Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra řízení

Diplomová práce

Metodika hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů

Bc. Pavlína Janišová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Pavlína Janišová

Provoz a ekonomika

Název práce

Metodika hodnocení rizik pro posouzení vlivu na ochranu osobních údajů

Název anglicky

Methodology for risk assessment for data protection impact assessment

---

Cíle práce

Hlavním cílem diplomové práce je vytvoření metodiky hodnocení rizik pro posouzení vlivu na ochranu osobních údajů dle Nařízení Evropského parlamentu a Rady (EU) 2016/679 a návrh opatření k řešení těchto rizik včetně opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením.

Metodika

Práce se skládá ze dvou částí – teoretické a praktické. Teoretická část bude zpracována na základě analýzy sekundárních zdrojů. Praktická část bude zpracována na základě výstupů z kvalitativního výzkumu.

Syntéza výchozí znalostní báze: 11/2016 – 08/2017

Kvalitativní výzkum: 09/2017 – 11/2017

Agregace poznatků: 12/2017 – 02/2018

Odevzdání práce na katedru: 03/2018

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Riziko, proces řízení rizik, identifikace rizik, analýza rizik, hodnocení rizik, GDPR

Doporučené zdroje informací

BAUMRUK, J., CIKRT, M., HLÁVKOVÁ, J. et al. Analýza rizik při práci: Příručka pro zaměstnavatele. Praha: Fortuna, 2001. ISBN 80-7071-183-3.

ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

ČSN ISO/IEC 27005. Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

HNILICA, J., FOTR J. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 1. vyd. Praha: Grada, 2009, 262 s. Expert (Grada). ISBN 978-80247-2560-4.

MERNA, T., FAISAL, F. Risk management. Brno: Computer Press, 2007. ISBN 978-80-251-1547-3.

Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

SMEJKAL, V. RAIS, K. Řízení rizik ve firmách a jiných organizacích. Praha: Grada, 2013. ISBN 978-80-247-4644-9.

TICHÝ, M. Ovládání rizika: analýza a management. Praha: C.H. Beck, 2006. ISBN 80-717-9415-5.

VÁCHAL, J., VOCHOZKA, M. Podnikové řízení. Praha: Grada Publishing, 2013. ISBN 978-80-247-4642-5.

ZUZÁK, R., KÖNIGOVÁ, M. Krizové řízení podniku. Praha: Grada Publishing, 2009. ISBN 978-80-247-3156-8.

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Martina Fejfarová, Ph.D.

Garantující pracoviště

Katedra řízení

Elektronicky schváleno dne 22. 12. 2017

prof. Ing. Ivana Tichá, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 12. 1. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 17. 02. 2018

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Metodika hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Martině Fejfarové, Ph.D. za odborné vedení, pomoc a její čas při zpracování této diplomové práce. Poděkování také patří všem, kteří mi v průběhu zpracování poskytovali cenné rady a mé rodině a blízkým, kteří mě po celou dobu studia morálně podporovali.

Metodika pro Posouzení vlivu na ochranu osobních údajů

Abstrakt

Diplomová práce se zabývá problematikou procesu řízení rizik a jejím hlavním cílem je vytvořit metodiku hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů dle 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, ve spolupráci s poradenskou společností Taylor McCoy, s.r.o. zabývající se poskytováním služeb v oblasti informační bezpečnosti. Dílčím cílem této práce je návrh postupu při výběru opatření k řešení těchto rizik, včetně opatření a mechanismů k zajištění ochrany osobních údajů fyzických osob a k doložení souladu s tímto Nařízením.

Práce je členěna do dvou základních částí. Teoretická část práce je zpracována na základě studia norem, standardů řízení rizik, zmíněného Nařízení Evropského parlamentu a Rady (EU) 2016/679, a rovněž odborné literatury, která obsahuje především knižní zdroje s tématikou procesu řízení rizik se zaměřením na informační bezpečnost a ochranu osobních údajů. Praktická část se zabývá vytvořením metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů a návrhem postupu při výběru opatření k řešení těchto rizik, včetně opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto Nařízením. Výsledky praktické části diplomové práce byly předloženy uvedené společnosti.

Klíčová slova: Riziko, Proces řízení rizik, Hodnocení rizik, Posouzení vlivu na ochranu osobních údajů, GDPR

Methodology for risk assessment for Data protection impact assessment

---

Abstract

The thesis deals with the process of risk management and the main target of this thesis is to develop a methodology of risk assessment for Data protection impact assessment according to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ES in cooperation with the company Taylor McCoy, s.r.o. dealing with information security. The partial target of this thesis is to propose a procedure for the selections of measures to these risks, including controls and mechanisms to ensure the protection of personal data of individuals and to demonstrate compliance with this Regulation.

The work is divided into two basic parts. The theoretical part is processed based on the study of norms and standards of risk management, mentioned Regulation and likewise study of technical literature on the theme of risk management process with a focus on information security and protection of personal data of individuals. The practical part is focused on developing a methodology of risk assessment for Data protection impact assessment and proposing a procedure for the selections of measures to these risks, including controls and mechanisms to ensure the protection of personal data of individuals and to demonstrate compliance with this Regulation. The outputs of the practical part of the thesis were discussed and submitted by management of the company.

Keywords: Risk, Risk management process, Risk assessment, Data Protection Impact Assessment, General Data Protection Regulation

OBSAH

Seznam schémat

Seznam tabulek

1 Úvod

Hospodářská a sociální integrace, která vyplývá z fungování vnitřního trhu, v posledních letech vedla ke značnému nárůstu přeshraničních toků osobních údajů. Výměna osobních údajů mezi veřejnými i soukromými aktéry se zvýšila v celé Evropské Unii. Tato globalizace a rychlý technologický rozvoj s sebou přináší nové výzvy pro oblast ochrany osobních údajů, jelikož rozsah shromažďování a sdílení osobních údajů významně narostl. Technologie umožňují jak soukromým subjektům, tak i orgánům veřejné moci využívat k provádění svých činností osobní údaje v nebývalém rozsahu. Také fyzické osoby zveřejňují své osobní údaje stále častěji, a to v globálním měřítku. Tyto technologie změnily společenský život i ekonomiku a měly dále usnadňovat volný pohyb osobních údajů jak v rámci Evropské Unie, tak i předávání do třetích zemí a mezinárodních organizací, ale zároveň by měly zajistit odpovídající úroveň ochrany osobních údajů. Takovýto vývoj vyžaduje pevný a soudržný rámec pro ochranu osobních údajů v celé Unii, který by umožnil rozvoj digitální ekonomiky na celém vnitřním trhu a zároveň by posílil právní i praktickou jistotu fyzický osob, hospodářských subjektů a orgánů veřejné moci.

Aby byla zajištěna jednotná a vysoká úroveň ochrany fyzických osob v souvislosti se zpracováním osobních údajů v celé Unii a odstranily se překážky bránící volnému pohybu osobních údajů v rámci vnitřního trhu, bylo nezbytné přijmout nařízení, které zajistí soudržné a rovnocenné uplatňování pravidel ochrany základních práv a svobod fyzických osob ve všech členských státech v souvislosti se zpracováním jejich osobních údajů, zpracovatelům údajů uloží povinnosti a úkoly, které zajistí důkladné kontrolování a monitorování zpracování osobních údajů a také rovnocenné sankce ve všech členských státech Unie.

Nařízení Evropského parlamentu a Rady (EU) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES bylo přijato 27. dubna 2016 s platností od 25. května 2018. Toto nařízení (General Data Protection Regulation, dále jen GDPR) nahrazuje směrnici na ochranu osobních údajů 95/46/ES a přináší tak dosud největší revoluci v ochraně osobních údajů s cílem chránit práva občanů EU proti neoprávněnému zacházení s jejich daty a osobními údaji.

2 Cíl práce a metodika

Hlavním cílem diplomové práce je na základě studia norem, standardů řízení rizik a Nařízení Evropského parlamentu a Rady (EU) 2016/679 (General Data Protection Regulation) vytvořit metodiku hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů dle zmíněného Nařízení ve spolupráci s poradenskou společností Taylor McCoy, s.r.o. zabývající se poskytováním služeb v oblasti informační bezpečnosti.

