. 12 stanovovala mimo jiné zákaz vystavovat kohokoliv svévolnému zasahování do soukromého života a korespondence [1].

Obdobně jako Všeobecná deklarace lidských práv zaručovala v čl. 8 právo na respektování rodinného a soukromého života Evropská úmluva o ochraně lidských práv a svobod sjednaná v roce 1950 v Římě [1].

Tyto dva významné dokumenty deklarovaly právo na ochranu soukromí obecně, ale nevěnovaly se blíže právu na ochranu osobních údajů při jejich zpracování, které bylo v době přijetí těchto dokumentů přirozenou součástí práva na ochranu soukromí, protože okolnosti prozatím nenutily tuto oblast zvlášť vyčlenit [1].

1.1 Vývoj a stav ochrany osobních údajů v České republice

V prostředí České republiky začala být ochrana osobních údajů při jejich zpracování samostatně řešena až přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který jak již z názvu vyplývá, upravoval pouze zpracování osobních údajů v informačních systémech [1].

Český právní řád poskytuje osobním údajům komplexní právní ochranu. Základ týkající se ochrany osobních údajů je obsažen již v Listině, která je součástí ústavního pořádku.

Právo na ochranu osobních údajů je často kladeno do protikladu s právem na informace [2].

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky mimo jiné říká, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě [3].

O plnohodnotné ochraně osobních údajů při jejich zpracování v České republice lze hovořit až od 1. června 2000, kdy nabyl účinnosti zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, kterým byl zároveň zřízen Úřad pro ochranu osobních údajů, jako dozorový úřad nad dodržováním povinností stanovených při zpracování osobních údajů [1].

ZoOU (Zákon o ochraně osobních údajů – dále jen ZoOU) stanoví pro osoby, které se rozhodnou zpracovávat osobní údaje a stanou se tak správci nebo zpracovateli, celou řadu povinností. Tyto povinnosti jsou soustředěny především (ale nejen) v § 5 ZoOU. Toto ustanovení tak představuje jednu z klíčových částí ZoOU, neboť jeho nerespektování při zpracování znamená kolizi se zákonem a hrozbu sankce za správní delikt [4].

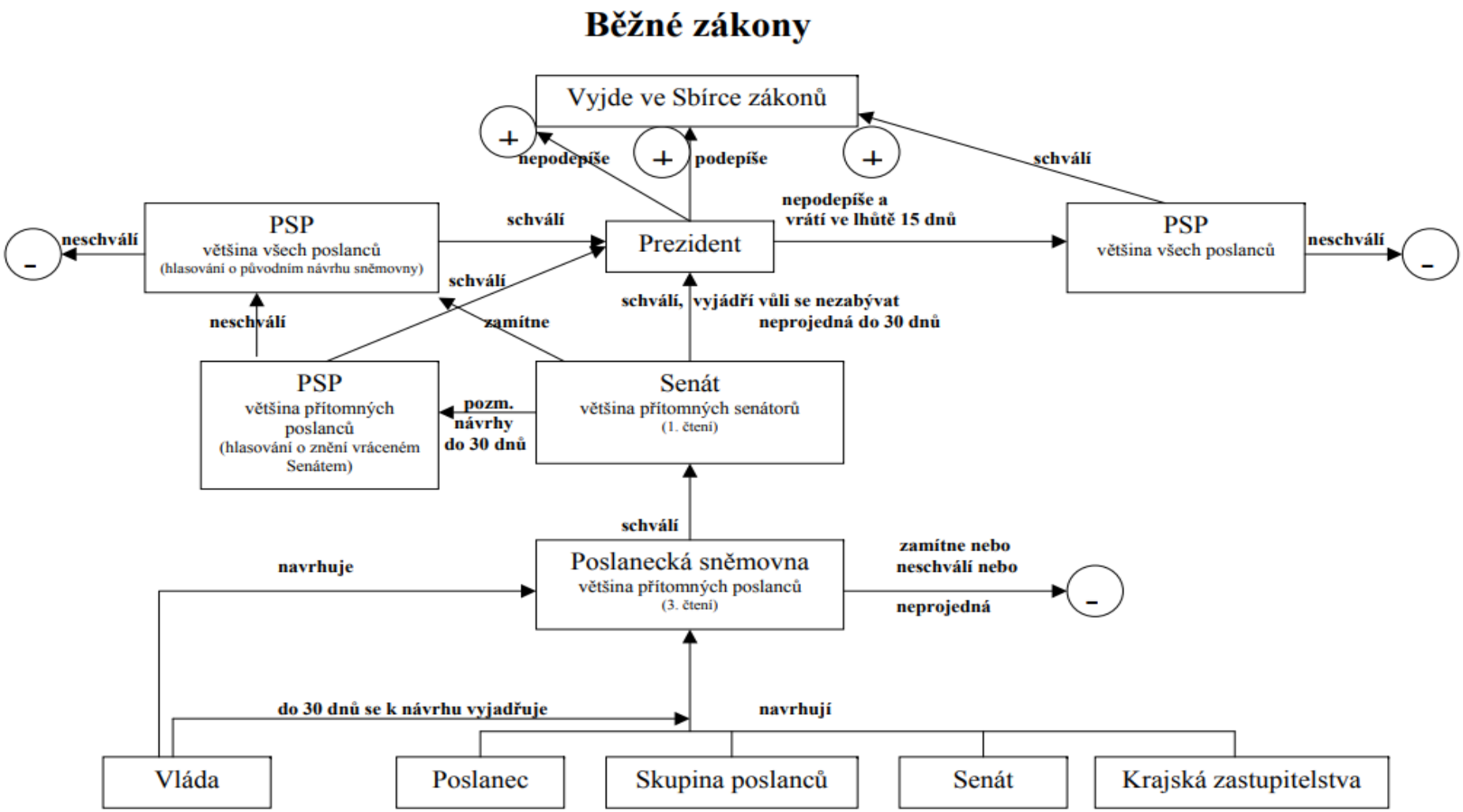
1.2 Evropská unie

V roce 2016 Evropská unie přijala obecné nařízení o ochraně údajů (GDPR), které je platné ve všech 28 členských státech [5]. Nařízení dává subjektům údajů (lidem – občanům) mnohem větší práva, stanovuje mnohem přísnější požadavky jak správcům, tak zpracovatelům (firmám a institucím) a uplatňuje výrazně vyšší sankce, než tomu bylo doposud [5]. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů) je v platnosti a účinnost nastala 25. května 2018 po dvouleté periodě určené k přípravě. Nahrazuje tak současný zákon č. 101/2000 Sb., o ochraně osobních údajů [5].

Nový zákon o zpracování osobních údajů

V souvislosti s GDPR musí Česká republika přijmout nový zákon o zpracování osobních údajů (ZZOÚ), který jednak zruší stávající zákon o ochraně osobních údajů a jednak upraví některé otázky, jež GDPR přímo neřeší nebo v nichž jednotlivým státům umožňuje přísnější či méně přísnou úpravu [6]. Vládní návrh zákona o zpracování osobních údajů byl ve třetím čtení jako sněmovní tisk č. 138 schválen 5. 12. 2018. Poslanecká sněmovna jej 8. 1. 2019 podstoupila Senátu jako tisk 25/0. Senát návrh 30. 1. 2019 projednal a vrátil sněmovně s pozměňovacími návrhy. Dne 12. 3. 2019 hlasováno o přijetí zákona. Zákon byl přijat a dne 10. 4. 2019 podepsán prezidentem. Zákon vyhlášen 24. 4. 2019 ve Sbírce zákonů pod číslem 110/2019 [7]. Legislativní proces znázorňuje Obrázek 1.

Tento vládní návrh zákona o zpracování osobních údajů je také nazýván Českým adaptačním zákonem. Obsahuje změny oproti zákonu o ochraně osobních údajů a reaguje na Obecné nařízení (GDPR). Největší změny se týkají především škol a malých obcí. Český adaptační zákon stanovuje maximální výši pokuty na 15 tis. Kč [8]. Jedná se o pokuty při porušení zákona o ochraně osobních údajů. Problémy kvůli absenci Českého adaptačního zákona měl Úřad pro ochranu osobních údajů [8].



Obrázek 1: Schéma legislativního procesu [9]

2 OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Obecné nařízení představuje nový právní rámec ochrany osobních údajů v evropském prostoru [5]. Charakteristická pro Obecné nařízení je jeho univerzální použitelnost ve všech státech Evropské unie (a Islandu, Norska a Lichtenštejnska) [5]. Anglická zkratka Obecného nařízení, se kterou se lze setkat v odborných textech či hovoru, je GDPR [5].

2.1 Působnost Obecného nařízení

Působnost lze obecně označit jako vymezení rozsahu a realizace právního předpisu a obecně ji lze dělit na osobní, věcnou, místní a časovou [1].

2.1.1 Osobní působnost

Osobní působnost stanovuje okruh subjektů (adresáty), na které se právní předpis vztahuje. Adresáty Obecného nařízení jsou zejména správci, zpracovatelé, subjekty údajů [1].

2.1.2 Věcná působnost

Věcná působnost vymezuje, jaké vztahy právní předpis upravuje, tedy na co se vztahuje (pozitivní vymezení), případně na co se nevztahuje (negativní vymezení). Obecné nařízení obsahuje jak pozitivní, tak negativní vymezení věcné působnosti [1].

2.1.3 Místní působnost

Místní působnost omezuje působnost právního předpisu na určité území, zejména na to, kde lze jeho aplikaci efektivně vymáhat prostřednictvím dozorových úřadů [1].

2.1.4 Časová působnost

Časová působnost vymezuje dobu, po kterou je právní předpis součástí právního řádu. Je nutné rozlišovat mezi platností a účinností právního předpisu, tj. i Obecné nařízení. Platnost znamená, že právní předpis prošel stanoveným legislativním procesem a byl vyhlášen v příslušné sbírce (pokud jde o zákony, tak ve Sbírce zákonů, pokud jde o právní předpis Evropské unie, tak v Ústředním věstníku Evropské unie), čímž se stává součástí právního řádu. Účinnost znamená, že právní předpis je pro adresáty již závazný a může být aplikován [1].

2.2 Zásady Obecného nařízení

Článek 5 Nařízení upravuje základní zásady zpracování osobních údajů. Ty jsou základními pravidly, od kterých se odvíjejí všechny procesy zpracování a která slouží jako základní určovatelé toho, jak může správce s osobními údaji nakládat [10].

2.2.1 Zásada zákonnosti

Zásada zákonnosti stanoví, že zpracovávat osobní údaje lze jen na základě jednoho z definovaných právních titulů a že zpracování nesmí být v rozporu se zákonem [10].

2.2.2 Zásada korektnosti a transparentnosti

Zásada korektnosti a transparentnosti ukládají správci povinnost být otevřený ohledně zpracování a zajišťovat co největší míru informovanosti subjektů údajů [10].

2.2.3 Zásada účelového omezení

Zásada účelového omezení správci zakazuje – až na výjimky – zpracovávat osobní údaje za jinými účely, než za kterými byly shromážděny [10].

2.2.4 Zásada minimalizace údajů

Zásada minimalizace údajů určuje, jaké údaje může správce za daným účelem zpracovávat. Zpracovány musejí být vždy pouze takové osobní údaje, které jsou pro dosažení účelu nezbytné, a to pouze v nutném rozsahu [10].

2.2.5 Zásada přesnosti

Zásada přesnosti stanoví, že zpracované osobní údaje musejí být přesné a podle potřeby aktualizované. Správce musí přijmout vhodná opatření k tomu, aby nepřesné osobní údaje vymazal nebo opravil [10].

2.2.6 Zásada omezení uložení

Zásada omezení uložení zakotvuje povinnost správce vymazat nebo anonymizovat osobní údaje, které již nepotřebuje pro účel, za kterým byly shromážděny (s výjimkou pro další zpracování) [10].

2.2.7 Zásada integrity a důvěrnosti

Zásada integrity a důvěrnosti určuje základní povinnosti při zabezpečení zpracování osobních údajů správce. Správce musí přijmout vhodná technická a organizační opatření, aby zajistil integritu a důvěrnost osobních údajů [10].

2.2.8 Zásada odpovědnosti

Zásada odpovědnosti nakonec ukládá správci povinnost zajistit soulad se všemi výše uvedenými zásadami a být schopen tento soulad prokázat. Pro dodržení této povinnosti bude správce muset uchovávat důkazy ohledně všech opatření, která přijal s cílem zajistit soulad s Nařízením, jako jsou např. různá posouzení, dokumentace systémů zpracování, popisy bezpečnostních opatření, důkazy o udělených souhlasech se zpracováním či splnění informační povinnosti [10].

2.3 Povinnosti Obecného nařízení

Obecné nařízení přináší povinnosti, které je nezbytné dodržovat.

2.3.1 Povinnost vést záznamy o činnostech zpracování

Kromě povinnosti vést záznamy o činnostech zpracování a ustanovit pověřence, jsou ostatní povinnosti založeny na přístupu založeném na riziku, tj. jejich uplatnění je vázáno na přítomnost rizika či vysokého rizika pro práva a svobody subjektu údajů [5].

2.3.2 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů musí provést správce, pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude představovat vysoké riziko pro práva a svobody fyzických osob. Posouzení se musí provést před započetím předmětného zpracování. Pokud byl ustanoven pověřenec pro ochranu osobních údajů, vyžádá si správce jeho posudek [5].

2.3.3 Předchozí konzultace

Správce je povinen konzultovat zpracování osobních údajů s Úřadem pro ochranu osobních údajů, pokud z posouzení vlivu na ochranu osobních údajů vyplyne, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika. Účelem předchozí konzultace je tak korigovat hrozící vysoké riziko [5].

2.4 Obecné nařízení nedopadá

Toto nařízení se nevztahuje na zpracování osobních údajů prováděné:

a) při výkonu činností, které nespadají do oblasti působnosti práva Evropské unie,
b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU,
c) fyzickou osobou v průběhu výlučně osobních či domácích činností,
d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení [10].

3 OSOBNÍ ÚDAJE

Definice osobního údaje je pro aplikaci Obecného nařízení stěžejní vzhledem k tomu, že zpracování osobních údajů se ze své podstaty týká pouze údajů osobních [1].

3.1 Definice osobních údajů pro účely nařízení Evropského parlamentu a rady (EU) 2016/679

Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby [10].

Osobním údajem se rozumí jakákoliv informace, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby. Nejedná se tedy pouze o identifikační údaje, na jejichž základě lze konkrétní osobu jednoznačně určit, ale o veškeré informace, které se určitelného člověka týkají, byť jej ani samy o sobě, ani v kombinaci s dalšími informacemi neidentifikují (např. počet dětí, dosažené vzdělání, zůstatek na bankovním účtu). Není rozhodující, zda je údaj zcela pravdivý a objektivně měřitelný (datum narození, místo bydliště, údaj o vlastnictví určité věci) [10].

3.1.1 Anonymní údaje

Zcela odlišnými údaji, než jsou osobní údaje, jsou údaje anonymní, které na rozdíl od osobních, nelze vztáhnout k identifikované či neidentifikované osobě. Anonymní údaje jsou tedy takové údaje, mezi nimiž neexistuje pouto se subjektem údajů a toto pouto nemůže být správcem ani nikým jiným (za rozumného předpokladu) obnoveno [1].

3.1.2 Pseudonymizované údaje

Za anonymní údaje však nelze považovat údaje pseudonymizované, na které se musí stále nahlížet jako na osobní údaje, protože jak vyplývá z pojmu pseudonymizace, jde jen o zdánlivou, nepravou anonymizaci [1].