Mezi dílčí cíle patří:

- vypracování literární rešerše k dané problematice,
- charakteristika vybrané společnosti,
- realizace osobních rozhovorů,
- návrh postupu výběru opatření k řešení rizik včetně opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto Nařízením.

Diplomová práce je členěna do dvou částí, na část teoretickou a praktickou. Teoretická část práce byla zpracována na základě studia norem, standardů řízení rizik, Nařízení Evropského parlamentu a Rady (EU) 2016/679, výkladových pokynů pracovní skupiny WP29, jež vydává dokumenty ke zmíněnému Nařízení, a rovněž odborné literatury, která obsahuje především knižní zdroje s tématikou procesu řízení rizik se zaměřením na informační bezpečnost a ochranu osobních údajů. V této části diplomové práce byly nejprve zpracovány informace ohledně obecného procesu řízení rizik, včetně identifikace aktiv, hrozeb a zranitelností, a metod výpočtu rizik. Poté se práce zabývá charakteristikou obecných principů ochrany soukromí, jež jsou dalším východiskem GDPR. Následně byla pozornost zaměřena na problematiku Nařízení GDPR, charakteristiku rizik v kontextu GDPR a jejich identifikaci a ošetření se zvláštním zřetelem na rizika subjektů údajů. Součástí je rovněž zpracování specifik procesu řízení rizik ochrany osobních údajů v kontextu GDPR, jež se liší oproti obecnému procesu.

Praktická část diplomové práce byla zpracována na základě studia doporučovaných metodik pro posuzování rizik v oblasti osobních údajů (např. metodiky vydané francouzským dozorovým úřadem CNIL nebo britským ICO), Nařízení Evropského parlamentu a Rady (EU) 2016/679 a výkladových pokynů pracovní skupiny WP29. Dále vychází ze zpracované literatury popsané v teoretické části práce, z analýzy relevantních interních dokumentů

zabývajícími se řízením rizik a z osobních rozhovorů s odpovědnými pracovníky. Rozhovory s bezpečnostním manažerem a bezpečnostním správcem probíhaly v předem stanoveném termínu a odehrávaly se v prostorách společnosti. Otázky byly předem připravené a standardizované (viz Příloha č. 1). Odpovědi byly písemně zaznamenány a využity pro následné zpracování.

Nejprve byla provedena charakteristika zvolené společnosti, popis jejího organizačního uspořádání, včetně orientace podnikatelských aktivit a dokumentační základny. Přesné informace ohledně aktivit společnosti a jejích dalších charakteristik byly zpracovány na základě informací poskytnutých v rámci osobních rozhovorů s bezpečnostním manažerem a bezpečnostním správcem. Dále je dle studia relevantních interních dokumentů popsán současný stav procesu řízení rizik a pravidla ochrany osobních údajů, jimiž se společnost řídí.

V další části práce je vytvořena metodika hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů, která vychází z principů uvedených v ČSN ISO/IEC 27005 (1) a ISO/IEC 29134 (20) s přihlédnutím k náležitostem Posouzení vlivu na ochranu osobních údajů (Příloha č. 2), jež mohou být použita k prokázání, že konkrétní metodika je dostatečně komplexní a splňuje standardy požadované Nařízením. Harmonogram postupu vytvoření této metodiky je uveden v kapitole 4.3.1. Dále je na základě studia normy ISO/IEC 29151 (23) zpracován návrh postupu výběru opatření k řešení těchto rizik, včetně opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto Nařízením. Výsledky praktické části diplomové práce byly předloženy uvedené společnosti.

3 Teoretická východiska

GDPR vychází ze dvou východisek, a to z obecných rámců řízení rizik a ochrany soukromí. Pro účely vytvoření metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů byly zvoleny principy řízení rizik a ochrany soukromí formalizované normami ISO, konkrétně ISO/IEC 27005 (1) (Řízení rizik bezpečnosti informací) a ISO/IEC 29100 (2) (Obecný rámec ochrany soukromí). V následujících kapitolách jsou popsány obecné principy obou konceptů a vztaženy k problematice Nařízení GDPR (3).

3.1 Riziko a jeho možné definice

Význam a pojetí rizika prošlo určitým historickým vývojem. Podle Merny a kol. (4) můžeme o původu slova „riziko“ uvažovat jako o arabském slově *risq*, nebo jako o latinském slově *riscum*. Arabské slovo *risq* mělo význam náhodného a příznivého výsledku, zatímco latinské *riscum* se vztahovalo k pochybnosti, jakou může představovat korálový útes pro lodní dopravu. Riziko tedy bylo spojováno s náhodnými, ale i nepříznivými událostmi a odvahou podstoupit nebezpečí. Řecká odvozenina arabského slova *risq*, jež se používala ve dvanáctém století, byla spojována jak s negativními, tak pozitivními výsledky či událostmi. Pozdější vývoj pojetí rizika v 17. až 20. století se pohyboval spíše ve spojení s negativními výsledky. Na základě dnešních výkladů se rizikem obecně rozumí nebezpečí, nebezpečí vzniku škody, pravděpodobnost či možnost vzniku ztráty nebo odchýlení skutečných a očekávaných výsledků.

Tichý (5) souhlasí s tvrzením Merny a kol. (4), že v dnešní době se riziko chápe především jako určité nebezpečí a dodává, že pojmy „nebezpečí“ a „riziko“ jsou velice často zaměňovány anebo se oběma připisuje týž význam. Jejich definice jsou ale pozoruhodné tím, že za riziko jsou považovány i „kladné“ odchylky od očekávané hodnoty. To je logické, protože často realizace nebezpečí, které je pro určitou osobu nepříznivé, je současně pro jinou osobu příznivé. Za riziko se považuje míra nebo stupeň ohrožení, zdroj nebezpečí, pravděpodobnost vzniku příslušné újmy, objekt vystavený nebezpečí nebo možná nejistá situace, která může mít kladný nebo záporný účinek na cíle projektu.

Smejkal a Rais (6) uvádí, že například finanční teorie obvykle definuje riziko jako volatilitu finanční veličiny (zisku, hodnoty portfolia atd.) okolo očekávané hodnoty v důsledku změn

určitých parametrů. Obecně lze riziko vyjádřit jako situaci, ve které existuje možnost nepříznivé odchylky od žádoucího výsledku, který očekáváme.

Jiný pohled na pojetí rizika poskytuje Hnilica a Fotr (7), jež se zaměřují na podnikatelská rizika. Předpokládají, že odchylky výsledků podnikatelské činnosti od výsledků předpokládaných jsou žádoucí (směřují k vyššímu zisku), nežádoucí (směřují ke ztrátě), nebo odlišné velikosti. A to od malých odchylek, kdy se výsledky blíží k výsledkům předpokládaným, až k odchylkám velkého rozsahu, což může znamenat významné finanční obtíže nebo úpadek v případě nežádoucí odchylky.

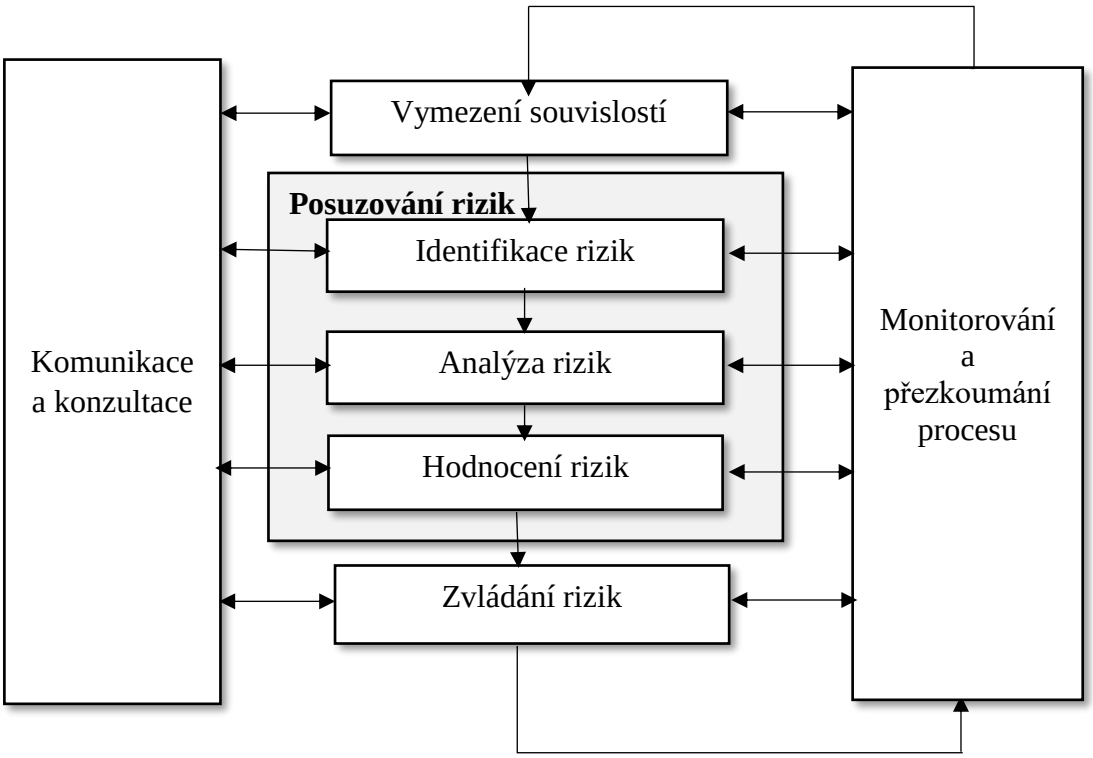
3.1.1 Posouzení rizik

Posouzení rizik umožňuje prioritizaci rizik na základě vnímané důležitosti, která kvantifikuje riziko nebo jej kvalitativně popisuje. Zároveň také určuje význam a hodnotu aktiv, identifikuje hrozby a možné zranitelnosti. Analyzuje účinky stávajících opatření na identifikované riziko, na základě toho stanoví potenciální dopady a navrhne prioritu rizik (1).

Podle Zuzáka a Königové (8) řízení rizik nelze chápat jako činnost jednorázovou či periodickou, ale jako permanentní aktivitu, při které jsou rizika nejen identifikována a popisována, ale také analyzována, vyhodnocována a pravidelně monitorována. Merna a kol. (4) souhlasí a zároveň doplňují, že posouzení rizik zahrnuje organizovaný proces, který zajišťuje systematické zjišťování, analyzování, hodnocení a kontrolu odezvy na rizikové události, a to po celou dobu trvání určitého projektu.

Při procesu posouzení rizik je snaha zamezit působení již existujících i budoucích faktorů a zároveň je navrhováno řešení, které pomůže eliminovat důsledek nežádoucích vlivů a také umožní využít příležitosti pro působení pozitivních vlivů. Rozhodovací proces, který vychází z analýzy rizik, je součástí procesu posouzení rizik. Po zvážení zejména ekonomických, sociálních a technických faktorů následuje vývoj a srovnání možných vhodných opatření. Poté se z nich vybere to, které bude existující riziko minimalizovat a snižovat závažnost jeho dopadu. Výstupem jsou tedy ohodnocená rizika, která byla prioritizována na základě stanovených kritérií hodnocení rizik (6).

Schéma č. 1 – Proces řízení rizik



Zdroj: vlastní zpracování dle (9)

Posouzení rizik se tedy skládá z následujících činností:

- identifikace rizik,
- analýza rizik,
- hodnocení rizik (1).

3.1.1.1 Identifikace rizik

Dle Merny a kol. (4) je identifikace rizik nejdůležitějším a zároveň časově nejnáročnějším krokem v rámci podrobné analýzy rizik a jejich alokací. Zároveň platí, že identifikace rizik je aktivitou zčásti periodickou (identifikace určitých rizik se opakuje ve stanovených intervalech) a zčásti průběžnou.

Proces identifikace rizik je závislý na informacích, které nemusí být vždy snadno dostupné, a proto platí, že čím je lepší informační základna procesu řízení rizik, tím jsou výsledky přesnější (4). S tímto faktem souhlasí i Hnilica a Fotr (7) a dodávají, že v dalších fázích řízení rizik lze pracovat jen s riziky, která byla včas zjištěna, zaznamenána a zhodnocena.

Hlavním cílem identifikace rizik je poskytnout vyčerpávající soubor rizikových faktorů, které by mohly mít vliv na hospodářské nebo jiné výsledky firmy nebo hodnotu jejich aktiv. Jedná se zejména o rizika, která mohou negativně, ale i pozitivně ovlivnit hospodářské či jiné výsledky organizace (7).

3.1.1.2 Identifikace aktiv a vlastníků

Aktivum představuje určité hodnoty, které jsou pro organizaci důležité a je tedy nutno je chránit. Ke každému aktivu by měl být identifikován vlastník aktiva pro zajištění záruky a odpovědnosti za aktivum. Vlastník aktiva k němu sice nemá vlastnická práva, ale má přiměřenou odpovědnost za jeho vývoj, produkci a bezpečnost (1).

Cílem ohodnocení aktiv je stanovit kvalitativní hodnotu skupiny aktiv, která je určována podle pořizovacích nákladů aktiv, resp. reprodukční pořizovací ceny, nákladů na nákup zničených nebo obnovu poškozených aktiv, důležitosti aktiva pro existenci subjektu, finančních i nefinančních škod v případě havárie, přírodní katastrofy apod. Výstup ohodnocení aktiv je poté zaznamenán v Registru aktiv (6).

Podle normy ČSN ISO/IEC 27005 (1) je cílem identifikace aktiv vytvořit a udržovat strukturovaný seznam aktiv a jejich charakteristik. Výstupem identifikace aktiv by měl být seznam aktiv, u kterých je potřeba zajistit řízení rizik, a důležitost procesů činností, jež se k aktivům vztahují. Tento výstup identifikace aktiv je zaznamenán v Registru aktiv.

3.1.1.3 Identifikace hrozeb

Aktiva jsou předmětem působení mnoha typů hrozeb. Hrozba má potenciální schopnost způsobit nežádoucí incident, který může mít za následek narušení dostupnosti, důvěrnosti či integrity aktiv. Hrozbu identifikujeme, formulujeme a hodnotíme jako potenciální příčinu nechtěného incidentu, který může vyústit v poškození aktiva. Hrozby mohou mít přírodní či lidský původ. V případě lidských hrozeb mohou být úmyslné nebo náhodné. Některé hrozby mohou poškodit více než jedno aktivum. V těchto případech mohou mít různý dopad, podle toho, jaká aktiva byla zasažena. Dopad hrozby je důsledek nežádoucího incidentu, způsobeného buď náhodně, nebo úmyslně, který má vliv na aktiva. Možné následky zahrnují hmotné ztráty nebo jiné negativní vlivy na chod organizace (1).

K podstatě hrozby patří především překonání bezpečnostních opatření, využití zranitelností a působení na aktivum, kde způsobí škodu. Riziko je poté kvantifikací působení hrozeb na aktivum, přičemž riziko, které zůstává i po zavedení bezpečnostních opatření představuje zbytkové riziko (9). Smejkal a Rais (6) dále doplňují, že základní charakteristikou hrozby je její úroveň, která se hodnotí podle následujících faktorů:

- nebezpečnost – schopnost způsobit škodu;
- přístup – obtížnost zasažení aktiva hrozbou;
- motivace – zájem na realizaci uvedené hrozby vůči aktivu.

Zdrojem hrozby je podle Řeháka (9) jakýkoliv faktor, který může působit na procesy nebo cíle organizace. Rozlišujeme tedy vnější činitele a vnitřní prvky organizace, které způsobují aktivaci konkrétní hrozby, jež je poté příčinou možných nežádoucích dopadů na aktivum dané organizace.

Podle normy ČSN ISO/IEC 27005 (1) lze vstup k identifikaci hrozeb a pravděpodobnosti výskytu získat od pracovníků lidských zdrojů, uživatelů aktiv či jejich vlastníků. Výstupem identifikace hrozeb by měl být seznam hrozeb s identifikací zdroje a typu hrozby.