3.1.3 Rodné číslo

Ač není rodné číslo zvláštní kategorií osobních údajů, má zvláštní postavení spočívající v určení zákonných podmínek, za kterých jej lze využívat, a z toho pohledu jej lze označit za „kvazicitlivý“ osobní údaj [1]. Podmínky pro využívání rodných čísel jsou stanoveny v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů [1].

3.1.4 Kopírování občanského průkazu

Je nutné si uvědomit, že občanský průkaz je veřejná listina, kterou občan prokazuje své jméno, popř. jména, přímení, podobu a státní občanství České republiky, jakož i další údaje v něm zapsané. Občanský průkaz tedy obsahuje soubor osobních údajů, který je způsobilý ke zfalšování a zneužití identity. Proto je nebezpečné, pokud se tento souhrn prostřednictvím kopie občanského průkazu dostane do rukou komukoliv dalšímu, přičemž s každou pořízenou kopií roste riziko jejího zneužití [1].

3.1.5 Zvláštní kategorie osobních údajů (citlivé údaje)

Některé osobní údaje jsou takového charakteru, že mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci [5]. Zakazuje se zpracování údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby [10].

3.2 Účel zpracování osobních údajů

Alfou a omegou zpracování osobních údajů a souvisejících povinností pro správce je účel zpracování. Účel zpracování musí být legitimní a nesmí být protiprávní. Účel zpracování velmi úzce souvisí se zásadami zpracování a rovněž s právními důvody, které v sobě mají zahrnutý účel zpracování (až na souhlas subjektu údajů, nicméně i souhlas musí být dán pro určitý účel zpracování) [1].

3.3 Právní důvody zpracování osobních údajů

Právní důvody zpracování osobních údajů znamenají oprávnění správce osobní údaje zpracovávat [5].

3.3.1 Souhlas se zpracováním osobních údajů

Souhlas je jedním z právních důvodů, na základě kterého může správce osobní údaje zpracovávat. Souhlas se vždy poskytuje k určitému účelu zpracování, který musí subjekt údajů znát [2]. Zásadní je tzv. odlišitelnost souhlasu, což znamená, že souhlas musí být odlišen od jiných skutečností, ke kterým se subjekt údajů vyjadřuje [5].

Pro účely tohoto nařízení se rozumí „souhlasem“ subjektu údajů jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů [10].

3.3.2 Odvolatelnost souhlasu

Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním [5].

3.3.3 Právo na opravu nepřesných údajů

Subjekt údajů má právo na opravu nepřesných osobních údajů, které se ho týkají [5].

3.4 Subjekt údajů

Subjektem údajů je fyzická osoba, jíž se osobní údaje týkají. Subjekt údajů není právnická osoba. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách [5].

3.4.1 Svoboda a odlišitelnost souhlasu

Subjekt údajů není povinen souhlas udělit a nesmí být za jeho neudělení ze strany správce nijak trestán [1]. Odlišitelnost souhlasu značí především to, že by měl být rozumným způsobem odlišitelný od samotného textu. To neznamená, že musí být předkládán na samostatném formuláři, ale měl by být rozumným způsobem odlišitelný od ostatního textu [1].

3.4.2 Ochrana dítěte

Děti zasluhují zvláštní ochranu osobních údajů, protože si mohou být méně vědomy dotčených rizik, důsledků a záruk a svých práv v souvislosti se zpracováním osobních údajů. Tato zvláštní ochrana by se měla zejména vztahovat na používání osobních údajů dětí pro účely

marketingu nebo vytváření osobnostních či uživatelských profilů a shromažďování osobních údajů týkajících se dětí při využívání služeb nabízených přímo dětem [10].

Existuje zvláštní ustanovení o souhlasu dětí „v souvislosti s nabídkou služeb informační společnosti“, tedy služeb vyžádaných a poskytnutých přes internet. GDPR chápe pod pojmem děti osoby mladší 16 let [5].

3.5 Správce

Správcem je subjekt, nerozhoduje, jaké právní formy, který určuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti [5].

3.6 Zpracovatel

Zpracovatelem je subjekt, kterého si správce najímá, aby pro něj prováděl s osobními údaji zpracovatelské operace. Jinými slovy zpracovatel zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří nebo vyplývají z činnosti, pro kterou byl zpracovatel správcem pověřen [5].

3.7 Vztah správce a zpracovatel

Správce může ke zpracování osobních údajů přibrat jiný subjekt, který pro něj bude osobní údaje zpracovávat. Za tím účelem musí být mezi správcem a zpracovatelem uzavřena písemná smlouva [5].

3.8 Hodnota osobních údajů

Základem úspěchu každé společnosti v současném digitalizovaném světě je schopnost efektivně zpracovávat informace a data, včetně jejich kvalitního zabezpečení [5]. Nové předpisy vyžadují společnou a nerozdílnou odpovědnost. Staré čínské přísloví praví: „*Co nemá cenu, nemá ani hodnotu*.“ Reálná hodnota osobních údajů se objevila teprve nedávno. Kybernetická bezpečnost je jedním z klíčových úkolů budoucnosti, protože krádež osobních údajů vystavuje občany EU významným rizikům [5].

3.9 Zabezpečení osobních údajů

Správce musí přijmout s ohledem na povahu, rozsah a účely zpracování technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Obecným nařízením. Jedním z prvků zabezpečení osobních údajů je např. jejich pseudonymizace nebo šifrování. Tyto prvky však nejsou povinné [5].

3.9.1 Hlášení správce při bezpečnostním incidentu ÚOOÚ

Pokud dojde k porušení zabezpečení osobních údajů, musí správce toto porušení bez zbytného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásit dozornému úřadu (Úřadu pro ochranu osobních údajů). Právě používání pseudonymizace či šifrování může případné riziko zcela eliminovat, a tudíž i zbavit správce nutnosti případ ohlásit dozorovému úřadu. Vždy je však nutné míru rizika posoudit [5].

3.9.2 Určení rizika porušení bezpečnosti

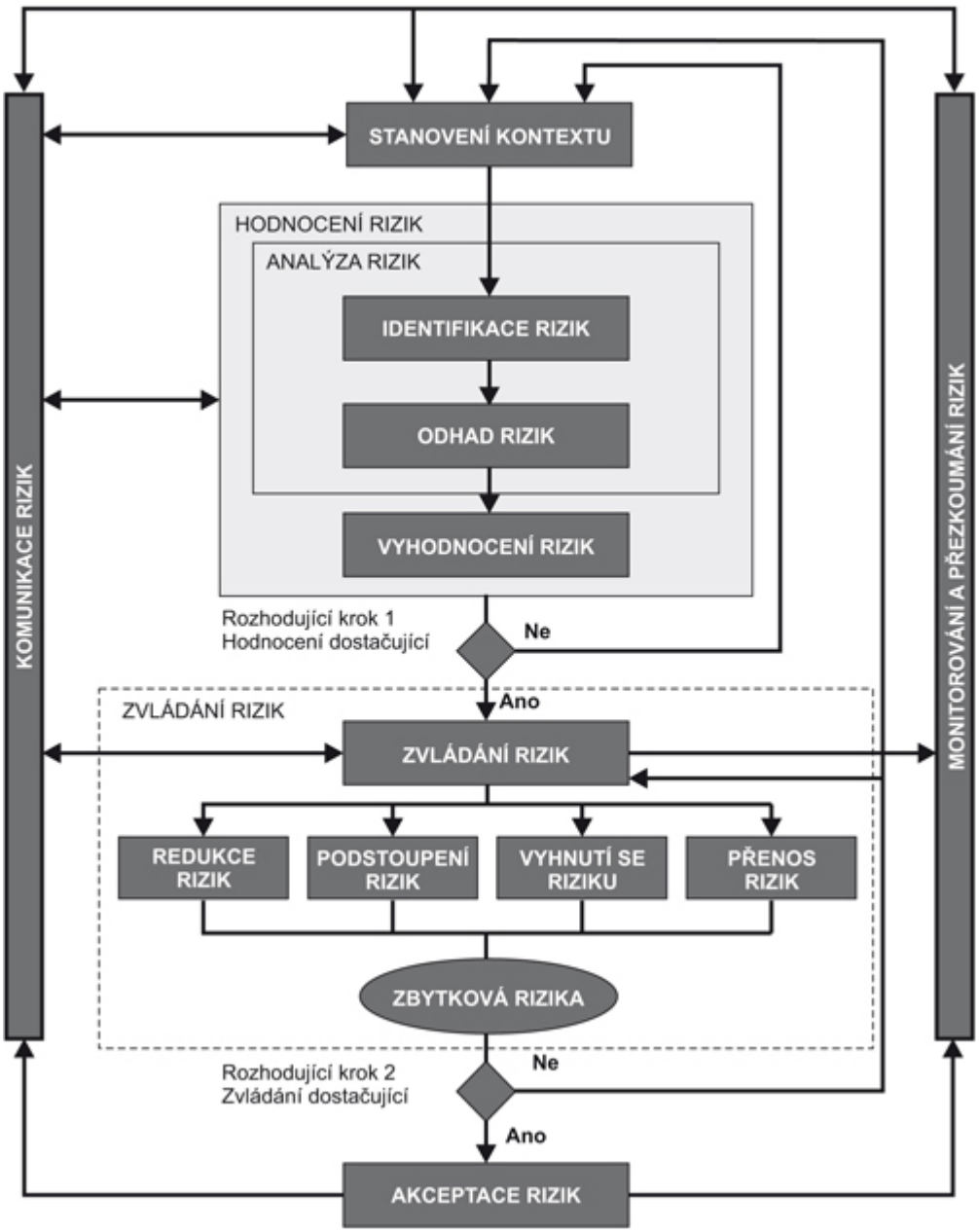
Při určování rizika porušení zabezpečení bude nutné vycházet zejména z kategorie osobních údajů, které byly porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtu dotčených subjektů údajů [5].

3.10 Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů musí být jmenován na základě svých profesních kvalit, zejména na základě svých odborných znalostí práva a praxe v oblasti ochrany údajů [10]. Hlavním úkolem pověřence je především být nápomocný správcům, dosáhnout souladu zpracování osobních údajů a tím chránit i práva a svobody subjektu údajů u rizikovějších zpracování, jelikož povinnost jej jmenovat je omezena pouze pro některé správce, v souladu s přístupem založeným na riziku [1]. Pověřenec pro ochranu osobních údajů může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb [10]. Školy mají povinnost jmenovat pověřence pro ochranu osobních údajů. Tato povinnost jim vyplývá z obecného nařízení GDPR, protože vystupují jako veřejný subjekt. Za veřejný subjekt se ve smyslu GDPR přitom považuje orgán zřízený zákonem nebo na základě zákona v oblasti práva veřejného, který plní zákonem stanovené úkoly ve veřejném zájmu. Veřejné školy musí mít svého pověřence pro ochranu osobních údajů [11].

4 POJMY V OBLASTI ŘÍZENÍ RIZIK

Řízení rizik je oblast řízení zaměřující se na analýzu a snížení rizika, pomocí různých metod a technik prevence rizik, které eliminují nebo odhalují budoucí faktory zvyšující riziko. Riziko je všudy přítomným a charakteristickým průvodním jevem fungování organizací v soudobém turbulentním prostředí [12].



Obrázek 2: Proces managementu rizik [13]

V obecné rovině lze stanovit šest kroků k řízení rizik:

1. Stanovení souvislostí,
2. Identifikace rizik,
3. Analýza rizik,
4. Hodnocení rizik,
5. Řízení rizik,
6. Kontrola [14].

Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů a naopak umožňují využít příležitosti působení pozitivních vlivů. Součástí procesu řízení rizik je rozhodovací proces, vycházející z analýzy rizika. Po zvážení dalších faktorů, zejména ekonomických, technických, ale i sociálních a politických, se management pro řízení rizik vyvíjí, analyzuje a srovnává možná preventivní a regulační opatření. Posléze z nich vybere ta, která existující riziko minimalizují [15].

Řízení rizik je součástí managementu rizik stejně jako analýza rizik a hodnocení rizik. Management rizik je důležitou oblastí manažerských dovedností a znalostí. Podcenění managementu rizik může vést k finančním ztrátám pro organizaci. Řízení rizik a management rizik spolu vzájemně souvisí.

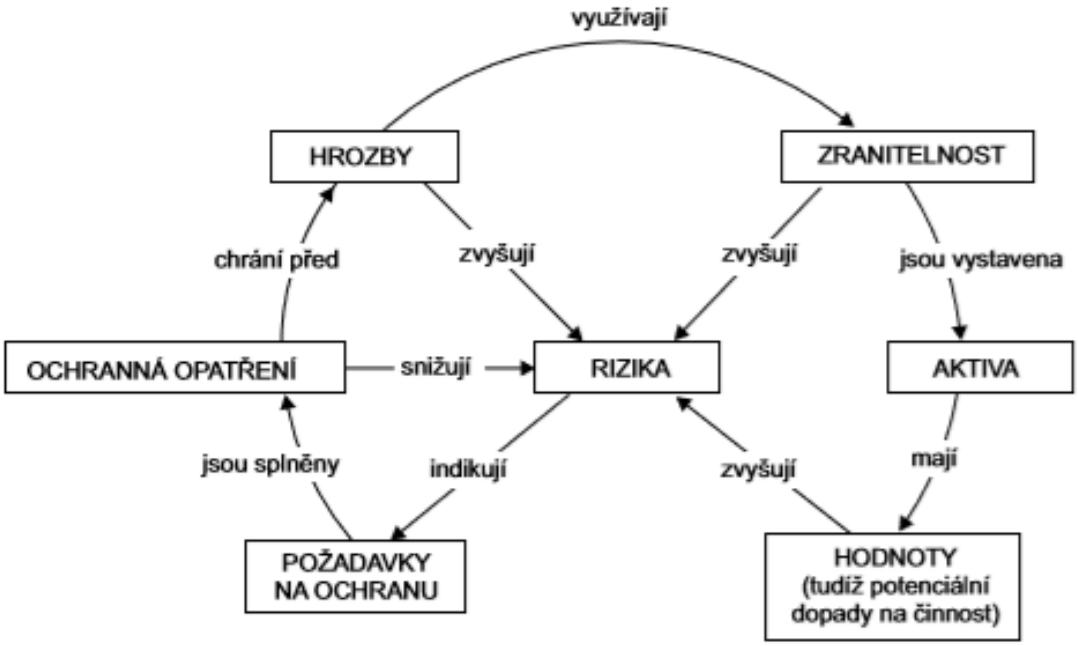
Riziko

Riziko je často chápáno jako nebezpečí vzniku určité ztráty [15].

Riziko pro ochranu osobních údajů

Úroveň rizika se stanoví na základě závažnosti a pravděpodobnosti:

- Závažnost možného následku představuje míru významu rizika. V zásadě závisí na míře negativních účinků možných dopadů.
- Pravděpodobnost vzniku nebezpečné situace ohrožení představuje míru možností vzniku rizika. V zásadě závisí na míře zranitelnosti podpůrných aktiv čelících ohrožení a úroveň schopností zdrojů rizik aktiva zneužít [5].



Obrázek 3: Vztahy při řízení rizik [15]

Proces

Proces je sled činností, které na sebe vzájemně navazují, vytvářejí tok práce postupující od jednoho člověka k druhému a tvoří hodnotu. Každý proces má nějaké vstupy, nějaké výstupy a spotřebovává nějaké zdroje. Každá proces je spuštěn nějakou událostí. Procesy tedy rozhodně musí být nějak nastavené a musí být nějak řízené, aby nezavládl úplný chaos [16].

4.1 Základní pojmy analýzy rizik

Při analýze rizik je nezbytné znát obsahovou náplň pojmů se kterými pracujeme. Mezi základní pojmy patří:

4.1.1 Aktivum

Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí na hmotná a na nehmotná [15].