3.1.1.4 Identifikace zranitelností

Zranitelnosti spojené s aktivy představují slabá místa na úrovni fyzické, organizační, procesní, personální nebo technologické. Zranitelnost nemusí vyžadovat přijetí opatření, pokud nemá odpovídající hrozbu, avšak měla by být monitorována pro případ, že by došlo ke změně. Opatření, které je nefunkční nebo se nepoužívá správně, může samo o sobě představovat zranitelnost. Zranitelnosti mohou být využity hrozbami, které mohou způsobit incident. Zranitelnost sama o sobě však není příčinou škody. Je pouze podmínkou, která může umožnit hrozbě, aby ovlivnila aktiva. Jestliže hrozba nemá odpovídající zranitelnost, nemusí vyústit v riziko (6).

Pokud nějaká hrozba využije zranitelnost nějakého aktiva, dojde k realizaci rizika formou bezpečnostního incidentu. Bezpečnostní incident je událost, která není standardní součástí procesu a je obvykle spojená s výpadkem dostupnosti informací nebo služby, narušení důvěrnosti nebo integrity informací. Výstupem identifikace zranitelností je seznam zranitelností ve vztahu k aktivům, opatřením a hrozbám (1).

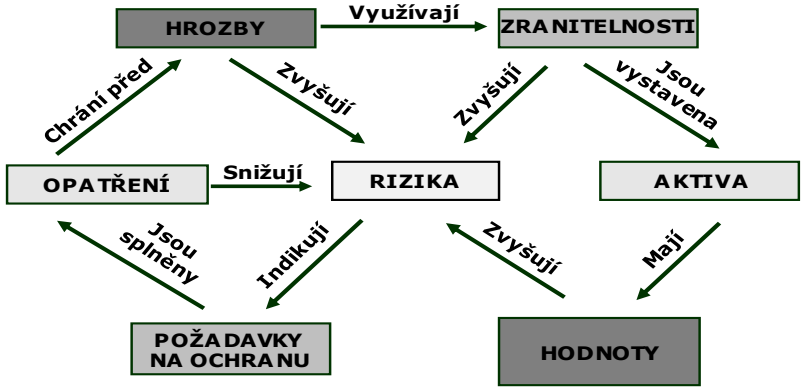
3.1.1.5 Identifikace stávajících opatření

Opatření jsou praktiky, postupy nebo mechanismy, které mohou snížit dopad rizika nebo přímo snížit riziko poskytnutím ochrany před hrozbou, snížením zranitelnosti aktiva, snížením pravděpodobnosti vzniku mimořádného incidentu nebo omezením jeho dopadu. Měla by být provedena i identifikace stávajících opatření, která již byla učiněna, aby se předešlo zbytečným nákladům např. při duplikaci opatření. Zároveň by měla být provedena kontrola správné funkčnosti opatření, pokud totiž opatření nefunguje dle předpokladů, může způsobit zranitelnost. Pro odhadnutí účinnosti opatření je nutné zjistit, jak snižuje pravděpodobnost hrozby, dopad incidentu nebo snadnost zneužití zranitelností. Pokud je existující či plánované opatření identifikováno jako nedostačující nebo neúčinné, mělo by se toto opatření zkontrolovat a určit, zda by nemělo být odstraněno nebo nahrazeno jiným vhodnějším opatřením. Výstupem identifikace stávajících opatření by měl být seznam plánovaných a existujících opatření, jejich zavedení a stav užívání (1).

3.1.1.6 Shrnutí vztahů v managementu rizik

Skutečnosti působící v managementu rizik informační bezpečnosti a hlavní vztahy mezi nimi vyjadřuje následující schéma:

Schéma č. 2 – Skutečnosti působící v managementu rizik informační bezpečnosti



Zdroj: vlastní zpracování, upraveno dle (6)

Riziko je potenciální možnost, že daná hrozba využije zranitelnost aktiva (tj. nastane incident), a zároveň způsobí ztrátu nebo poškození aktiva (tj. má nežádoucí dopad). Míra (úroveň) rizika je tedy daná kombinací tří faktorů, pravděpodobností výskytu nežádoucího

incidentu (úrovní hrozby), úrovní zranitelnosti a hodnotou aktiva, tedy míry dopadu nežádoucího incidentu. Tyto tři faktory se podílí na růstu míry rizika a pouze ochranná opatření působí na snížení jeho míry (6).

3.1.2 Analýza rizik

Analýza rizik podle Merny a kol. (4) zahrnuje vyhodnocení rizik a také vzájemné působení rizik při vyhodnocování možných výstupů. V první řadě vyžaduje určení, zda riziková událost zaručuje odezvu. Hlavním výstupem analýzy rizik je seznam příležitostí, jež se musí sledovat, a ohrožení, která vyžadují pozornost. Tento proces analýzy rizik musí zároveň zdokumentovat zdroje rizik a rizikové události, které byly řídícím týmem vědomě přijaty či ignorovány.

Důvodem pro analýzu rizik je zmapování aktuálního stavu řízení rizik, identifikace nedostatků a vytvoření podkladů pro následnou správu rizik a zpracování plánu zvládání rizik (10). Řehák (9) doplňuje, že analýza rizik poskytuje vstupy pro zhodnocení rizik a následné rozhodnutí, zda je identifikované riziko zvladatelné, případně jaké jsou metody pro zvládání rizik a nejvhodnější strategie pro případný další kontrolovaný vývoj událostí. Dle Smejkala a Raise (6) je chápána jako proces zjišťování nebezpečí, kterému je organizace vystavena, jaké škody mohou případná rizika napáchat a pravděpodobností dopadu na aktiva a jejich uskutečnění, tzn. určení rizik a jejich závažnosti.

Analýza rizik může být prováděna v různých stupních podrobnosti v závislosti na rozsahu zranitelnosti, předcházejících incidentech a také na kritičnosti aktiv. V závislosti na okolnostech může být analýza rizik kvalitativní, kvantitativní nebo kombinací obou. V praxi je většinou nejprve používána kvalitativní analýza pro odhalení větších rizik a získání indikace úrovně rizika. Provést kvalitativní analýzu je obvykle méně nákladné a složité, než kvantitativní analýza (1).

3.1.3 Hodnocení rizik

Hodnocení rizik je závěrečnou fází procesu posouzení rizik a jak uvádí Hnilica a Fotr (7), podklady pro posouzení rizika spojeného s určitým objektem, totiž zda je přijatelné nebo nepřijatelné, poskytují výsledky analýzy rizik. S tímto faktem souhlasí i Řehák (9) a doplňuje, že smyslem hodnocení rizik je napomáhat procesu rozhodování o tom, jaká rizika by měla být zvládána přednostně.

Vstupem pro hodnocení rizik by tedy dle normy ČSN ISO/IEC 27005 (1) měl být seznam rizik se stanovenými kritérii pro jejich hodnocení a přiřazenými úrovněmi hodnot identifikovaných rizik. Následně se porovnají úrovně hodnot rizik s kritérii pro hodnocení rizik a na základě toho se stanoví přijatelnost rizik a jejich prioritizace. Pokud úroveň hodnoty rizika nesplňuje kritéria, riziko musí být zvládáno. Rozhodnutí učiněná v rámci této fáze hodnocení rizik jsou tedy založena na stanovené **akceptovatelné úrovni rizik**. Výstupem hodnocení rizik by měl být seznam rizik, kterým byla stanovena priorita podle kritérií hodnocení rizik v souvislosti se scénáři událostí, které k těmto rizikům vedou.

Dle Smejkala a Raise (6) mohou výsledky hodnocení rizik pomoct určit následující kroky pro zvládání rizik a rovněž pro zavedení nápravných opatření určených ke snížení jejich výskytu.

Matice hodnocení rizik

Základem matice hodnocení rizik je expertní posuzování významnosti rizik pracovníky, jež mají dostatek znalostí a zkušeností v oblastech, kam dosahují jednotlivá rizika. Tato významnost, která je podstatou expertního posuzování, se posuzuje na základě dvou hledisek. První hledisko tvoří pravděpodobnost výskytu rizika a k druhému patří intenzita negativního dopadu rizika na danou organizaci, subjekt či jejich aktiva. Riziko je poté tím významnější, čím je větší pravděpodobnost jeho výskytu a čím je vyšší intenzita negativního dopadu rizika na organizaci či jiný subjekt. Toto expertní posuzování významnosti faktorů rizika může mít více forem. Mezi základní formu patří kvalitativní hodnocení, které matici hodnocení rizik zobrazuje v grafické podobě a nevyjadřuje tedy významnost rizika v číselné formě. Další formou je semikvantitativní hodnocení, které naopak vyjadřuje významnost faktorů rizika pomocí číselné formy také s využitím matice hodnocení rizik (7).

Zuzák a Königová (8) doplňují, že do matice hodnocení rizika jsou zaznamenávána vnitřní i vnější rizika organizace. Ke každému takovému riziku musí být stanoveno dané časové období, pravděpodobnost výskytu i závažnost dopadu rizika na organizaci či její aktiva. Rizika jsou poté zanesena do matice hodnocení rizik, z čehož následně vyplývají rizika, jež se mohou stát ohniskem krize.

3.1.4 Zvládání rizik

Podle normy ČSN ISO/IEC 27005 (1) je vstupem pro zvládání rizik seznam rizik, jimž byla udělena priorita podle stanovených kritérií hodnocení rizik. V rámci subprocesu zvládání rizik by měl být definován plán zvládání rizik, který rozpracovává postupy pokrytí identifikovaných rizik, jež převyšují stanovenou míru akceptovatelného rizika, a zároveň definuje pořadí priorit, v němž by měly být aplikovány vybrané způsoby zvládání rizik a to včetně jejich časových rámců. Po definování plánu zvládání rizik by měla být určena zbytková rizika. Jelikož se identifikace i hodnocení hrozeb a zranitelností aktiva provádí z pohledu, jako by nebylo aplikováno žádné bezpečnostní opatření, hodnota aktuálního (zbytkového) rizika se určí následně formou identifikace a stanovením míry účinnosti stávajících zavedených bezpečnostních opatření. Je tedy třeba zjistit, zda zbytkové riziko stále nesplňuje kritéria pro akceptaci rizik, v takovém případě by bylo nezbytné opakovat další zvládání rizik, než by se mohlo přejít k akceptaci rizik.

Řehák (9) souhlasí s tím, že zvládání rizik je cyklický subproces procesu řízení rizik a spočívá v opětovném posuzování zvládání rizik s ohledem na přijatá nápravná opatření a rozhodnutí, zda je zbytková úroveň rizika akceptovatelná či nikoliv. Pokud toto riziko akceptovatelné není, je potřeba znovu provést zvládání rizik a následně ověřit jeho účinnost. Měla by tedy být stanovena opatření, která povedou k podstoupení, redukci, přenosu nebo vyhnutí se riziku. Zvládání rizik trvá tak dlouho, dokud zbytková úroveň rizika nedosáhne akceptovatelné úrovně, která by odpovídala stanoveným kritériím hodnocení rizik.

Každý ze způsobů zvládání rizik by měl být použit v případě, kdy představuje nejméně nákladný způsob pro dosažení určitého cíle ve formě úplné eliminace rizika nebo jeho snížení. Tyto způsoby by tedy měly být v souladu s očekávanými náklady na jejich implementaci a rovněž s očekávanými přínosy, které by vyplývaly z těchto způsobů (6).

Modifikace rizika

V rámci modifikace rizika by měla být vybrána, odstraněna nebo upravena opatření, která by vedla k jeho snížení pod akceptovatelnou úroveň a k možnosti následné akceptace zbytkového rizika. Tato opatření musí být účinná, přijatelná z hlediska etiky, ekologie a právního řádu. Dále musí být efektivní a včasná - připravena před naplněním hrozby (6).

Podstoupení rizika

Jak uvádí norma ČSN ISO/IEC 27005 (1, s. 27): „*Jestliže úroveň rizik splňuje kritéria akceptace rizik, není zapotřebí přijímat další opatření a riziko lze podstoupit.“* Vstupem pro akceptaci rizik jsou rizika, která jsou v analýze rizik označena jako akceptovatelná. Výstupem je odsouhlasený seznam akceptovaných rizik s jejich odůvodněním. Akceptace rizik musí být formálně zaznamenána, schválena. V případě akceptace rizika musí být jednoznačně dohledatelná odpovědnost za dané rozhodnutí (např. autor návrhu akceptace rizika, projednání, formální akceptace).

Podle Smejkala a Raise (11) se podstoupení (retence) rizika člení na riziko podstoupené vědomě a nevědomě. Vědomě riziko podstoupíme, pokud ho rozpoznáme, ale neuplatníme proti němu žádné opatření. Naopak pokud riziko nerozpoznáme a nevědomky ho zadržíme, jedná se o riziko podstoupené nevědomě.

Sdílení rizika

Přesun rizika je podle Smejkala a kol. (6) i Řeháka (9) defenzivním přístupem k riziku, přičemž základním rysem je přesun rizika na ekonomicky silnější subjekt, který je schopen toto riziko účinněji zvládat. Mezi nejčastější formy přesunu rizika patří leasing, franšíza, odkup pohledávek – faktoring, forfaiting nebo uzavírání obchodních smluv s partnerem, který bude zajišťovat dozor nad systémem a bude schopen přijmout okamžitá opatření k nápravě. Je důležité podotknout, že je možné sdílet odpovědnost za zvládnutí rizika, ale nelze sdílet odpovědnost za jeho dopad.

Vyhnutí se riziku

Podle normy ČSN ISO/IEC 27005 (1) vyhnutí se riziku znamená, že by se organizace měla vyvarovat obchodu, činnosti, projektu, který by mohl dát vzniknout riziku. Tento způsob zvládání rizik je sice metodou velmi defenzivní, ale měl by se uplatňovat v případě, že rizika z naplnění hrozby jsou příliš vysoká nebo náklady na implementaci bezpečnostních opatření převyšují přínosy.

3.1.5 Monitorování rizik

Monitorování a neustálé přezkoumávání rizik je potřeba považovat za nezbytnou součást procesu řízení rizik. Vstupem pro monitorování a přezkoumávání rizikových faktorů jsou

veškeré informace o rizicích zjištěných při provádění všech činností řízení rizik. Monitorování rizik je důležité pro detekci změn hrozeb, dopadů, zranitelností či pravděpodobností výskytu, která se mohou změnit náhle, bez jakéhokoliv předchozího náznaku. Dle normy ČSN ISO/IEC 27005 (1, s. 28): *„Měla by být monitorována a přezkoumávána rizika a jejich faktory (např. hodnota aktiv, dopady, hrozby, zranitelnosti, pravděpodobnost výskytu), aby bylo možno v raném stádiu identifikovat jakékoliv změny v kontextu společnosti a udržovat přehled komplexního obrazu rizik“.*

Podle Řeháka (9) je nezbytnou součástí monitorování rizik neustálé zaznamenávání, aby mohly být všechny doklady o provedení jednotlivých činností snadno dohledatelné. Tyto záznamy nám poté poskytují základ pro zlepšování nástrojů a metod, ale také celého procesu.

3.2 Obecný rámec ochrany soukromí

Vzhledem k rostoucímu počtu informačních a komunikačních technologií, které zpracovávají osobní údaje, zvyšujícímu se komerčnímu užití a sdílení osobních údajů může být pro společnosti ochrana soukromí a dosažení souladu s různými platnými zákony komplexním a náročním úkolem. Cílem obecného rámce ochrany soukromí popsaného řadou norem ISO/IEC 29100 (2) je pomoci společnostem zvládat požadavky na ochranu osobních údajů v souvislosti s informačními technologiemi tím, že:

- stanoví společnou terminologii ochrany osobních údajů,
- definují zúčastněné osoby a jejich role při zpracování osobních údajů,
- popíší požadavky na ochranu soukromí,
- odkáží na známé zásady ochrany osobních údajů.