4.1.2 Hrozba

Hrozba je libovolný subjekt, jenž svým působením (činností) může poškodit nebo zničit konkrétní chráněnou hodnotu nebo zájem jiného subjektu [17].

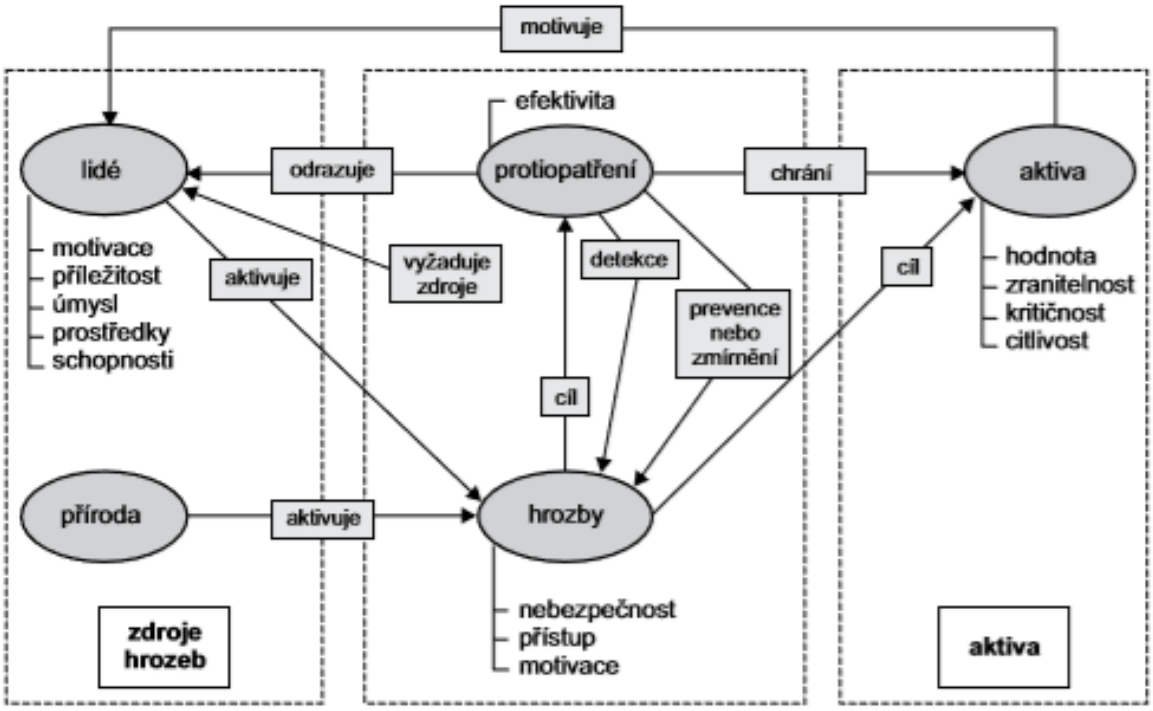
Hrozby mohou být přírodního nebo lidského původu a mohou být náhodné nebo úmyslné. Mohou pocházet zevnitř i zvenčí organizace [15].

4.1.3 Zranitelnost

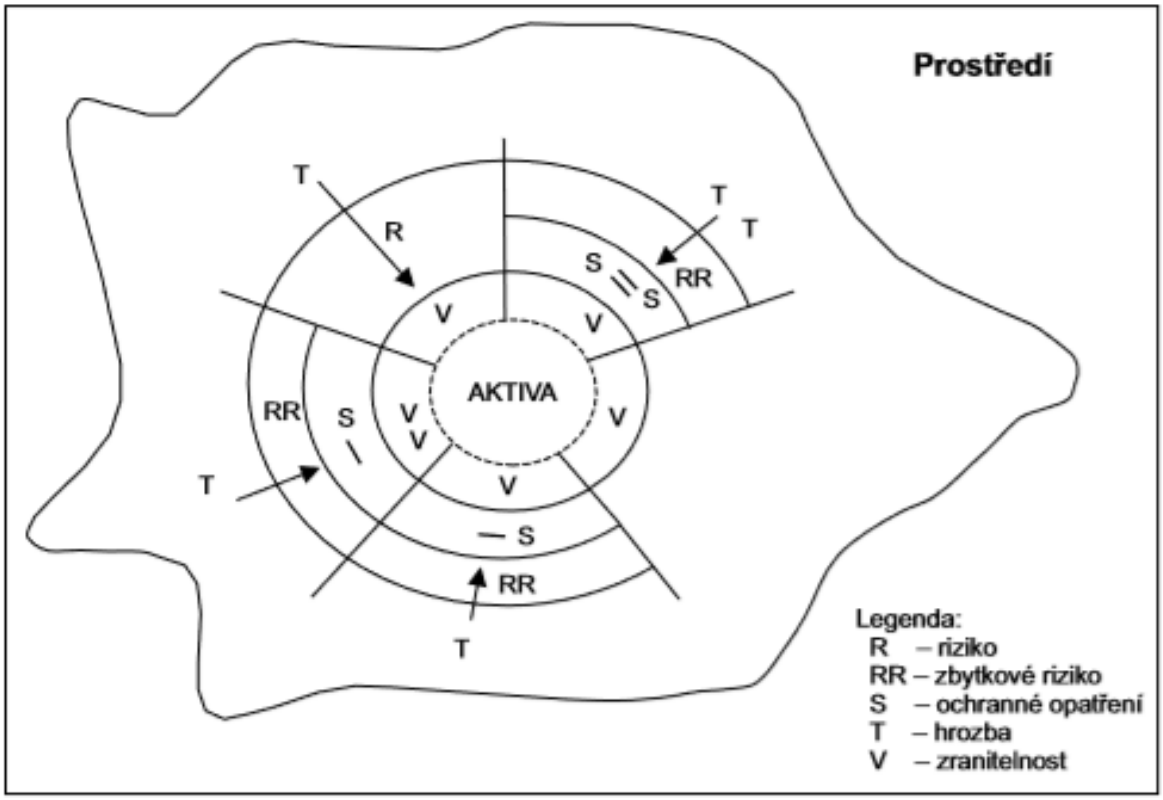
Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva, který může hrozba využít pro uplatnění svého nežádoucího vlivu [15].

4.1.4 Protiopatření

Protiopatření je postup, proces, procedura, technický prostředek nebo cokoli, co bylo speciálně navrženo pro zmírnění působení hrozby, snížení zranitelnosti nebo dopadu hrozby [15].



Obrázek 4: Analýza rizik dle základních vztahů a souvislostí [15]



Obrázek 5: Vztahy při analýze rizik dle jednotlivých prvků analýzy [15]

4.2 Metody analýzy rizik

Způsob vyjádření veličin, s nimiž se v analýze rizik pracuje, lze použít jako základní hledisko pro rozdělení těchto metod. Existují přitom dva základní přístupy k jejímu řešení: kvantitativní a kvalitativní metody vyjádření veličin analýzy rizik. V analýze rizik se používá buď jeden z těchto dvou přístupů, nebo jejich kombinace [15].

Kvalitativní metody jsou postaveny na popisu závažnosti potenciálního dopadu a na pravděpodobnosti, že daná událost nastane [15].

Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Používají číselné ocenění jak v případě pravděpodobnosti vzniku události (či lépe řečeno incidentu), tak i při ocenění dopadu dané události [15].

Kombinované metody vycházejí z číselných údajů. Cíl je však díky kvalitativnímu hodnocení ve větším přiblížení se realitě oproti předpokladům, ze kterých vycházejí kvantitativní metody. Je ovšem třeba mít na zřeteli, že údaje použité v kvalitativních metodách nemusí vždy odrážet přímo pravděpodobnost události či výši jejího dopadu, ale mohou být ovlivněny měřítkem stupnice, která je v konkrétní metodě použita [15].

Každý proces má svoje výhody a nevýhody. Východiskem pro zvolení optimálního přístupu je porovnání reálného stavu analyzovaného prostředí s výhodami či úskalími, které s sebou vybraná metoda přinese. Rozhodnutí, který přístup je pro daný objekt vhodný, závisí zejména na následujících skutečnostech:

1. jakých cílů má být použitím analýzy rizik dosaženo,

2. k jakým účelům objekt slouží,

3. jaká je hodnota aktiv spojených s objektem,

4. zda jsou funkce, které objekt poskytuje, kritické a pro koho,

5. jaká je úroveň investic do objektu a jaká je výše nákladů na obnovení jeho funkčnosti [15].

II. PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA VYBRANÉ ORGANIZACE

Kapitola bude zaměřena na analýzu organizace, která byla vybrána ke zmapovaní řízení procesů v rozsahu obecného nařízení GDPR. V první řadě je nezbytné zmínit historii a vznik organizace. Následně se uvedou základní údaje o organizaci, organizační struktuře a celkovém fungování organizace, včetně hospodaření. Analýza organizace je důležitá z hlediska pochopení fungování organizace jako celku.

5.1 Historie organizace

Vybraná organizace XY vznikla 1. 1. 2003. Jedná se o příspěvkovou organizaci – mateřskou školu. Tato organizace je právním subjektem. Je zapsaná do školského rejstříku na základě rozhodnutí krajského úřadu - odboru školství, mládeže a tělovýchovy. Dále je zapsaná v obchodním rejstříku vedeném u krajského soudu. Zřizovatelem organizace je obec.

5.2 Základní údaje o organizaci

Organizace svoji činnost řídí zákonem č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů. Část druhá a § 33 tohoto zákona nám definují cíle předškolní vzdělávání.

Předškolní vzdělávání podporuje rozvoj osobnosti dítěte předškolního věku, podílí se na jeho zdravém citovém, rozumovém a tělesném rozvoji a na osvojení základních pravidel chování, základních životních hodnot a mezilidských vztahů. Předškolní vzdělávání vytváří základní předpoklady pro pokračování ve vzdělávání. Předškolní vzdělávání napomáhá vyrovnávat nerovnoměrnosti vývoje dětí před vstupem do základního vzdělávání a poskytuje speciálně pedagogickou péči dětem se speciálními vzdělávacími potřebami [18].

Organizaci metodicky řídí Ministerstvo školství, mládeže a tělovýchovy. Činnost organizace je financována z prostředků zřizovatele, tedy obce a ze státního rozpočtu prostřednictvím krajského úřadu.

5.2.1 Organizační řád organizace

Organizační řád příspěvkové organizace upravuje její postavení, působnost a členění (s přihlédnutím k místním provozním podmínkám). Je základní normou školy ve smyslu zákona č. 561/2004 Sb., školského zákona o předškolním, základním, středním, vyšším odborném

a jiném vzdělávání (dále jen školský zákon), zákona č. 563/2004 Sb., o pedagogických pracovnících, zákona č. 262/2006 Sb., zákoníku práce, zákona č. 106/1999 Sb., o svobodném přístupu k informacím, zákona č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů a vyhlášky č. 14/2005 ve znění vyhlášky č. 43/2006 o mateřských školách [19].

Organizační struktura:

- ředitelka školy,
- učitelka mateřské školy,
- školnice, osoba vydávající stravu,
- chůva pro děti 2 – 3leté,
- asistent pedagoga.

Organizaci tvoří tři úseky:

- výchovně vzdělávací úsek,
- provozní úsek,
- stravovací úsek.

Činnost organizace se řídí vnitřními organizačními a řídícími normami:

- Odpisový plán,
- Oběh účetních dokladů,
- O zabezpečení zákona o finanční kontrole,
- O účetnictví,
- Provedení inventarizace majetku a závazků,
- O účtování a oceňování dlouhodobého majetku,
- Předpis pro stanovení rozpočtu FKSP,
- Vnitřní platový předpis,
- O školním a závodním stravování,
- Směrnice k čerpání dovolené,
- Úplata za předškolní vzdělávání,
- Cestovní náhrady,
- Provozní řád venkovních hracích ploch,
- Primární prevence sociálně patologických jevů dětí v mateřské škole,
- Vnitřní řád školní výdejny stravy,
- Provozní řád MŠ XY,
- Organizační řád MŠ XY,

- Školní řád,
- Směrnice o ochraně osobních údajů,
- Archivní a skartační řád.

Vnitřní kontrolní systém vychází z ustanovení zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění a jeho cílem je kontrola dodržování právních předpisů při hospodaření s veřejnými prostředky. Rovněž je nutné zajistit ochranu těchto prostředků proti rizikům jež mohou vzniknout nedodržováním předpisů.

5.2.2 Organizační členění

Mateřská škola vznikla jako samostatný právní subjekt a má 1 třídu. K budově patří přilehlá školní zahrada s pískovištěm, dřevěným domečkem na hračky, herními sestavami, přírodními koutky, dřevěnými stoly a lavicemi, které umožňují herní, vzdělávací i pohybové aktivity dětí po celý rok [20].

Budova je jednopatrová. V patře je obecní byt a prostory pro uskladnění školních pomůcek a sušení prádla. Mateřská škola se nachází v přízemí. Je tvořena šatnou dětí a zaměstnanců, velkou třídou, sociálním zařízením, jídelnou, ložnicí a kanceláří paní ředitelky. Jednotlivé místnosti jsou stavebně odděleny. Mateřská škola nemá vlastní jídelnu. Je zde pouze výdejna stravy. Strava je dovážena z jiné školy. Děti nejsou pouze místní, ale dojíždí z okolních vsí a blízkého města [20].

Mateřská škola má celodenní provoz od 6.30 do 16.00 hodin. Do mateřské školy dochází 22 dětí. Kapacita školky je 28 dětí.

Chod školky zajišťují pedagogičtí a nepedagogičtí pracovníci, viz Tabulka 1:

Tabulka 1: Počet pracovníků

Pedagogičtí pracovníci			
Pracovní zařazení	Počet	Vzdělání	Úvazek
ředitelka	1	vysokoškolské - stupeň 2	1
učitelka	1	vysokoškolské - stupeň 1	1
Nepedagogičtí pracovníci			
Pracovní zařazení	Počet	Vzdělání	Úvazek
školnice	1	středoškolské	0,65
výdejna stravy	1	středoškolské	0,35
chůva	1	vysokoškolské - stupeň 2	0,5
asistent pedagoga	1	vysokoškolské - stupeň 2	0,5

5.2.3 Výchova a vzdělávání dětí

Zápis dětí probíhá na základě informačních letáků a plakátu v prostorách školky. Dále mateřská škola využívá internetové stránky, které jsou součástí webových stránek zřizující obce.

Kritéria pro přijímání dětí k předškolnímu vzdělávání:

- trvalý pobyt dítěte (přednost děti místní),
- datum narození (dřívější narození),
- typ docházky (celodenní docházka),
- sourozenec v mateřské škole,
- poslední rok před zahájením povinné školní docházky,
- dítě s odkladem povinné školní docházky.

5.2.4 Školní vzdělávací program

Předškolní vzdělávání je realizováno podle školního vzdělávacího programu (dále jen ŠVP), který byl vypracován 1. září 2016, zpracovaný v souladu se zásadami Rámcově vzdělávacího programu pro předškolní vzdělávání. Nedílnou součástí ŠVP je Program primární prevence rizikového chování u dětí mateřské školy [19].

Dále je součástí i Primární prevence sociálně patologických jevů u dětí v mateřské škole. K posouzení této problematiky slouží mimo jiné rozhovory s dětmi a jejich zákonnými zástupci, dotazníky pro rodiče. Konkrétní případy, který by se mohly vyskytnout se předávají k řešení MěÚ, Polici ČR.