Následující oblasti týkající se soukromí a zpracovávání osobních údajů v ICT systémech tvoří rámec pro ochranu soukromí popsaný v řadě norem ISO/IEC 29100 (2).

a) aktéři a jejich role – je důležité určit subjekty zapojené do zpracování osobních údajů, jichž existují čtyři typy:
    - subjekty údajů – poskytují své osobní údaje ke zpracování správcům a zpracovatelům osobních údajů, a pokud to není v příslušných právních předpisech stanoveno jinak, dávají svůj souhlas k tomu, jak mají být jejich informace zpracovány. Subjekty údajů zahrnují například zaměstnance uvedené v systému lidských zdrojů společnosti či spotřebitele uvedené

v úvěrové smlouvě. Není vždy nutné, aby byla daná fyzická osoba identifikována přímo jménem, ale může být identifikována i nepřímo např. prostřednictvím čísla účtu, čísla sociálního zabezpečení apod.

- správce osobních údajů – určují za jakým účelem a jak budou zpracovávat osobní údaje subjektů údajů a v rámci toho musí zajistit dodržování zásad ochrany osobních údajů v průběhu celého zpracování. Správce by měl pečlivě posoudit, zda zpracovává citlivé osobní údaje a zavádí přiměřené kontroly ochrany soukromí a bezpečnosti založené na požadavcích stanovených v příslušné jurisdikci, stejně jako případné nepříznivé důsledky plynoucí pro subjekty údajů zjištěné při hodnocení rizika ochrany osobních údajů.
- zpracovatel osobních údajů – provádí zpracování osobních údajů jménem správce a jedná v souladu s jeho pokyny. Dodržuje stanovené požadavky na ochranu soukromí a provádí příslušné kontroly.
- třetí strana – může přijímat osobní údaje od správce či zpracovatele osobních údajů. Obvykle se třetí strana stane správcem poté, co obdrží dané osobní údaje.

b) interakce a vzájemná spolupráce – role identifikované výše mohou vzájemně spolupracovat různými způsoby. Pokud jde o možné toky osobních údajů mezi subjekty údajů, správci, zpracovateli a třetími stranami, existují následující scénáře:
   - subjekt údajů poskytuje své osobní údaje správci (např. při registraci služby poskytované správcem),
   - správce poskytuje osobní údaje zpracovateli, jenž je zpracovává jeho jménem a na základě jeho pokynů (např. jako součást dohody o outsourcingu),
   - subjekt údajů poskytuje své osobní údaje zpracovateli, který je dále zpracovává jménem správce,
   - správce poskytuje subjektu údajů osobní údaje, které s ním souvisejí (např. na základě požadavku subjektu údajů o jejich předložení),
   - zpracovatel poskytuje osobní údaje subjektů údajů (např. na základě pokynů správce),
   - zpracovatel poskytuje osobní údaje správci (např. po provedení služby, pro kterou byl určen),

- správce poskytuje osobní údaje třetí straně (např. v rámci obchodní smlouvy),
- zpracovatel poskytuje osobní údaje třetí straně (např. podle pokynů správce).

c) rozpoznání osobních údajů – aby bylo možné určit, zda by měla být fyzická osoba považována za osobu identifikovatelnou, je třeba vzít v úvahu několik faktorů. Zejména všechny prostředky, jež mohou rozumně využívat účastníci, kteří jsou držiteli těchto údajů, nebo kterákoliv jiná strana, aby tuto fyzickou osobu identifikovali. Následující body poskytují vysvětlení jak určit, zda se jedná o osobní údaj, a je tudíž třeba považovat fyzickou osobu za identifikovatelnou:
   - pokud údaj obsahuje informace nebo je spojen s identifikátorem, jenž jasně odkazuje na fyzickou osobu (např. číslo sociálního zabezpečení),
   - pokud údaj obsahuje informace nebo je spojen s identifikátorem, který může souviset s fyzickou osobou (např. číslo pasu, bankovního účtu),
   - pokud údaj obsahuje informace nebo je spojen s identifikátorem, který lze použít k vytvoření komunikace s danou fyzickou osobou (např. přesné zeměpisné umístění, telefonní číslo apod.),
   - pokud údaj obsahuje odkaz, který propojuje data s některým z výše uvedených identifikátorů.

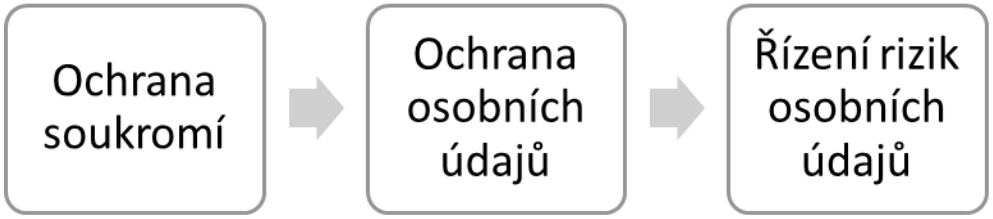
Pro účely obecného rámce ochrany soukromí je osobním údajem jakákoliv informace, která se týká určené nebo přímo či nepřímo určitelné fyzické osoby, pokud zasahuje do jejího soukromí. Informace bude považována za osobní údaj pokud obsahuje charakteristiku, jež odlišuje fyzickou osobu od jiných fyzických osob (např. biometrická data). Je důležité poznamenat, že určitá charakteristika odlišující fyzickou osobu od jiných fyzických osob se může měnit v závislosti na kontextu užívání. Například jestliže příjmení fyzické osoby může být nedostatečné k identifikaci této fyzické osoby v celosvětovém měřítku, bude často stačit k rozlišení této fyzické osoby v podnikovém měřítku (2).

Jakmile údaj obsahuje charakteristiku k určité identifikovatelné fyzické osobě, je třeba rozhodnout, zda informace o této fyzické osobě něco říkají, například pokud se týká jejích vlastností nebo chování. Příklady zahrnují lékařské záznamy, finanční profily nebo osobní zájmy vyplývající ze sledování používání internetových stránek. Rovněž jednoduché atributové prohlášení o fyzické osobě, jako je věk nebo její pohlaví, mohou propojené informace kvalifikovat za osobní údaj. Bez ohledu na to, zda lze zjistit vztah

s identifikovatelnou fyzickou osobou, musí být s těmito informacemi zacházeno také jako s osobním údajem (2).

Dle obecného rámce ochrany soukromí je rovněž důležité rozlišit citlivé osobní údaje, zahrnující informace odhalující rasu, etnický původ, náboženské či filosofické přesvědčení, politické názory, členství v odborových organizacích, sexuální orientaci nebo fyzické a duševní zdraví subjektu údajů. Dále mohou být za citlivé informace považovány údaje, jež obsahují informace, které by mohly usnadnit krádež totožnosti nebo jinak způsobit finanční škodu fyzické osobě (např. čísla kreditních karet, informace o bankovním účtu aj.) a informace, které by mohly být použity k určení polohy v reálném čase. Zpracování těchto citlivých informací vyžaduje zvláštní opatření. V některých právních jurisdikcích může být zpracování citlivých osobních údajů zakázáno platným zákonem nebo může být vyžadována implementace speficických prvků (např. šifrování lékařských osobních údajů při jejich přenosu) (2).

Schéma č. 3 – Obecný rámec ochrany soukromí



Zdroj: vlastní zpracování

d) požadavky na ochranu soukromí

Dle řady norem ISO/IEC 29100 (2) jsou společnosti motivovány k ochraně osobních údajů z různých důvodů, např. chránit soukromí společnosti, dodržovat právní a regulační požadavky, zvýšit důvěru spotřebitelů apod. Požadavky na ochranu soukromí se mohou vztahovat na mnoho různých aspektů zpracování osobních údajů, a to od jejich shromažďování a uchovávání, přenos třetím stranám, smluvní vztah mezi správci a zpracovateli až po mezinárodní přenos osobních údajů.

Požadavky na ochranu soukromí jsou identifikovány jako součást celkového procesu řízení rizik pro ochranu soukromí, který je ovlivněn právními a regulačními faktory pro ochranu soukromí fyzické osoby a ochranu jejich osobních údajů, smluvními, obchodními a dalšími faktory. V souvislosti s tím společnosti provádějí řízení rizik a rozvíjejí rizikové profily

spojené s jejich informačními systémy. Proces řízení rizik osobních údajů zahrnuje následující procesy:

- stanovení kontextu, porozumění technickému prostředí společnosti a faktorů ovlivňující řízení ochrany soukromí (tj. právní, smluvní, obchodní a další faktory),
- posouzení rizik jejich identifikací, analýzou a vyhodnocením rizik osobních údajů,
- ošetření rizik, a to vymezením požadavků na ochranu osobních údajů, implementací příslušných opatření k vyhnutí se nebo snížení rizik vůči dotčeným subjektům údajů,
- sdělování a konzultace o každém procesu řízení rizik a informování subjektů údajů o rizicích a opatřeních,
- monitorování a přezkoumávání sledovaných rizik osobních údajů a opatření pro následné zlepšení procesu řízení rizik (2).

Jedním z výstupů může být posouzení dopadů na soukromí. Posouzení dopadu ochrany soukromí by mělo být součástí širšího rámce řízení rizik společnosti.

e) opatření na ochranu soukromí

Společnosti by měly stanovit a provádět daná opatření tak, aby splňovaly požadavky na ochranu osobních údajů, jež byly stanoveny v procesu posuzování a zpracování rizik v oblasti ochrany soukromí. Je důležité poznamenat, že ne všechny operace zpracování osobních údajů vyžadují stejnou úroveň a typ ochrany, některé typy zpracování osobních údajů mohou vyžadovat specifická opatření, jejichž potřeba se projeví až po pečlivé analýze předpokládané operace. Společnost by měla rozlišovat mezi jednotlivými operacemi zpracování osobních údajů podle konkrétních rizik, která představují, aby mohla správně určit vhodná opatření pro konkrétní případy (2).

3.3 General Data Protection Regulation

Listina základních práv Evropské Unie a Smlouva o fungování Evropské unie (EU) přiznávají každému právo na ochranu osobních údajů, které se jej týkají. K zajištění tohoto práva bylo přijato 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).

Ačkoliv cíle a zásady směrnice 95/46/ES, ze které vychází i zákon České republiky č. 101/2000 Sb. (o ochraně osobních údajů), stále platí, nezabránilo to roztříštěnosti v provádění ochrany osobních údajů v celé Unii, právní nejistotě a rozšířenému pocitu veřejnosti, že v souvislosti s ochranou fyzických osob existují značná rizika, zejména pokud se jedná o činnosti prováděné online. Práva jednotlivců k ochraně jejich osobních údajů jsou tímto novým Nařízením výrazně posílena, čemuž odpovídají i nové povinnosti správců a zpracovatelů osobních údajů. Je potřeba si uvědomit, že ochrana osobních údajů se týká každého, protože v roli zákazníka jsme dennodenně. Co se ve společnosti a obchodních vztazích rychle mění, je míra automatizace zpracování osobních údajů, a to je důležitý fakt, na který Nařízení GDPR reaguje. Jestliže tedy osoba, která zpracovává osobní údaje, dosud nevěnovala ochraně osobních údajů a rizikům plynoucích pro subjekty údajů (každý, jehož osobní údaje jsou zpracovávány) náležitou pozornost, pak i jeden rok může být krátká doba pro implementaci nových pravidel (3).

Dostatečnou motivací pro přijetí včasných opatření mohou být hrozící sankce za nedodržení požadavků Nařízení GDPR, které jsou mnohem vyšší než doposud. Zatímco podle současného zákona o ochraně osobních údajů lze za nejzávažnější delikty uložit pokutu v maximální výši 10 000 000 Kč, tak podle nového Nařízení GDPR bude možné uložit pokutu až do výše 20 000 000 EUR, nebo pokud se jedná o podnik až do výše 4% celkového ročního obratu celosvětově za předchozí finanční rok (podle toho, která hodnota je vyšší). Takovéto pokuty budou ukládány po celém území EU, tudíž postup dozorových úřadů (v ČR Úřad pro ochranu osobních údajů) bude víceméně jednotný, a to prostřednictvím mechanismu jednotnosti, jehož cílem je přispět k jednotnému uplatňování tohoto Nařízení v celé Unii, kdy dozorové úřady budou spolupracovat mezi sebou navzájem (3).

Požadavky Nařízení GDPR (3) jdou nad rámec současného zákona 101/2000 Sb. o ochraně osobních údajů (12). Jedná se zejména o:

- Rozšíření definice osobních údajů – Nařízení zahrnuje jakákoliv data, která vedou k identifikování osobních údajů jednotlivců, tedy včetně zdravotních údajů, čísel dokladů totožnosti, platební karty, adresy, IP adresy, e-mailové

adresy, lokalizační data, fotografie, také jakékoliv informace o chování zákazníka při nákupech (cookies) a data, ze kterých lze odvodit průběh budoucího jednání konkrétního člověka.

- Zpřísnění pravidel pro získání platného souhlasu pro zpracování osobních údajů – společnost, která shromažďuje osobní údaje, musí prokázat jasný a potvrzující souhlas pro zpracování těchto dat, zejména co se týče přesného a srozumitelného vysvětlení, jaké osobní údaje se sbírají a jak budou dále zprácovány a využity.
- Rozšíření a upřesnění práv subjektů údajů – např. princip minimalizace údajů, který vyžaduje, aby správce osobních údajů nedržel údaje déle, než je nezbytně nutné. Zároveň také nesmí změnit způsob využití dat z účelu, pro který byla data původně shromažďována. Pokud by takovou změnu chtěl udělat, musí si vyžádat nový souhlas od majitele dat. K dalším právům subjektů údajů patří:
    - Právo subjektů údajů na přístup k údajům – správce osobních údajů musí být připraven vyhotovit a předat žadateli kopii veškerých zpracovávaných údajů, a to i v běžně používané elektronické podobě.
    - Právo na námitku proti zpracování – správce musí přestat zpracovávat údaje, pokud neprokáže závažné důvody ke zpracování.
    - Právo na výmaz údajů – správce musí být na žádost připraven vymazat veškeré zpracovávané údaje.
    - Právo na přenositelnost – správce musí být schopen předat zpracovávané údaje ve strukturovaném běžně používaném strojově číselném formátu.
    - Právo na omezení zpracování – správce musí být připraven bez zbytečného odkladu od přijaté žádosti omezit prováděné zpracování, tj. správce smí údaje pouze uchovávat.
- Povinnosti správce osobních údajů – správce má povinnost nepřetržitě monitorovat případné narušení dat a následný únik osobních údajů – pokud se tak stane, je povinen informovat Úřad pro ochranu osobních údajů o úniku nejpozději do 72 hodin od zjištění a rovněž subjekty údajů v případě porušení

zabezpečení osobních údajů, které může mít za následek vysoké riziko pro práva a svobody dotčených osob.

S aktualizovanými pravidly by měly být seznámeny všechny osoby zapojené do zpracování osobních údajů. Shoda s těmito pravidly, s Nařízením a další příslušnou legislativou bude vyžadovat jmenování pověřence pro ochranu osobních údajů (tzv. DPO) podle článku 37-39 Nařízení GDPR (3). Nařízení umožňuje outsourcing role DPO. K jeho základním činnostem bude patřit pravidelné a systematické monitorování souladu s Nařízením, poskytování souvisejícího poradenství a spolupráce s dozorovým úřadem.

Pro zajištění souladu s Nařízením GDPR (3), ale také kvůli značně zvýšeným pokutám, možným žalobám kvůli nárokům poškozených osob a dalším evidentním bezpečnostním rizikům, je nutné provést analýzu rizik a posouzení jejich dopadů na ochranu osobních údajů příslušných subjektů údajů.

3.3.1 Riziko v kontextu GDPR

Nařízení GDPR (3) se zaměřuje na hodnocení rizikovosti zpracování osobních údajů z pohledů subjektů údajů a z pohledu společností. Tato diplomová práce se zabývá hodnocením rizik zpracování osobních údajů z pohledu subjektů údajů. Řízení rizik práv a svobod fyzických osob probíhá pomocí následujících tří procesů:

- stanovení kontextu – s přihlédnutím k povaze, rozsahu, kontextu, účelům zpracování a zdrojům rizik;
- posouzení rizik – zhodnotit konkrétní pravděpodobnost a závažnost rizika;
- ošetření rizik – zamýšlená opatření, mechanismy a záruky pro zmírnění rizika a jeho potenciálního dopadu, zajištění ochrany osobních údajů a prokázání souladu s Nařízením (13).