Rodiče mají možnost seznámit se s informačním materiálem „Desatero pro rodiče“, který dává rodičům možnost získat informace o dovednostech, schopnostech a znalostech, které by dítě mělo dosáhnout před vstupem do ZŠ [19].

Dále mají k dispozici metodický materiál „Kolektivní logopedické chvilky“, který informuje rodiče, jak mohou přispět ke gymnastice mluvidel dětí a tím i lepší výslovnosti [19].

Děti se účastní výuky plavání, kurzu bruslení na zimním stadionu, výuky anglického jazyka.

5.3 Rozpočet organizace

Mateřská škola XY hospodaří na základě rozpočtu. Rozpočet organizace tvoří příspěvek na provoz od zřizovatele, kterým je obec XY. Další část rozpočtu tvoří příjmy na přímé náklady, což jsou platy, povinné odvody – sociální, zdravotní pojištění a fond kulturních a sociálních potřeb, ostatní neinvestiční výdaje. Tyto prostředky jsou organizaci přerozdělovány krajským úřadem na základě počtu dětí a úvazků zaměstnanců. Mateřská škola má povinnost svůj rozpočet zveřejňovat. Návrh rozpočtu je předložen obci a ta jej schválí, či nikoli. Pokud rozpočet není schválen, je nutné provést úpravy dle požadavků obou stran. Po vzájemné dohodě mateřské školy a obce je vypracován návrh rozpočtu a vyvěšen minimálně 15 dnů před projednáváním v zastupitelstvu obce. Po schválení zastupitelstvem obce je rozpočet pro organizaci závazný. Je vyvěšen na stránkách obce, pokud mateřská škola nemá své vlastní webové stránky.

Tabulka 2: Rozpočet Mateřské školy XY na rok 2019 [21]

Položka rozpočtu	**Hlavní činnost**	
	Návrh rozpočtu na rok 2019	Schválený rozpočet na rok 2019
Výnosy celkem (účt. třída 6)	1 440 000,00 Kč	1 440 000,00 Kč
Náklady celkem (účt. třída 5)	1 440 000,00 Kč	1 440 000,00 Kč

6 ANALÝZA PROCESŮ V ORGANIZACI

Mateřská škola XY je organizací určenou k předškolnímu vzdělávání. Tím pádem jednotlivé procesy souvisí s touto činností. Organizace se při své činnosti řídí školním řádem.

Všechny děti mají právo na rovný přístup ke vzdělávání bez ohledu na etnickou, náboženskou příslušnost a úroveň schopností. Všechny děti mají právo na toleranci a akceptaci individuálních rozdílů, zprostředkování rozdílů, zprostředkování poznání vlastního kulturního zakotvení a porozumění, spravedlnost a solidaritu [22].

Zde jsou popsány jednotlivé procesy organizace.

6.1 Výkon práv a povinností dětí a jejich zákonných zástupců

Mateřská škola podporuje vývoj dětí jak po psychické stránce, tak tělesné a sociální. Vyvíjí aktivity k rozvoji dítěte předškolního věku. Spolupracuje s rodiči, kteří se aktivně podílí na procesu vzdělávání.

Zajišťuje diskrétnost a ochranu informací, týkajících se jejich osobního a rodinného života [22].

Rodiče mají povinnost předávat dítě učitelce osobně, hlásit změny osobních údajů i osobních dat dítěte. Posílat dítě do školky vhodně oblečené. Dbát na zdraví dítěte. Platit úhradu za předškolní vzdělávání.

Samozřejmě své povinnosti si musí plnit i pedagogičtí zaměstnanci. Starat se o zdravý vývoj dětí a zabránit zneužití jejich osobních údajů a údajů o jejich zákonných zástupcích. Dodržovat předpisy BOZP, PO a hygieny.

6.2 Přijímací řízení

Do mateřské školy jsou přijímány děti ve věku od 3 do 6 let. Mohou být přijímány i děti ve věku dvou let. Předškolní vzdělávání je povinné. Děti jsou přijímány do školky na základě zápisu. Rodiče vyplní přihlášku, doloží potvrzení od lékaře a očkovací průkaz. Ředitelka rozhodne o přijetí dítěte písemným rozhodnutím. Děti jsou vedeny pod registračními čísly. Po obdržení rozhodnutí se rodiče dostaví do mateřské školy, aby poskytli informace do školské matriky.

6.3 Povinné předškolní vzdělávání

Předškolní vzdělávání se týká dětí, které dosáhly pátého roku před započetím školního roku. Pokud nepřihlásí zákonný zástupce dítě k povinnému školnímu vzdělávání, dopustí se přestupku podle § 182 a školského zákona [22]. Nepřítomnost dítěte omlouvají zákonní zástupci. Je dobré uvést i důvod nepřítomnosti dítěte. Učitelka vede knihu docházky.

6.4 Individuální vzdělávání dítěte

Pokud se zákonný zástupce rozhodne pro individuální vzdělávání dítěte musí tuto skutečnost oznámit ve spádové mateřské škole. Tuto informaci podává písemně formou oznámení. Tento doklad musí obsahovat osobní údaje dítěte, jako jsou jméno, příjmení, datum narození, rodné číslo, adresu trvalého pobytu a důvody individuálního vzdělávání

6.5 Vzdělávání dětí se speciálními potřebami

Vzdělávání dětí se speciálními potřebami řeší podpůrná opatření. Tato opatření se odvíjí od potřeb dítěte. Podpůrná opatření se člení do pěti stupňů.

Podpůrná opatření prvního stupně uplatňuje škola i bez doporučení školského zařízení na základě plánu pedagogické podpory. Podpůrná opatření druhého až pátého stupně uplatňuje s doporučením školského poradenského zařízení (pedagogicko-psychologická poradna) [22].

6.6 Vzdělávání dětí mladších tří let

Mateřská škola má prostory, materiální, hygienické a bezpečnostní podmínky i pro tyto děti mladší tří let.

6.7 Provoz a vnitřní režim organizace

Mateřská škola XY má tři ročníky. Vzdělávají se zde děti od tří, potažmo dvou let do šesti. Tyto děti jsou v jedné třídě. Chod organizace je omezen jen v době prázdnin. Za zdravotní stav dětí odpovídají jejich zástupci. Organizace zajišťuje pro děti stravování, které je dováženo ze školní jídelny z nedaleké obce XY. Pro potřeby školní jídelny je nezbytné vyhotovovat měsíčně seznam dětí, které jídlo odebírají. Zde je uvedeno jméno a příjmení dítěte, počet obědů v měsíci a výše úhrady za obědy.

Podle zákona č. 561/2004 Sb., a podle vyhlášky č. 35/2006 Sb., o předškolním vzdělávání v platném znění je stanovena úplata za předškolní vzdělávání, tzv. školné [22].

Školné je vybíráno na základě předpisných seznamů, kde je uvedeno jméno a příjmení dítěte a výše úhrady. Tyto seznamy slouží pro samotný výběr pokladníkem školky a posléze účetní organizace k zaúčtování. Účetní organizace má přístup nejen k osobním údajům dětí, ale i k osobním údajům zaměstnanců mateřské školy. Tyto údaje slouží pro mzdovou agendu.

6.8 Podmínky zajištění bezpečnosti a ochrany zdraví dětí

Organizace musí zajišťovat podmínky pro bezpečnost dětí, zaměstnanců ale i rodičů. Musí vést agendu o úrazech. Apelovat na rodiče, aby vedli děti k poslušnosti a ukázněnosti. Při výskytu vší mít zájem o to, aby se onemocnění nerozšiřovalo na další děti. Je důležité vést děti k bezpečnému chování.

Škola musí dbát i na bezpečnost dětí tím, že zamezí nepovolaným osobám vstup do prostor mateřské školy. Zabezpečí vstupy do prostor tak, aby nebylo možné se zde dostat nepozorovaně. A děti seznamuje s pojmem nebezpečí a s riziky ohrožení života a zdraví. Mezi nebezpečné jevy patří mimo jiné šikana, diskriminace, nepřátelství, násilí.

6.9 Podmínky zacházení s majetkem školy

Škola se snaží zabránit tomu, aby docházelo k svévolnému ničení majetku, ať již dětmi nebo rodiči.

6.10 Pravidla pro uchovávání dokumentů

Mateřská škola má svůj archivační a skartační řád. Veškeré dokumenty musí být archivovány po zákonem stanovenou dobu.

Ve vazbě na potřebu zajištění řádné funkce systému pro záznam a uchování účetních záznamů pro každou činnost je stanovený termín, po kterou musí být originální dokumenty k dispozici kontrolním orgánům [23].

7 ANALÝZA SOUČASNÉHO STAVU OCHRANY OSOBNÍCH ÚDAJŮ V MATEŘSKÉ ŠKOLE XY

Škola či školské zařízení obvykle zpracovává především osobní údaje učitelů, žáků, rodičů žáků a dalších zákonných zástupců nebo dokonce třetích osob (babička, dědeček, teta, chůva, sousedka) [24].

Mateřská škola musí analyzovat, jakým způsobem nakládá s osobními údaji, jaké údaje zpracovává, k jakým účelům a na základě jakého právního důvodu.

Pro přípravu revize osobních údajů, stanovení účelu jejího zpracování, analýzu procesů a analýzu rizik je potřebné si připravit následující informace a podklady [25]:

- dokumenty v listinné i elektronické podobě, které obsahují osobní údaje fyzických, osob, včetně pracovníků, kteří s nimi pracují,
- souhlasy se zpracováním osobních údajů,
- smlouvy, včetně pracovních smluv, smluv s dodavateli softwaru, externími správci informačních systémů,
- faktury a licenční smlouvy vážící se k licencím provozovaných SW produktů,
- vnitřní předpisy, směrnice a nařízení [25].

7.1 Identifikace rizik

Na základě předložených dokladů byla řešena identifikace rizik, které mohou vzniknout při činnosti organizace. Do následujících tabulek jsou vybrány ty oblasti, které nejvíce souvisí s bezpečností a ochranou osobních údajů.

Tabulka 3: Zabezpečení mateřské školy

Zabezpečení mateřské školy	
Dokument	Klíče
Účel zpracování	Zabezpečení prostor mateřské školy
Údaje	Název místnosti, jméno, příjmení
Příjemce	Ředitelka mateřské školy
Zákon	Organizačně technické opatření
Komnetář	Od všech uzamykatelných prostor, včetně trezoru a skříní existují dva klíče, jeden používá ředitelka mateřské školy a jeden je uložen v archivu

Zabezpečení mateřské školy XY a to především klíčový režim. Vstupy do budovy, do kanceláří, třídy, lehárny. Zde je nutné zajistit seznam klíčů, osob, které s klíči nakládají a mají k nim přístup. Zhotovení rezervních klíčů a jejich uložení a uzamčení v trezoru.

Tabulka 4: Účetnictví

Účetnictví	
Dokument	Účetní doklady
Účel zpracování	Ekonomické agendy
Údaje	Jméno, příjmení, adresa
Příjemce	Dodavatel, odběratel
Zákon	Zákon č. 563/1991 Sb., o účetnictví
Komentář	Všechny účetní doklady jsou evidovány v šanonech, které jsou uloženy ve skříni účtárny. Od místnosti má klíče účetní. V elektronické podobě jsou uloženy v účetním programu firmy Gordic pod heslem. Do programu má přístup pouze účetní.

Účetnictví organizace obsahující účetní a mzdové doklady. Nakládání s těmito doklady, zabezpečení kanceláří, skříní, počítače. Zároveň by měl být zabezpečen účetní a mzdový software.

Tabulka 5: Smlouvy

Smlouvy	
Dokument	Smlouva
Účel zpracování	Plnění smluv, archivace
Údaje	Jméno, příjmení, adresa, datum narození, rodné číslo
Příjemce	Smluvní strana
Zákon	Zákon č. 561/2004 Sb., školský zákon, Zákon č.
	262/20016 Sb., zákoník práce, Zákon č. 89/2012 Sb., občanský zákoník, zákon č. 499/2004 Sb., o archivnictví a spisové službě
Komentář	Originály smluv jsou u účetní v uzamykatelné skříni. Jedná se o pracovní smlouvy, dohody o provedení práce, darovací smlouvy, smlouvy o poskytnutí dotací. Kopie smluv jsou uloženy u ředitelky školy v uzamykatelné skříni V elektronické podobě jsou uloženy v programu na zpracování mzdové agendy firmy Gordic pod heslem. Do programu má přístup pouze účetní.

Archivace smluv a přístup k nim. Jedná se především o smlouvy pracovní, včetně dohod o provedení práce, smlouvy o dotacích, smlouvy s dodavateli. Tyto dokumenty musí být v uzamčené skříní. Přístup by k nim měla mít jen účetní organizace.

Tabulka 6: Vystavená rozhodnutí

Vystavená rozhodnutí	
Dokument	Žádosti, stížnosti, rozhodnutí
Účel zpracování	Rozhodování mateřské školy
Údaje	Jméno, příjmení, adresa, datum narození
Příjemce	Žadatel
Zákon	Zákon č. 500/2004 Sb., správní řád
Komentář	V listinné podobě vedeny u ředitelky školy v uzamykatelné skříni. Evidence v podacím deníku. Uložení v šanonech.

Vystavená rozhodnutí mateřské školy o přijetí či nepřijetí dětí. Tyto dokumenty spadají přímo pod ředitelku mateřské školy. Zamezení přístupu neoprávněných osob, uzamčení ve skříni, zaheslování počítače.

Tabulka 7: Školní matrika

Školní matrika	
Dokument	Přihlášky dětí, evidenční karty, lékařské záznamy,
Účel zpracování	Školní matrika
Údaje	Jméno, příjmení, bydliště, datum narození, rodné číslo, údaje dětí i zákonných zástupců, omezení, speciální potřeby
Příjemce	ředitelka, učitelky
Zákon	Zákon č. 561/2004 Sb., školský zákon
Komentář	V listinné podobě vedeny u ředitelky školy v uzamykatelné skříni. Uložení v šanonech. Vedení třídní knihy v listinné podobě, uložena v uzamykatelné skříni.

Školní matrika je nejdůležitější oblastí práce s osobními údaji a zde hrozí velké riziko zneužití dat nepovolanými osobami. Uchování v šanonech v uzamčené skříní, zaheslování PC.

Tabulka 8: Správa adresářů

Správa adresářů	
Dokument	Adresáře
Účel zpracování	Pro komunikaci s rodiči
Údaje	Jméno, příjmení, adresa, e-mail, telefon
Příjemce	ředitelka
Zákon	
Komentář	Adresáře jsou v listinné podobě v šanonu v uzamykatelné skříni. Dále jsou vedeny v počítači ředitelky v programu exel a jsou chráněny heslem.

Správa adresářů obsahující údaje o jménech, adresách, telefonních číslech, e-mailech osob. Zde hrozí zneužití těchto údajů.

Tabulka 9: Přístup do datové schránky

Přístup do datové schránky	
Dokument	Datová schránka
Účel zpracování	Doručování elektronických dokumentů
Údaje	Jméno, příjmení, adresa, e-mail, telefon
Příjemce	ředitelka, účetní
Zákon	Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
Komentář	Přístup do datové schránky mají ředitelka a účetní. Každá vlastní token s certifikátem. Token je chráněn heslem

Přístup do datové schránky. Datová schránka je zaheslována a neměl by mít do ní nikdo nepovolaný přístup.

Tabulka 10: Kontaktní e-mail mateřské školy

Kontaktní e-mail mateřské školy	
Dokument	Služební e-mail
Účel zpracování	Komunikace s rodiči, se zřizovatelem, městským úřadem, krajským úřadem, dodavateli
Údaje	Jméno, příjmení, e-mailová adresa
Příjemce	ředitelka, účetní
Zákon	
Komentář	Počítače ředitelky i účetní jsou zaheslovány

Kontaktní e-mail mateřské školy může být napaden. E-mail by měl být chráněn heslem.

Tabulka 11: Webové stránky mateřské školy

Webové stránky mateřské školy	
Dokument	Webové stránky
Účel zpracování	Propagace mateřské školy, dokumenty školy, informace pro rodiče
Údaje	Jméno, příjmení, fotografie
Příjemce	Veřejnost
Zákon	
Komentář	Na webových stránkách se objevují jméno a příjmení dětí, fotografie z akcí, údaje o narozeninách dítěte

Administrace webových stránek obsahující údaje o jménech dětí, jejich oslavách a rovněž fotografie dětí mohou být díky přístupu k internetu zneužity.

Tabulka 12: Razítka

Razítka	
Dokument	Razítka
Účel zpracování	Evidence dle spisového řádu
Údaje	Jméno, příjmení, číslo razítka
Příjemce	ředitelka
Zákon	Zákon č. 97/1974 Sb., o archivnictví
Komentář	Razítka jsou v uzamykatelné zásuvce psacího stolu v kanceláři ředitelky školy

Uchování razítek organizace a ochrana před zneužitím, by neměla mít až tak velký dopad na ochranu osobních údajů, ale zase mohou být zneužita a poškodit organizaci jako celek.

Tabulka 13: Používání služebního mobilního telefonu

Používání služebního mobilního telefonu	
Dokument	Služební mobilní telefon
Účel zpracování	Komunikace s rodiči, školní jídelnou, zřizovatelem, dodavateli, jinými školami, úřady
Údaje	Jméno, příjmení, telefon
Příjemce	ředitelka, učitelka, školnice, asistentky
Zákon	
Komentář	Služební mobilní telefon používá ředitelka, učitelka, školnice, asistentky

Používání služebního mobilního telefonu a přístup k němu, tady by měla být obezřetnost při sdělování osobních údajů. Přístup do telefonu zabezpečit PINem.

7.2 Analýza rizik

Po provedení identifikace rizik se přistoupí k provedení analýzy rizik. Na základě provedené analýzy bude posouzena rizikovost jednotlivých procesů a navržen další postup. Pro analýzu rizik se byla využita metoda FMEA.

Metoda FMEA (Failure Mode and Effect Analysis), v překladu Analýza možných vad a jejich následků, obvykle se nepřekládá a používá se zkratka FMEA [26].

Jedná se o analytickou techniku, jejímž cílem je identifikovat místa možného vzniku vad nebo poruch v systémech. Vzhledem ke své univerzálnosti nachází uplatnění v řadě oblastí, zejména v oblasti řízení rizik a řízení kvality, či řízení bezpečnosti. Podstatou metody FMEA je systematická identifikace všech možných vad výrobků nebo procesu a jejich důsledků, identifikace kroků zamezení, snížení nebo omezení příčin těchto vad a zdokumentování celého procesu [26].

Metoda FMEA je použita při analýze současného stavu ochrany osobních údajů v mateřské škole XY. Univerzálnost této metody je použitelná i na oblast osobních údajů. Podrobně člení jednotlivé procesy a zjišťuje slabá místa, tato místa ohodnotí, zjistí rizikovost a následně doporučí opatření ke snížení rizika dané oblasti. Při použití této metody se pracuje následujícím způsobem:

- stanoví se proces, který se bude posuzovat,
- určí se možná chyba, ke které může během procesu dojít,
- z toho vyplyne možný důsledek, který chyba způsobila,
- určí se příčina chyby,
- zaměří se na kontrolu a prevenci, zda byla dostatečná,
- číselně se ohodnotí význam, vznik a odhalení chyby,
- vyhodnotí se možné riziko,
- doporučí opatření,
- určí se odpovědná osoba za nápravu a termín do kterého bude náprava provedena,
- po provedených opatřeních se opět ohodnotí význam, vznik a odhalení chyby,
- spočítá se možné riziko.

Postup při oceňování vad metodou FMEA

Tabulka 14: Význam vady v procesu [27]

Důsledek	**Kritéria:** **Závažnost důsledku ve vztahu k procesu**	**Známka hodnocení**
Nesplnění bezpečnostních požadavků a předpisů	Možný způsob poruchy, který bez varování znamená nesoulad s právními předpisy	10
	Možný způsob poruchy, který i s varováním znamená nesoulad s právními předpisy	9
Ztráta nebo zhoršení primární funkce	Ztráta primární funkce	8
	Zhoršení primární funkce	7
Ztráta nebo zhoršení sekundární funkce	Ztráta sekundární funkce	6
	Zhoršení sekundární funkce	5
Nepříjemnost	Nesoulad zřejmý	4
	Nesoulad méně zřejmý	3
	Nesoulad zanedbatelný	2
Žádný důsledek	Žádný znatelný důsledek	1

Význam je hodnota spojovaná s nejvážnějším důsledkem v případě daného způsobu poruchy [27].

Tabulka 15: Výskyt vady v procesu [27]

Pravděpodobnost poruchy procesu	**Kritéria: Vznik příčiny**	**Známka hodnocení**
Velmi velká	Nově zavedené činnosti	10
Velká	Porucha při zavedení nové činosti je v provozních podmínkách nevyhnutelná	9
	Porucha při zavedení nové činosti je v provozních podmínkách pravděpodobná	8
	Porucha při zavedení nové činosti je v provozních podmínkách nejistá	7
Střední	Četné poruchy spojované se zaváděnými činnostmi	6
	Náhodné poruchy spojované se zaváděnými činnostmi	5
	Ojedinělé poruchy spojované se zaváděnými činnostmi	4
Malá	Pouze ojedinělé poruchy spojované s téměř identickými činnostmi	3
	Žádné zjištěné poruchy spojované s téměř identickými činnostmi	2
Velmi malá	Porucha eliminována nástroji prevence	1

Výskyt znamená pravděpodobnost výskytu specifické příčiny/mechanismu, což má za následek způsob poruchy [27].

Tabulka 16: Odhalení poruchy [27]

Pravděpodobnost odhalení	**Kritéria: Pravděpodobnost odhalení**	**Známka hodnocení**
Téměř nemožná	Nelze odhalit, není analyzováno	10
Velmi mizivá	Analýza má malou odhalovací schopnost	9
Mizivá	Ověřování procesů zda jsou vyhovující pro činnost organizace	8
Velmi malá	Ověřování procesů a jejich poruchovost	7
Malá	Ověřování procesů a zhoršování situace	6
Střední	Ověřování částí procesů zda jsou vyhovující pro činnost organizace	5
Středně velká	Ověřování částí procesů a jejich poruchovost	4
Velká	Ověřování částí procesů a zhoršování situace	3
Velmi velká	Analýza má velkou odhalovací schopnost	2
Téměř jistá	Poruchy nemohou nastat z důvodu prevence	1

Doporučeným přístupem pro nástroj řízení odhalení je předpoklad, že se porucha vyskytla, a následné posouzení způsobilostí nástrojů řízení stávajícího návrhu produktu při odhalovaní způsobu poruchy [27].

V následujících tabulkách bude FMEA analýza pro oblasti popsané v kapitole 7.1:

Tabulka 17: Zabezpečení mateřské školy

Název FMEA	**Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**	**Datum konání FMEA**	17.02.2019
Předmět FMEA	Zabezpečení mateřské školy		
	Klíče		
FMEA Tým	Marcela Králová		

Proces	**Možná chyba**	**Možný důsledek**	**Příčina**	**Kontrola, preventivní opatření**	**Význam**	**Vznik**	**Odhalení**	**Možné riziko**	**Doporučená opatření**	**Odpovědnost**	**Termín**	**Provedená opatření**	**Význam**	**Výskyt**	**Odhalení**	**Možné riziko**	**Stav**
Zabezpečení budovy mateřské školy	Neuzamčení budovy	Vstup neoprávněných osob do budovy	Podcenění bezpečnostních opatření	Kontrola přístupu ke klíčům	10	7	3	210	Vytvořit písemný seznam klíčů a osob, kterým byly klíče vydány, pravidelná kontrola dveří	ředitelka, školnice, učitelka	II/19	Vytvořen nový seznam klíčů. Seznam osob, kterým byly vydány. Uložení náhradních klíčů v trezoru.	4	5	3	60	
	Neuzamčení skříní, trezoru	Přístup k neuzamčeným dokumentům	Nedbalost zaměstnanců	Kontrola přístupu ke klíčům, kontrola uzamykání skříní a trezoru	10	8	3	240	Vytvořit písemný seznam klíčů a osob, kterým byly vydány.	ředitelka, školnice, učitelka	II/19	Vytvořen nový seznam klíčů. Seznam osob, kterým byly vydána. Uložení v trezoru. Proškolení zaměstnanců o bezpečnosti.	4	5	3	60	
	Neuzamčení budovy, skříní, trezoru	Únik osobních údajů, bezpečnost zaměstnanců a dětí	Nedbalost zaměstnanců	Kontrola uzamčení dveří, skříní, trezoru	10	7	3	210	Zavést kamerový systém, zabezpečovací zařízení hlavního vchodu	ředitelka, školnice, učitelka	II/19	Výběrové řízení na dodavatele kamerového systému a zabezpečovacího zařízení	4	5	4	80	

Tabulka 18: Účetnictví

Název FMEA	**Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**	**Datum konání FMEA**	17.02.2019
Předmět FMEA	Účetnictví		
	Účetní doklady		
FMEA Tým	Marcela Králová		

Proces	**Možná chyba**	**Možný důsledek**	**Příčina**	**Kontrola, preventivní opatření**	**Význam**	**Vznik**	**Odhalení**	**Možné riziko**	**Doporučená opatření**	**Odpovědnost**	**Termín**	**Provedená opatření**	**Význam**	**Výskyt**	**Odhalení**	**Možné riziko**	**Stav**
Účetnictví	Neuzamčení kanceláře	Přístup neoprávněné osoby do kanceláře účetní	Podcenění bezpečnostních opatření	Kontrola zamykání kanceláře účetní	10	3	2	60	Poučení zaměstnance o bezpečnosti, pravidelná kontrola dveří	účetní	II/19	Vytvořen nový seznam klíčů. Seznam osob, kterým byly vydány. Zřízení kamerového systému.	3	3	1	9	
	Neuzamčení skříní, neuschování dokladů	Neuschování dokladů v době nepřítomnosti účetní	Nedbalost účetní	Kontrola přístupu ke klíčům, kontrola uzamykání skříní	10	3	2	60	Poučení zaměstnance o ochraně osobních údajů	účetní	II/19	Vytvořen nový seznam klíčů. Seznam osob, kterým byly vydána. Proškolení zaměstnanců o ochraně osobních údajů.	3	3	1	9	
	Neuzamčení skříní, neuschování dokladů	Únik osobních údajů o zaměstnancích a dětech	Nedbalost účetní	Kontrola uzamčení dveří, skříní	10	3	2	60	Poučení zaměstnance o ochraně osobních údajů	Králová	II/19	Proškolení zaměstnanců o ochraně osobních údajů. Možné sankce za porušení ochrany.	3	3	1	9	
	Nezaheslování účetních a mzdových programů	Přístup do počítače účetní	Nedbalost účetní	Servisní návštěvy dodavatele softwaru	10	3	1	30	Pravidelná změna hesla účetních a mzdových programů	účetní	II/19	Prověřit zabezpečení softwaru a zaručení šifrování údajů a anonymizaci	4	3	1	12	

Tabulka 19:Archivace smluv

Název FMEA	**Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**	**Datum konání FMEA**	17.02.2019
Předmět FMEA	Archivace smluv		
	Smlouvy		
FMEA Tým	Marcela Králová		

Proces	Možná chyba	Možný důsledek	Příčina	Kontrola, preventivní opatření	Význam	Vznik	Odhalení	Možné riziko	Doporučená opatření	Odpovědnost	Termín	Provedená opatření	Význam	Výskyt	Odhalení	Možné riziko	Stav
Archivace smluv	Neuzamčení kanceláří	Přístup neoprávněné osoby do kanceláře účetní a kanceláře ředitelky	Podcenění bezpečnostních opatření	Kontrola zamykání kanceláře účetní a ředitelky	10	5	3	150	Poučení zaměstnance o bezpečnosti, pravidelná kontrola dveří	ředitelka, účetní	II/19	Vytvořen nový seznam klíčů. Seznam osob, kterým byly vydány. Zřízení kamerového systému.	3	3	1	9	
	Neuzamčení skříní, neuschování dokladů	Neuschování smluv v době nepřítomnosti účetní a ředitelky	Nedbalost účetní, ředitelky	Kontrola přístupu ke klíčům, kontrola uzamykání skříní	10	5	3	150	Poučení zaměstnance o ochraně osobních údajů	ředitelka, účetní	II/19	Vytvořen nový seznam klíčů. Seznam osob, kterým byly vydána. Proškolení zaměstnanců o ochraně osobních údajů.	3	3	1	9	
	Neuzamčení skříní, neuschování dokladů	Únik osobních údajů o zaměstnanci a dětech	Nedbalost účetní, ředitelky	Kontrola uzamčení dveří, skříní	10	5	3	150	Poučení zaměstnance o ochraně osobních údajů	ředitelka, účetní	II/19	Proškolení zaměstnanců o ochraně osobních údajů. Možné sankce za porušení ochrany.	3	3	1	9	
	Nezaheslování počítače účetní a ředitelky	Přístup do počítače účetní a ředitelky	Nedbalost účetní, ředitelky	Servisní návštěvy smluvního IT pracovníka	10	3	3	90	Pravidelná změna hesla počítače	ředitelka, účetní	II/19	Prověřit zabezpečení softwaru a zaručení šifrování údajů a anonymizaci	4	3	1	12	

Tabulka 20: Vystavená rozhodnutí, školní matrika

Název FMEA	**Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**	**Datum konání FMEA**	17.02.2019
Předmět FMEA	Vystavená rozhodnutí / Školní matrika		
FMEA Tým	Marcela Králová		

Proces	**Možná chyba**	**Možný důsledek**	**Příčina**	**Kontrola, preventivní opatření**	**Význam**	**Vznik**	**Odhalení**	**Možné riziko**	**Doporučená opatření**	**Odpovědnost**	**Termín**	**Provedená opatření**	**Význam**	**Výskyt**	**Odhalení**	**Možné riziko**	**Stav**
Vystavená rozhodnutí	Neuzamčení kanceláří	Přístup neoprávněné osoby do kanceláře ředitelky	Podcenění bezpečnostních opatření	Kontrola zamykání kanceláře ředitelky	10	3	3	90	Poučení ředitelky o bezpečnosti, pravidelná kontrola dveří uzamykání kanceláře	ředitelka	II/19	Seznam klíčů od kanceláře a seznam osob, které k nim mají přístup. Dodržování bezpečnosti a uzamykání dveří.	3	3	1	9	
	Neuzamčení skříní, neuschování rozhodnutí	Neuschování rozhodnutí v době nepřítomnosti ředitelky	Nedbalost ředitelky	Kontrola přístupu ke klíčům, kontrola uzamykání skříní	10	3	3	90	Poučení ředitelky o ochraně osobních údajů	ředitelka	II/19	Kontrola uzamykání skříní. Pořízení programu pro spisovou službu.	3	3	1	9	
Školní matrika	Neuzamčení skříní, neuschování dokladů	Únik osobních údajů o zaměstnancích a dětech, zákonných zástupcích dětí	Nedbalost ředitelky	Kontrola uzamčení dveří, skříní	10	5	4	200	Poučení ředitelky o ochraně osobních údajů	ředitelka	II/19	Proškolení ředitelky i ostatních zaměstnanců o ochraně osobních údajů. Možné sankce za porušení ochrany.	3	4	2	24	
	Nezaheslování počítače ředitelky	Přístup do počítače ředitelky	Nedbalost ředitelky	Servisní návštěvy smluvního IT pracovníka	10	4	4	160	Pravidelná změna hesla počítače	ředitelka	II/19	Prověřit zabezpečení softwaru a zaručení šifrování údajů a anonymizaci	4	3	1	12	

Tabulka 21: Správa adresářů, uskladnění razítek, používání služebního telefonu

Název FMEA	**Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**	**Datum konání FMEA** 17.02.2019	
Předmět FMEA	Správa adresářů, uskladnění razítek Používání služebního telefonu		
FMEA Tým	Marcela Králová		

Proces	**Možná chyba**	**Možný důsledek**	**Příčina**	**Kontrola, preventivní opatření**	**Význam**	**Vznik**	**Odhalení**	**Možné riziko**	**Doporučená opatření**	**Odpovědnost**	**Termín**	**Provedená opatření**	**Význam**	**Výskyt**	**Odhalení**	**Možné riziko**	**Stav**
Správa adresářů	Neuzamčení kanceláře, neuzamčení šuplíků v pracovním stole	Přístup neoprávněné osoby do kanceláře ředitelky	Podcenění bezpečnostních opatření	Kontrola zamykání kanceláře ředitelky, uschování adresářů	9	6	7	378	Poučení ředitelky o bezpečnosti, pravidelná kontrola dveří uzamykání kanceláře	ředitelka	II/19	Seznam klíčů od kanceláře a seznam osob, které k nim mají přístup. Dodržování bezpečnosti a uzamykání dveří. Uzamykání adresářů do šuplíku v psacím stole ředitelky.	5	5	5	125	
	Nezaheslování počítače ředitelky	Přístup do počítače ředitelky	Nedbalost ředitelky, učitelky	Kontrola přístupu ke klíčům, kontrola uzamykání skříní	10	5	3	150	Poučení ředitelky o ochraně osobních údajů	ředitelka, učitelka	II/19	Kontrola uzamykání skříní. Pravidelná změna hesla počítače.	3	3	1	9	
Uskladnění razítek	Neuzamčení kanceláře ředitelky, neuzamčení zásuvky v psacím stole ředitelky.	Přístup nepovolané osoby do kanceláře ředitelky.	Nedbalost ředitelky	Kontrola uzamčení dveří, psacího stolu	9	5	4	180	Seznam razítek. Přidělení čísla razítku. Soupis osob, které je používají.	ředitelka	II/19	Kontrola uzamykání kanceláře a zásuvek v psacím stole ředitelky. Stanovit podmínky manipulace s razítky mateřské školy	4	4	2	32	
Používání služebního telefonu	Ponechání telefonu volně přístupného	Zneužití služebního telefonu	Nedbalost ředitelky, učitelky, školnice, asistenta pedagoga	Kontrola telefonu, kontrola volaných čísel, zaheslování PINem	10	3	3	90	Ukládání telefonu na stejné místo. Mimo dosah dětí a cizích osob.	ředitelka, učitelka, školnice, asistent pedagoga	II/19	Telefonu vyhrazeno místo v jídelně na polici a v kanceláři ředitelky. Možnost braní telefonu na vycházky. Zodpovídá učitelka.	4	3	3	36	

Tabulka 22: Datová schránka, služební email, webové schránky

Název FMEA	**Řízení rizik procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů**	**Datum konání FMEA**	17.02.2019
Předmět FMEA	Datová schránka, služební e-mail, webové stránky		
FMEA Tým	Marcela Králová		

Proces	**Možná chyba**	**Možný důsledek**	**Příčina**	**Kontrola, preventivní opatření**	**Význam**	**Vznik**	**Odhalení**	**Možné riziko**	**Doporučená opatření**	**Odpovědnost**	**Termín**	**Provedená opatření**	**Význam**	**Výskyt**	**Odhalení**	**Možné riziko**	**Stav**
Přístup do datové schránky	Nezaheslování počítače. Neuschování tokenu s certifikátem. Neodhlášení se z datové schránky.	Přístup neoprávněné osoby do datové schránky mateřské školy	Nedbalost ředitelky, účetní	Kontrola umístění a uschování tokenu s certifikátem.	10	5	4	200	Token s certifikátem uschovávat v trezoru. Používat jen pokud je to nutné.	ředitelka, účetní	II/19	Uschování tokenu v trezoru. Použití jen při vstupu do datové schránky. Po ukončení práce odhlášení z datové schránky a uschování tokenu	4	3	3	36	
Používání služebního e-mailu	Nezaheslování počítače ředitelky, neuzavření služebního e-mailu po ukončení činnosti v něm.	Přístup do služebního e-mailu	Nedbalost ředitelky, účetní	Kontrola práce se služebním e-mailem	10	5	4	200	Odhlašování se z e-mailu	ředitelka, účetní	II/19	Dodržování pravidel při práci se služebním e-mailem	3	3	3	27	
webové stránky	Nezaheslování počítače. Neodhlášení se z administrátorského prostředí webových stránek.	Přístup na webové stránky mateřské školy	Nedbalost ředitelky	Kontrola práce s webovými stránkami	10	5	5	250	odhlašování sr z administrátorského prostředí webových stránek	ředitelka	II/19	Kontrola práce s webovými stránkami mateřské školy, kontrola vložených informací	4	4	2	32	
Administrace webových stránek	Nezaheslování počítače. Neodhlášení se z administrátorského prostředí webových stránek.	Zneužití webových stránek mateřské školy	Nedbalost ředitelky	Kontrola práce s webovými stránkami	10	5	5	250	Odhlašování se z administrátorského prostředí webových stránek.	ředitelka	II/19	Kontrola práce s webovými stránkami mateřské školy, kontrola vložených informací	4	3	3	36	

7.3 Hodnocení rizik

Na základě provedené analýzy rizik současného stavu ochrany osobních údajů v mateřské škole XY pomocí metody FMEA došlo k ohodnocení zjištěného stavu. Byla zjištěna slabá místa a rizikovost jednotlivých analyzovaných procesů organizace. Součástí metody byla i doporučena opatření, která by měla minimalizovat riziko. V případě provedení doporučených opatření by bylo znovu spočítáno možné riziko. Tento údaj je pouze doplňující a slouží k porovnání účinnosti navržených a následně přijatých opatření se stavem původním. Tento stav říká organizaci, na co se zaměřit, jaké vynaložit prostředky, jak pracovat se zaměstnanci, aby nedocházelo ke zneužívání osobních údajů. Samozřejmě, že nyní nejsme schopni posoudit, zda organizace doporučená opatření příjme a pokud ano, zda skutečně dojde k eliminaci rizik.

Pomocí FMEA se došlo k závěru, že rizikovými oblastmi je zabezpečení budovy, školní matrika, správa adresářů, uschovávání razítek, přístup do datové schránky, používání služebního e-mailu a administrace webových stránek. Nejméně rizikovou oblastí jsou účetní doklady a vydaná rozhodnutí. Po přijetí doporučených opatření by se rizikovost rapidně snížila. Pokud by tato opatření byla i nadále zodpovědně dodržována, mohlo by dojít k dalšímu snižování.

Vzhledem k tomu, že mateřská škola v současné době není příliš technicky vybavena a většina dokumentů je vedena v papírové podobě je riziko zneužití z vnějšího prostředí nižší. Hrozí zde riziko ze strany zaměstnanců, případně cizích osob, které by se do mateřské školy dostaly. V případě využívání výpočetní techniky a pracování s elektronickou podobou dokumentů je riziko zneužití osobních údajů vyšší, a to vzhledem k možnostem, které nám dává využívání internetu. Organizace však postupně přechází na elektronizaci dokumentů. Kdy dokumenty budou skenovány a zálohovány v počítači, případně na externích discích. Tím pádem bude nutné do budoucna se ve větší míře zaměřit i na rizika spojená s elektronickým uchováváním osobních údajů.

8 ŘÍZENÍ RIZIK A PROCESŮ ORGANIZACE

Problematika řízení rizik je rozsáhlá. V souvislosti s ochranou osobních údajů byla vybrána oblast bezpečnostního rizika. Tato oblast zahrnuje bezpečnost personální, která je zaměřena na osoby jejich zdraví a život, dále bezpečnost fyzická, zahrnující ochranu majetku organizace a bezpečnostní rizika informační, týkající se především ochrany informačního systému, sítě organizace, účetních programů, ochrany osobních údajů.

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti řeší informační a komunikační systémy. Specifikuje pojmy spojené s bezpečnostními opatřeními, kybernetickými incidenty v oblasti elektronických komunikací.

Vyhláška mimo jiné říká, že řízením rizik je činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [28].

Na základě analýzy jednotlivých procesů organizace, analýzy současného stavu ochrany dat, identifikace, analýzy rizik a hodnocení výsledků analýzy je nutné provést řízení rizik, která jsou spojená se zpracováním osobních údajů a přijmout vhodná technická a organizační opatření, aby zpracování osobních údajů bylo v souladu s Obecným nařízením. Na základě posouzení se rozhodneme, zda riziko eliminujeme nebo ho přijmeme.

8.1 Bezpečnost personální

Organizace musí zajistit svým zaměstnancům takové pracovní podmínky, aby nedošlo k poškození jejich zdraví či ztrátě na životě. Stejné podmínky musí být zajištěny pro děti, které do mateřské školy dochází a věnují se zde výuce a také pro jejich zákonné zástupce. Organizace má uzavřenou smlouvu se společností, která zde provádí školení BOZP a PO. Jedná se o vstupní školení, při přijmutí nového zaměstnance na základě žádosti o posouzení zdravotní způsobilosti k práci a doložení lékařského posudku. Pak se jedná o periodická školení – roční, BOZP a PO. Samotná ředitelka je pověřena kontrolou svých zaměstnanců a pravidelně kontroluje dodržování bezpečnosti a ochrany zdraví při práci. Z této kontroly vyhotovuje zápis. Tyto dokumenty obsahují osobní údaje zaměstnanců a jejich podpisy. Dokumentace je vedena v šanonu a uzamčena ve skříni v kanceláři ředitelky mateřské školy. V rámci řízení rizik je ochrana osobních údajů dostatečná. Přínosem by zajisté bylo vedení dokumentů i v elektronické podobě.

8.2 Bezpečnost fyzická

Bezpečnost fyzická se zaměřuje na ochranu majetku organizace. Mateřská škola XY nevlastní budovu, ve které se organizace nachází. Budovu má ve výpůjčce od obce XY. Proto v případě jakýchkoli požadavků na zabezpečení, opravy a údržbu musí žádat svého zřizovatele, tedy obec XY.

Budova je dosti stará. V roce 1883 zde probíhala první výuka. Mateřská škola prodělala několik úprav. Poslední rekonstrukce se uskutečnila v roce 2004 a v roce 2017 zde byla vyměněna okna dřevěná za plastová.

Z tohoto důvodu je zřejmé, že budova není moderní, spíše historická. Nemá žádné moderní bezpečnostní prvky. V rámci řízení rizik je nutné zajistit kromě klíčového režimu, také zebezpečovací zařízení, které bude nainstalováno u vchodových dveří do budovy. Zvonek umístěný u vchodových dveří je nedostačující a hodně poruchový. Dle mého názoru je účelné ke vchodu a do zadní části budovy umístit kamerový systém. Záleží na zvážení ředitelky školy a vedení obce, zda kamery umístit i uvnitř budovy.

K provozování kamerového systému je ovšem nutné, aby organizace měla směrnici k ochraně osobních údajů v kamerovém systému. Tato směrnice je nezbytná, pokud je kamerový systém umístěn uvnitř budovy. Vzor směrnice je možné získat na webových stránkách Svazu měst a obcí.

Klíčový režim je nastaven v pořádku. Ředitelka má vyhotoven soupis všech klíčů a seznam osob, které s nimi disponují. Tyto osoby stvrdili svým podpisem převzetí a manipulaci s klíči. Soupis spolu s náhradními klíči je uložen v trezoru v kanceláři ředitelky. Trezor je uzamčený a klíč má pouze ředitelka.

8.3 Bezpečnostní rizika informační

Za zpracování osobních údajů odpovídá v souladu s nařízením vždy správce, tedy škola nebo školské zařízení [29].

8.3.1 Účetnictví

Problematiku účetnictví řeší zákon č. 563/1991 Sb., o účetnictví. Tento zákon upravuje rozsah a způsob vedení účetnictví, požadavky na jeho průkaznost, rozsah a způsob zveřejňování informací z účetnictví a podmínky předávání účetních záznamů pro potřeby státu [30].

Tím pádem ke zpracování účetních dokladů není zapotřebí souhlasu se zpracováním osobních údajů. Účetní doklady obsahují osobní údaje, a to jak v přílohách účetních dokladů, tak na samotných dokladech, kde je nutné umístit podpisy. Jsou to podpisy příkazce operace, hlavní účetní a správce rozpočtu. Doklady jsou vedeny v šanonech a uzamčeny ve skříni. Účetní doklady jsou archivovány po dobu pěti let a poté jsou určeny ke skartaci.

Samotnou kapitolou ochrany osobních dat, je zpracování účetních dokladů na počítači. Organizace tuto agendu vede v účetních programech. Správa účetních programů spadá pod servisního technika společnosti, u které má organizace zakoupený účetní a personální software. Technik je externí osoba a jeho přístup k údajům organizace musí být ošetřen buď dodatkem ke stávající smlouvě nebo prohlášením o ochraně osobních údajů a mlčenlivosti. Co se týká dalších činností souvisejících s informačními technologiemi musí mít organizace smlouvu o činnostech spojených s ochranou informačních technologií se správcem IT. Samotná organizace pak musí mít příslušnou směrnici, která bude řešit ochranu informačních technologií se správcem IT. Organizace tuto směrnici nemá. Nemá uzavřenu žádnou smlouvu se servisním technikem. Neexistuje provozní řád informačních technologií, který by zachytil proces ochrany těchto technologií.

Vzhledem k bezpečnosti a uchování dat, by měla organizace zajistit i vhodné zálohování dat. Zálohy v počítači ředitelky mateřské školy jsou nedostačující. Jako vhodná se nabízí záloha dat na server poskytovatele služeb IT. Další rizikovou oblastí jsou tiskárny a reprografická technika.

Tiskárna se může stát zdrojem problému, respektive úniku osobních dat velmi jednoduše. Má svůj procesor, paměť, operační systém, často i harddisk, uživatelské rozhraní ve formě ovládacího panelu, síťové připojení běžně s přístupem na Internet či WIFI hotspot. A tudíž i zde hrozí stejná nebezpečí napadení či ztráty dat jako u počítačů [2].

8.3.2 Smlouvy, personalistika

Mateřská škola jako každá jiná organizace má své zaměstnance. Tato organizace má ředitelku, učitelku, chůvu, asistenta pedagoga a účetní. Organizace při uzavírání pracovních smluv a dohod o provedení práce se řídí zákonem č. 262/2006 Sb., zákoník práce. V souvislosti s uzavíráním pracovních smluv a dohod o provedení práce je nezbytné, aby organizace komunikovala i s jinými orgány, kterým předává osobní data. Jedná se především o správu sociálního zabezpečení, zdravotní pojišťovny, finanční úřad. K poskytování osobních údajů

těmto orgánům nepotřebuje organizace souhlas zaměstnanců. Tyto povinnosti jsou stanoveny zákonem. Dále organizace pro potřeby mzdové agendy vyžaduje po zaměstnancích vyplnění osobního dotazníku, doklad o vzdělání, telefonní kontakt, e-mailovou adresu, číslo účtu, případně údaje o partnerovi a dětech, zdravotní pojišťovnu. Tyto údaje opět souvisí s činností danou zákonem. Tím pádem souhlas zaměstnance se zpracováním osobních údajů nepotřebuje. Součástí pracovních smluv jsou i dodatky pojednávající o zachování mlčenlivosti zaměstnanců v souvislosti s ochranou osobních dat. Tyto dodatky jsou pracovníky podepsány. Organizace by měla shromažďovat jen ty údaje, které jsou nezbytné pro pracovněprávní vztahy. Zajímavým údajem je použití rodného čísla.

Rodné číslo lze podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, využívat – kromě užití pro účely státní správy a justice – pouze tehdy, stanoví-li tak zvláštní zákon, a jinak jen se souhlasem nositele rodného čísla [31].

To znamená, že žádný zákon neukládá uvádět rodné číslo na pracovních smlouvách, ale správa sociálního zabezpečení a zdravotní pojišťovny tento údaj na svých formulářích vyžadují. Proto je vhodné používat formulář, kde zaměstnanec svým podpisem stvrdí, že souhlasí s použitím rodného čísla pro daný účel.

Organizace rovněž vede evidenci o pracovní neschopnosti, mateřské dovolené, rodičovské dovolené, péči o dítě.

Osobní údaje o těhotenství, sexuální orientaci, rodinných a majetkových poměrech, původu, politické příslušnosti, náboženství, trestní bezúhonnosti, zdravotním stavu nelze po zaměstnancích vyžadovat. Pouze pokud by zaměstnanec dal výslovný souhlas se zpracováním těchto údajů. Organizace vede osobní spis zaměstnance, do kterého může nahlížet je ředitelka školy a účetní.

Další typy smluv, které organizace vlastní již nezasahují do oblasti personální. Jedná se o smlouvy s dodavateli energií, vody, smlouva s poskytovatelem internetu a telekomunikačních služeb. Smlouva s externí školní vyvařovnou na dodávku jídla pro děti, dále s firmou, která stravu do mateřské školy dováží. Smlouvy uzavřené s fyzickými osobami, a to jak darovací, tak na poskytnutí různých služeb, jako je školení pedagogů, asistentů. Školení pro rodiče. Akce pro děti, jako například divadelní představení, školička bruslení, plavání. Výuka na hudební nástroje, jazyková příprava.

Veškeré tyto smlouvy rovněž obsahují osobní údaje, a to minimálně podpis ředitelky školky, případně osob zastupující právnické osoby nebo přímo údaje týkající se samotných fyzických osob poskytujících služby. Tyto smlouvy jsou uloženy v šanonech a zamčeny ve skříni v kanceláři ředitelky. Některé dokumenty jsou skenovány do počítače. Personální agenda je v kanceláři účetní. Dokumenty jsou v šanonech v uzamčené skříni. Většina dokumentace je zároveň i v počítači. V rámci eliminace rizik je zapotřebí v daném časovém intervalu měnit přístupové heslo do počítače ředitelky. Pokud možno zavést servisní kontrolu počítače a sítě. Po skončení práce veškerou dokumentaci uzamykat do skříně.

8.3.3 Školní matrika, rozhodnutí

Školní matrika je důležitou a nemalou částí veškeré dokumentace organizace. Povinnou dokumentaci stanovuje § 28 zákona č. 561/2004 Sb., školský zákon. Z toho vyplývá, že organizace vyžaduje ty dokumenty, které jí stanovuje zákon. Veškeré dokumenty obsahují osobní údaje, a to údaje dětí, či jejich zákonných zástupců, lékaře, psychologů apod. Mezi tyto dokumenty patří např. přihláška dítěte k zápisu do mateřské školy, rozhodnutí ředitelky o přijetí dítěte do mateřské školy, evidenční list pro dítě v mateřské škole, přihláška ke stravování, evidenční list pro dítě v mateřské škole, kniha docházek za daný školní rok, třídní kniha, přehled vykonané práce, omluvný list (u dětí v posledním ročníku mateřské školy je stanoven zákonem o povinném předškolním vzdělávání), souhlas se zpracováním osobních údajů, záznamový arch pro hospitaci, evaluace (hodnocení), záznam o dítěti, přehled odpracované doby.

Zpracování osobních údajů ve školských zařízeních nelze obecně zakládat na souhlasu [32].

Písemné pověření k vyzvedávání dítěte pověřenou osobou nevyžaduje souhlas zákonného zástupce se zpracováním jeho osobních údajů.

Jinou oblastí jsou díla vytvořená dětmi. Pokud jsou podepsána, jedná se již o osobní údaj. Délka zpracování a uchování osobních údajů končí výmazem.

Pod výmaz bude spadat např. i předání obrázku namalovaného žákem, z něhož lze konkrétní dítě identifikovat (vzhledem k podpisu nebo uvedení jména apod.), rodiči daného dítěte. Okamžikem předání obrázku rodičům pak v tomto případě končí zpracování osobních údajů školou [24].

Pokud se jedná o dokumenty, se kterými se nakládá podle zákona č. 499/2004 Sb., o archivní a spisové službě. Řídí se ukládání tímto zákonem. Jinak jsou dokumenty po uplynutí doby a splnění účelu mazány.

Organizace má dva archivy. Klasický archiv je umístěn v patře v bývalé třídě. Zde je již zabezpečení nedostačující. Skříně nemají zámky, dveře do třídy jsou opatřeny málo bezpečným zámkem. Příruční archiv v kanceláři ředitelky mateřské školy. Tento archiv je zabezpečen dostatečně. Skříně jsou uzamčeny a klíče vlastní jen ředitelka školy. Samotná kancelář je uzamčena a nemá do ní nikdo přístup, ani zaměstnanci organizace. Vzhledem k bezpečnosti dokumentů, které se zde nacházejí by bylo vhodné umístit před vstup do kanceláře kameru. Umístění kamery uvnitř budovy má však svá úskalí.

Fotografie a video záznamy osob jsou z hlediska GDPR chápány jako osobní údaje, stejně jako informace o osobách, které jsou odvozeny z těchto materiálů. Nařízení GDPR chápe použití kamerových systémů jako sběr osobních dat, pokud na záznamech lze rozpoznat tváře jednotlivých osob. K povinnostem provozovatele kamerového systému patří sdělit osobám, které mohou být snímány, že k také činnosti dochází a kdo za systém zodpovídá [2].

8.3.4 Webové stránky, služební – email, datové schránky

Mateřská škola nemá vlastní webové stránky. Své příspěvky a fotografie umisťuje na webové stránky obce, která je jejím zřizovatelem. Ředitelka mateřské školy má vlastní přístupové údaje, se kterými se přihlašuje do tzv. redakčního systému. Zde má stanoveno omezení pro práci jen v sekci mateřská škola, kterou ji správce webových stránek vyhradil. Při otevření záložky mateřské školy na webu obce se zobrazí informace o jídelníčku na daný týden, informace pro rodiče, aktuality, fotogalerie, filosofie MŠ, seznam akcí na školní rok, GDPR.

Ve fotogalerii jsou fotografie dětí z různých akcí. Fotografie jsou bez popisu a jmen dětí.

V případě pořizování a zveřejňování reportážních fotografií z činnosti školy (situační záběry z vyučování, soutěží, dílen, veřejných vystoupení žáků apod.) se nejedná primárně o problematiku ochrany osobních údajů, ale o ochranu soukromí, tj. o postup podle ustanovení § 84 a násl. občanského zákoníku, která upravují pořizování podobizny. Souhlas se zpracováním osobních údajů k „ilustračním“ snímkům tedy není třeba vyžadovat [32].

Zákon č. 89/2012 Sb., občanský zákoník, § 84 zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením [33].

Pokud však tyto fotografie, obrázky, videa obsahují osobní údaje dětí, je nutné mít souhlas s použitím osobních údajů od jejich zákonných zástupců.

Jedním z velmi problematických momentů při ochraně osobních údajů jsou přenosy digitálních dat. Přenosem je myšleno několik procesů, jako je transfer pomocí sítí a internetu nebo fyzický přenos v mobilních zařízeních [2].

V případě využívání webových stránek je nutné mít ošetřenu heslovou politiku pro přístup do redakčního systému, servisní zajištění technikem IT, využívání antivirových programů a zabezpečení internetové sítě.

V dnešní době je zcela běžné, že jeden uživatel disponuje desítkami přístupů k webovým službám. Každý takový účet obsahuje osobní údaje od těch běžných, jako je adresa nebo email, až po ty velmi kritické, jako je číslo kreditní karty nebo přístupová hesla [2].

Jednou z variant, jak mohou pracovníci organizace zabezpečit elektronický soubor pro jeho zaslání elektronickou poštou příjemci, tak, aby nedošlo k jeho neoprávněnému zpracování je možnost doplnění hesla pro otevření takového souboru [34].

Přístup do služebního e-mailu má ředitelka mateřské školy. Zná přístupové údaje a ostatním zaměstnancům je neposkytuje. Přístup do služebního e-mailu poskytuje jen pod dozorem, kdy provede přihlášení a poté kontroluje činnost zaměstnance, který byl pověřen ve služebním e-mailu pracovat. Je nutné pravidelně měnit heslo pro přístup do služebního e-mailu a na webové stránky. Nesdělovat dalším osobám a nepoužívat jej v blízkosti jiné osoby.

Správu uživatelských přístupů do informačních systémů a mapování složek pro ukládání dokumentů má za povinnost správce IT [35].

Administrátorský účet nesmí být využíván pro běžnou pracovní činnost [35].

Zaměstnanci nesmí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení, což je stanoveno v § 316 zákona č. 262/2006 Sb., zákoník práce [36].

Ředitelka může přiměřeně kontrolovat, zda tato skutečnost není porušována, např. kontrolou objemu přijaté či odeslané pošty, navštívených domén v internetovém prohlížeči.

Vzhledem k tomu, že mateřská škola vlastní pouze jeden počítač umístěný v kanceláři ředitelky, je využívání počítače pro svou soukromou potřebu a následně pro případně porušení ochrany osobních údajů, mizivé.

S vývojem techniky se stále častěji ve školách i jinde využívá k uchování dat, tzv. cloudových služeb. K tomuto je třeba zdůraznit, že je povinností správce, v tomto případě školy, posoudit, zda je ochrana osobních údajů v rámci těchto služeb dostatečná i pro zpracování osobních údajů zaměstnanců a žáků školy [29].

Tyto služby poskytují většinou zahraniční právnické osoby a dokumenty nejsou vedeny v českém jazyce.

Datová schránka mateřské školy je opatřena heslem a přístup do ní má pouze ředitelka mateřské školy a účetní. Certifikát pro podepisování dokumentů je umístěn a tokenu. Ředitelka i účetní mají vlastní token a vlastní přihlašovací údaje. Heslo je pravidelně měněno. Token je uzamčen v trezoru v kanceláři ředitelky.

Pro komplexní činnost pracování s dokumenty by bylo vhodné, aby organizace měla elektronickou spisovou službu. Ředitelka by měla apelovat na svého zřizovatele, aby uvolnil finanční prostředky na zakoupení příslušného softwaru. Elektronická komunikace došlé a odeslané pošty ulehčí i následnou archivaci dokumentů. Touto cestou se zamezí případné ztrátě dokumentů a přehledu o dokumentech organizace.

8.3.5 Adresáře, razítka

Adresáře obsahující údaje o telefonních číslech, e-mailech, webových stránkách subjektů, se kterými organizace spolupracuje jsou uvedeny v písemné podobě na vizitkách a v sešitě. Ředitelka je uchovává ve svém pracovním stole, kde jsou v uzamčeném šuplíku.

Razítka jsou umístěna v trezoru a uzamčena. V trezoru je s razítky i seznam a jmenovité určení osob, které je mohou používat.

8.3.6 Používání služebního telefonu

Organizace vlastnila klasický tlačítkový telefon. Náklady na provoz byly vysoké, tudíž nové vedení přešlo na telefon mobilní. Organizace platí paušální částku. Došlo ke snížení nákladů zhruba o polovinu oproti předcházejícímu stavu. Mobilní telefon je klasický tlačítkový. Není to smartphone. Nekomunikuje s WiFi připojením. Při posouzení rizikovosti použití služebního telefonu se dojde k závěru, že nejde s ním fotit a případný únik osobních údajů by musel být v rámci telefonního hovoru, a to buď ze strany zaměstnanců nebo neoprávněné osoby, která by se dostala do budovy. K zamezení zneužití telefonu by bylo vhodné opatřit přihlášení do přístroje PINem. Ten by znali jen ti zaměstnanci, které by určila ředitelka. Zároveň by bylo vhodné PIN měnit. Ředitelka by měla ovšem ošetřit používání osobních telefonů

zaměstnanců. Mohlo by docházet k úniku osobních dat právě přes telefony soukromé. Tato skutečnost se sice jeví jako nereálná, už vzhledem k podepsané mlčenlivosti ze strany zaměstnanců. Ale riziko nemůžeme vyloučit.

8.3.7 Kybernetická bezpečnost

Oblast kybernetické bezpečnosti ve spojení s ochranou osobních údajů je v současné době velmi diskutované téma.

Většina dat, tedy i osobních údajů, je v digitální podobě. Ke sběru těchto informací dochází sice ještě mnohdy v listinné podobě, ale následně jsou takto získaná data převedena do digitální formy scannerem nebo prostě ručně přepsána [5].

Norma ISO 27001 je rámcovou normou pro ochranu a bezpečnost dat. Dle GDPR jsou osobní údaje kritické informace, které všechny organizace mají povinnost chránit. Existují některé požadavky stanovené GDPR, které norma ISO 27001 nepokrývá, jako je podpora práv subjektů osobních údajů: právo být informován, právo na vymazání údajů nebo přenositelnost dat [5].

Potenciálně nejnebezpečnějším způsobem kybernetické komunikace jsou otevřené Wi-Fi sítě. Vaše bezpečí je pouze tak vysoké, jak je bezpečný nejslabší článek v řetězci komunikace. V tomto případě bývá Wi-Fi tím nejméně spolehlivým kanálem. Situace je složitá i v případě telefonních hovorů nebo zasílání SMS zpráv přes operátory [5].

Elektronická komunikace může být napadena škodlivým softwarem jako např. ransomware.

Ransomware může být pro data, která máte dle GDPR chránit, jedním z velkých nebezpečí. Jeho hrozba se neskrývá v tom, že data útočník ukradne, ale naopak udělá to, co jste s největší pravděpodobností neudělali, tedy data zašifruje, znemožní k nim přístup a klíč v lepším případě získáte až zaplacením výkupného [5].

Důležité je využívat hashování. Základní vlastností hashování je jeho jednosměrnost. Vytvoření hashe z hesla je jednoduché, na internetu je možné najít celou řadu generátorů. Naopak získání hesla z hashe by nemělo být možné. Funkci hashování lze použít nejen k zašifrování hesla, ale také celých textů, souborů, nebo dokonce aplikací. S rozvojem technologie vznikly šifry, které patří do kategorie moderního kryptování. Lze je rozdělit na symetrické a asymetrické. Jejich hlavní rozdíl je v tom, zda se k zašifrování i rozšifrování zprávy využívá stejný klíč, či nikoliv [5].

Symetrické šifry využívají stejný klíč a asymetrické šifry využívají párový klíč.

9 SANKCE A PODMÍNKY UKLÁDÁNÍ POKUT

Další povinností pod zásadou transparentnosti je oznamování případů porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 obecného nařízení [37].

Tuto povinnost má správce, pokud je pravděpodobné, že porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob [37].

Podstatným a setrvalým úkolem pověřence je monitorovat soulad zpracování osobních údajů podle GDPR [38].

Součástí každé právní normy zpravidla bývá i sankční část, která má preventivní a donucující účinek na adresáty právní normy [1].

9.1 Podmínky ukládání pokut

Při rozhodování o tom, zda uložit pokutu, a při rozhodování o její výši v jednotlivých případech musí dozorový úřad zohlednit následující okolnosti [1]:

- povahu, závažnost a délku trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování,
- zda k porušení došlo úmyslně nebo z nedbalosti,
- kroky podniknuté ke zmírnění škod způsobených subjektem údajů,
- míru odpovědnosti správce či zpracovatele,
- míru spolupráce s dozorovým úřadem za účelem nápravy daného porušení,
- kategorie osobních údajů dotčené daným porušením [1].

9.2 Výše pokut

Obecné nařízení rozděluje druhy porušení do dvou kategorií, které jsou rozlišeny výší možné sankce, a to podle možného dopadu porušení na zájem chráněný Obecným nařízením, kterým je ochrana práv a svobod subjektu údajů při zpracování osobních údajů [1].

Skutkové podstaty jsou koncipovány poměrně široce, vždy jako porušení k povinnostem vyplývajícím z určených článků. Proto nelze zapomínat, že sankce může být udělena nejen za nesplnění „hlavní“ povinnosti, ale i ze nesplnění souvisejících povinností [1].

První kategorie obsahuje porušení Obecného nařízení, za které lze udělit pokutu do výše 10 000 000 EUR. Druhá kategorie zahrnuje závažné porušení, za které lze udělit pokutu do výše 20 000 000 EUR [1].

Český adaptační zákon dosáhl snížení výše pokut na přijatelnou míru. Pokuty stanovené v Obecném nařízení jsou pro většinu českých organizací likvidační.

Dle znění zákona č. 110/2019 Sb., o zpracování osobních údajů došlo ke stanovení pokut v následujících výších:

Fyzická osoba, právnická osoba nebo podnikající fyzická osoba se dopustí přestupku tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem.
Za přestupek podle odstavce 1 lze uložit pokutu do:
a) 1 000 000 Kč, nebo
b) 5 000 000 Kč, jde-li o přestupek spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.
Úřad upustí od uložení správního trestu také tehdy, jde-li o subjekty uvedené v čl. 83 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016/679 [39].

ZÁVĚR

Cílem bakalářské práce bylo řízení rizik a procesů v mateřské škole s ohledem na novou právní úpravu ochrany osobních údajů. Řízení rizik a procesů v organizaci je výsledná fáze vycházející z podrobné analýzy jednotlivých samostatných procesů, které v organizaci probíhají. Nejdůležitější činností bylo správně identifikovat rizika organizace, související s osobními údaji. Vzhledem k tomu, že organizace většinu dokumentů obsahujících osobní údaje zpracovává na základě zákona č. 561/2004 Sb., školský zákon, nepotřebuje k jejich zpracování souhlas daného subjektu. Osobní údaje ale musí chránit, aby nedošlo k jejich zneužití. Při komplexním pohledu na tuto problematiku bylo do posuzovaných oblastí zahrnuto zabezpečení samotné budovy mateřské školy, dále pak agendy související s vedením účetnictví a personalistikou, smlouvy a vydaná rozhodnutí organizace. Velice důležitá je školní matrika, která zpracovává veškeré potřebné údaje o dětech a jejich zákonných zástupcích. Dále pak správa adresářů s osobními údaji, využívání služebního mobilního telefonu, služebního e-mailu, přístupu do datové schránky a přístup na webové stránky organizace. Po provedení identifikace potencionálních zdrojů rizika došlo k samotné analýze rizik. Pomocí metody FMEA byly analyzovány jednotlivé rizikové oblasti. Výsledkem analýzy bylo zjištění současného stavu. Následné hodnocení rizik vyplývající z výsledků analýzy konstatovalo, že za nejméně rizikové oblasti jsou považovány oblast účetnictví, smlouvy a vydaná rozhodnutí. Zde jsou osobní údaje dostatečně chráněny proti případnému ohrožení. Naopak mezi rizikové oblasti patří zabečení budovy, školní matrika, správa adresářů, přístup do datové schránky, na služební e-mail, webové stránky a používání služebního mobilního telefonu. Zneužití osobních údajů v této oblasti je vysoké. Samotné řízení rizik a procesů vycházelo z těchto zjištění a zaměřilo se na eliminaci rizika, protože zde nejde odstranit rizika úplně. Řízení rizik a procesů se týká různých oblastí. Tato práce řeší oblast informační. Zde patří bezpečnost personální, fyzická a bezpečnostní rizika informační. Z toho vyplývá, že organizace by měla mít spolehlivé a kvalifikované zaměstnance. Jejich výběr je na ředitelce mateřské školy. Tito zaměstnanci musí být proškoleni, jak na úseku bezpečnosti práce, tak na úseku ochrany osobních údajů. Musí se řídit vnitřními předpisy organizace, nařízeními a pokyny ředitelky mateřské školy. Protože selhání lidského faktoru je největším rizikem pro organizaci. Ředitelka musí komunikovat mimo jiné i s majitelem budovy školy, tedy s obcí, aby došlo k zabezpečení budovy proti vstupu neoprávněných osob. V současné době by bylo vhodné používat zabezpečovací zařízení a případně instalovat kamerový systém, minimálně u vstupů do budovy. Bezpečností rizika informační zahrnují největší část řízení

rizik a procesů v této organizaci. Vzhledem k tomu, že většina osobních údajů je na dokumentech vedených v papírové podobě. Může se tento stav v době, kdy svět ovládá elektronická komunikace a s ní spojené zneužívání, zdát jako nejbezpečnější, ale není tomu tak. Proto by organizace měla disponovat elektronickou spisovou službou, pro vedení veškerých dokumentů. Tento program slouží pro přehled o dokumentech organizace a je nezbytný pro správnou archivaci dokumentů. K dalším výhodám patří přístup do datové schránky přes tuto aplikaci. Veškerá data by měla být i v elektronické podobě a zálohována. Chybí zajištění servisních služeb v IT oblasti a s tím i zabezpečení WiFi sítě. Pravidelný servis a aktualizace počítače ředitelky mateřské školy. Samotný fyzický archiv, který je nedostatečně zabezpečen, a to jak zámky na skříních, tak zabezpečením samotného přístupu do archivu.

Závěrem lze konstatovat, že organizace byla připravena na Obecné nařízení o ochraně osobních údajů. Měla povědomí o rizicích, která pro ni vyplývají. Podrobnou analýzou byla zjištěna slabá místa, která tato organizace ještě má. Ředitelka je si těchto slabých míst vědoma a vyvíjí aktivity k jejich odstranění. Samozřejmě, že tato snaha musí být pochopena i ze strany obce, jako zřizovatele. Obec musí posoudit finanční náročnost těchto opatření a přijmout stanovisko, se kterým ředitelku seznámí. Samozřejmě riziko sankcí za porušení Obecného nařízení o ochraně osobních údajů je nemalé a mělo by být obcí bráno na zřetel při jeho rozhodování.

SEZNAM POUŽITÉ LITERATURY

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

[2] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2.

[3] ČESKÁ REPUBLIKA. Sbírka zákonů České republiky: Usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky. In: *Sbírka zákonů, Česká republika*. Praha: Vydavatelství a nakladatelství MV ČR, 1992, ročník 1993, částka 1.

[4] BARTÍK, Václav a Eva JANEČKOVÁ. *Zpracování osobních údajů obcemi: (vybrané problémy)*. Praha: Wolters Kluwer Česká republika, 2013. ISBN 978-80-7357-962-3.

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

[6] *Elektronický zpravodaj pro pověřence: Hlídací pes pro osoby zodpovědné za GDPR* [online]. Praha: FORUM, 2018, 8 s. [cit. 2018-12-28]. Dostupné z: https://www.forum-media.cz/premium/end-demo/

[7] Sněmovní tisk 138/0, část č. 1/6 Vl.n.z. o zpracování osobních údajů - EU - RJ. In: *Poslanecká sněmovna Parlamentu České republiky* [online]. 2019 [cit. 2019-05-05]. Dostupné z: http://www.psp.cz/sqw/historie.sqw?o=8&T=138

[8] *Magazín GDPR*. Rychnov nad Kněžnou: Softbit Software, 2019, **2**(1).

[9] Schéma legislativního procesu. In: Poslanecká sněmovna Parlamentu České republiky: Přijímání zákonů[online]. Praha [cit. 2019-02-24]. Dostupné z: http://www.psp.cz/kps/pi/gi/schema_bezne_zakony.pdf

[10] NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

[11] MENDROK, Eva, Tomáš VAVRO a Marek ZEMAN. *Školy a ochrana osobních údajů podle GDPR*. Praha: Verlag Dashöfer, 2018. ISBN 978-80-87963-59-3.

[12] Řízení rizik. In: *ManagementMania.com* [online]. [cit. 2019-02-24]. Dostupné z: https://managementmania.com/cs/rizeni-rizik

[13] Jak volit nástroje pro snižování rizika. In: *BussinessInfo.cz: Oficiální portál pro podnikání a export*[online]. 2014 [cit. 2019-02-24]. Dostupné z: https://www.businessinfo.cz/cs/clanky/metody-snizovani-rizika-52919.html

[14] Šest kroků k úspěšnému řízení rizik. In: *CFOworld.cz: From IDG* [online]. 2011 [cit. 2019-02-24]. Dostupné z: https://cfoworld.cz/analyzy/sest-kroku-k-uspesnemu-rizeni-rizik-1188

[15] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích* [online]. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013 [cit. 2019-02-24]. Expert (Grada). ISBN 978-80-247-4644-9.

[16] Řízení procesů. In: *ManagementMania.com* [online]. [cit. 2019-02-24]. Dostupné z: https://managementmania.com/cs/rizeni-procesu

[17] ANTUŠÁK, Emil. *Krizový management: hrozby - krize - příležitosti*. Praha: Wolters Kluwer Česká republika, 2009. ISBN 978-80-7357-488-8.

[18] ČESKÁ REPUBLIKA. Zákon č. 561/2004, 562/2004 a 562/2004. In: *Sbírka zákonů, Česká republika*. Praha: Tiskárna Ministerstva vnitra, p.o., 2004, ročník 2004, číslo 190. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=561/2004&typeLaw=zakon&what=Cislo_zakona_smlouvy

[19] JUŘICOVÁ, Martina. *Organizační řád Mateřské školy Rakov*. Rakov, 2017.

[20] JUŘICOVÁ, Martina. Vlastní hodnocení činnosti mateřské školy za školní rok 2017/2018. Rakov, 2018.

[21] JUŘICOVÁ, Martina. *Rozpočet Mateřské školy XY na rok 2019*. Rakov, 2019.

[22] JUŘICOVÁ, Martina. *Školní řád*. Rakov, 2017.

[23] JUŘICOVÁ, Martina. *Archivační a skartační řád*. Rakov, 2017.

[24] Metodická pomůcka k aplikaci obecného nařízení o ochraně osobních údajů a zákona o zpracování osobních údajů v podmínkách školství [online]. In: . Praha: Ministerstvo školství, mládeže a tělovýchovy ČR, 2018, s. 91 [cit. 2019-03-30]. Dostupné z: http://www.msmt.cz/file/44592/

[25] KÝVALOVÁ, Pavlína. Analýza současného stavu ochrany osobních údajů v obci Rakov a posouzení míry souladu s požadavky Nařízení Evropského parlamentu a Rady (EU) č. 2016/679. 1. Rouské, 2018.

[26] FMEA: Failure Mode and Effect Analysis. *ManagementMania.com* [online]. 2016 [cit. 2019-03-30]. Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

[27] *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka*. 4. vyd. Praha: Česká společnost pro jakost, 2008. ISBN 978-80-02-02101-8.

[28] ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat: Vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů, Česká republika*. Praha: Tiskárna Ministerstva vnitra, p.o., 2018, částka 43, číslo 82. Dostupné také z: https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_82-2018sb.pdf

[29] Stručný návod na zabezpečení procesů souvisejících s GDPR ve školách (nástin pracovního postupu). In: *Ministerstvo školství, mládeže a tělovýchovy ČR* [online]. Praha, 2018 [cit. 2019-03-30]. Dostupné z: http://www.msmt.cz/dokumenty-3/strucny-navod-na-zabezpeceni-procesu-souvisejicich-s-gdpr

[30] ČSFR. Zákon č. 563/1991 Sb., o účetnictví. In: *Sbírka zákonů, Česká republika*. Praha: Federální ministerstvo vnitra ČSFR, 1991, částka 107, číslo 563. Dostupné také z: https://www.zakonyprolidi.cz/cs/1991-563/zneni-20180101

[31] ŠUBRT, Bořivoj, Zdeňka LEIBLOVÁ, Věra PŘÍHODOVÁ, et al. *Abeceda mzdové účetní ...* Olomouc: ANAG, 1996. Práce, mzdy, pojištění. ISBN 978-80-7554-189-5.

[32] Úřád pro ochranu osobních údajů: Ze školství - často kladené otázky. In: *Úřád pro ochranu osobních údajů: The office for personal data protection* [online]. Praha, 2018 [cit. 2019-03-30]. Dostupné z: https://www.uoou.cz/vismo/zobraz_dok.asp?id_org=200144&id_ktg=5088&n=ze-skolstvi

[33] ČESKÁ REPUBLIKA. Zákon č. 89/2012 Sb., občanský zákoník. In: *Sbírka zákonů, Česká republika*. Praha: Vydavatelství a nakladatelství MV ČR, 2012, částka 33, číslo 89. Dostupné také z: https://www.zakonyprolidi.cz/cs/2012-89

[34] *Magazín GDPR*. Rychnov nad Kněžnou: Softbit Software, 2018, **1**(1).

[35] *Magazín GDPR*. Rychnov nad Kněžnou: Softbit Software, 2018, **1**(2).

[36] *Magazín GDPR*. Rychnov nad Kněžnou: Softbit Software, 2018, **1**(3).

[37] CHLÁDKOVÁ, Jana. Pověřenci obcí na startovní čáře. *Informační servis: časopis Svazu měst a obcí České republiky*. Praha, 2018, **26**(5), 2.

[38] TAUSCH, Michal. GDPR očima odborníků. Gorinfo: Odborný bulletin pro uživatele informačních systémů ve veřejné zprávě. Jihlava, 2018, (2), 2.

[39] ČESKÁ REPUBLIKA. Zákon o ochraně osobních údajů č. 110/2019 Sb. In: *Sbírka zákonů, Česká republika*. Praha: Tiskárna Ministerstva vnitra, p.o., 2019, ročník 2019, částka 47, číslo 110. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38632

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP	Bezpečnost a ochrana zdraví při práci
ČR	Česká republika
EU	Evropská unie
EUR	Měna Euro
FKSP	Fond kulturních a sociálních potřeb
FMEA	Analýza možných vad a jejich následků (Failure Mode and Effect Analysis)
GDPR	Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
ISO	Celosvětově platné normy (International Organization for Standardization)
IT	Informační technologie
MěÚ	Městský úřad
PIN	Osobní identifikační číslo (Personal Identifikacion Number)
PO	Požární ochrana
SMS	Služba krátkých textových zpráv (Short Message Service)
UOOÚ	Úřad pro ochranu osobních údajů
WiFi	Bezdrátové připojení (Wireless Ethernet Compatibility Aliance)
ZoOU	Zákon o ochraně osobních údajů
ZZOÚ	Zákon o zpracování osobních údajů

SEZNAM OBRÁZKŮ

SEZNAM TABULEK