Nařízení rozpoznává tři druhy rizika pro práva a svobody fyzických osob:

a) Riziko – je obecné měřítko zavádění technických a organizačních opatření pro plnění povinností v Nařízení. Správce provádí posouzení rizika, což je komplexní analýza zaměřená na zjištění možné újmy pro subjekty údajů a pravděpodobnosti, s jakou může újma vzniknout. Na základě analýzy pak správce zavádí taková opatření, aby riziko co nejvíce zmírnil.

b) Vysoké riziko – pokud správce na základě posouzení rizika zjistí, že při zpracování hrozí vysoké riziko, aktivuje se pro něj povinnost provést Posouzení vlivu na ochranu osobních údajů dle čl. 35 Nařízení, dále povinnost předchozí konzultace s dozorovým úřadem dle čl. 36 Nařízení a v případě porušení zabezpečení osobních údajů notifikovat subjekty údajů.
c) Nízké riziko – může aktivovat některé výjimky z povinností dle Nařízení, např. může správce zprostit povinnosti ohlašovat porušení zabezpečení osobních údajů dozorovému úřadu (14).

Dle čl. 32 odst. 2 Nařízení GDPR (3, s. 52) se *„při posuzování vhodné úrovně bezpečnosti zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim“.*

V bodě 75 odůvodnění Nařízení GDPR (3) uvádí, že různě závažná a pravděpodobná rizika pro práva a svobody fyzických osob mohou vyplynout ze zpracování osobních údajů, které by mohlo vést k fyzické, hmotné či nehmotné újmě, a to především v případech:

- kdy by dané zpracování mohlo vést k diskriminaci, krádeži či zneužití identity, finanční ztrátě, poškození pověsti, ztrátě zaměstnání, ztrátě důvěrnosti osobních údajů nebo jakémukoliv významnému hospodářskému či společenskému znevýhodnění;
- kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje.

Správce osobních údajů s přihlédnutím k nákladům na provedení, povaze, rozsahu, kontextu, účelům zpracování i různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, zavádí vhodná technická, organizační a bezpečnostní opatření, aby zajistil vysokou úroveň zabezpečení odpovídající danému riziku a byl schopen doložit a prokázat soulad zpracování osobních údajů s Nařízením, a to zejména příslušnou dokumentací dle čl. 24 odst. 1 Nařízení GDPR (3).

3.4 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů neboli Data Protection Impact Assessment (DPIA) má vazbu na procesy posouzení a hodnocení rizik pro práva a svobody fyzických

osob neboli PIA (Privacy Impact Assessment), viz kapitola 3.5. Mezi pojmy PIA a DPIA je značný rozdíl a je důležité je nezaměňovat. Termín DPIA je explicitně definován v Nařízení GDPR a zahrnuje specifické povinnosti vedení záznamů a povinnosti pro správce osobních údajů. DPIA pomáhá snížit riziko týkající se ochrany osobních údajů a posuzuje dopady konkrétního rizikového zpracování osobních údajů na soukromí a potenciální rizika takového zpracování pro práva a svobody subjektů údajů (15).

Posouzení vlivu na ochranu osobních údajů je definováno ve článku 35 Nařízení GDPR (3). Pokud je pravděpodobné, že plánované zpracování osobních údajů může mít za následek vysoké riziko pro práva a svobody fyzických osob, pak musí správce před samotným zpracováním provést posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů, aby vyhodnotil zejména původ, povahu, zvláštnost, pravděpodobnost a závažnost tohoto rizika a za určitých podmínek si vyžádal předběžnou konzultaci u příslušného dozorového úřadu. Bod 90 odůvodnění Nařízení GDPR (3) uvádí, že takovéto posouzení vlivu by mělo obsahovat zejména zamýšlená opatření, záruky a mechanismy pro snížení rizika, pro zajištění ochrany osobních údajů a prokázání souladu s tímto Nařízením. Podle čl. 35 odst. 1 Nařízení GDPR (3) může pro soubor podobných operací zpracování, které představují podobné riziko, stačit jedno takové posouzení.

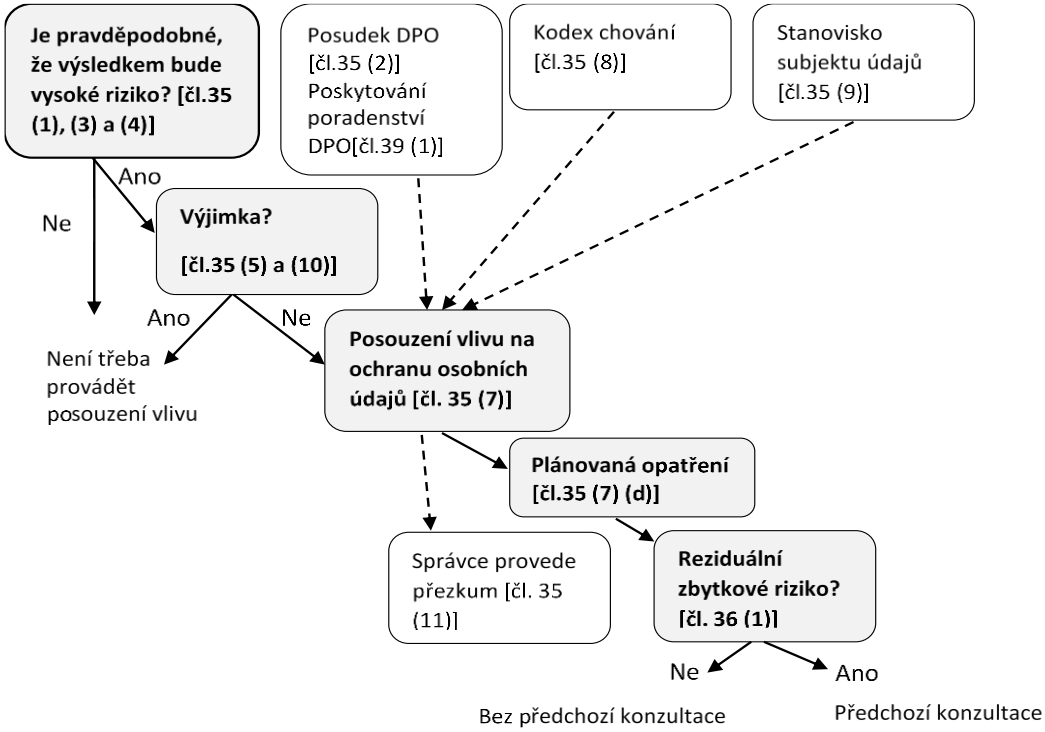
Dle čl. 35 odst. 3 Nařízení GDPR (3) je Posouzení vlivu na ochranu osobních údajů nutné zejména v případech:

- Systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatickém zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky anebo na ně mají podobně závažný dopad.
- Rozsáhlého zpracování zvláštních kategorií údajů (osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání, zpracování genetických údajů, biometrických údajů nebo údajů o zdravotním stavu či sexuální orientace fyzické osoby) nebo osobních údajů, která se týkají rozsudků v trestních věcech a trestných činů.
- Rozsáhlého a systematického monitorování veřejně přístupných prostor.

Dále také v případech:

- zpracování, které označil za rizikové dozorový úřad dle čl. 35 odst. 4 Nařízení, a
- zpracování, u kterého existuje pravděpodobnost, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob (14).

Schéma č. 4 – Proces Posouzení vlivu na ochranu osobních údajů v GDPR



Zdroj: vlastní zpracování, inspirace dle (13)

GDPR nevyžaduje provedení DPIA pro každý proces zpracování osobních údajů, které může vést k ohrožení práv a svobod fyzických osob. Vykonání DPIA je povinné pouze tehdy, pokud je u daného zpracování „*pravděpodobné, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob*“ dle čl. 35 odst. 1 (3, s. 53), který je doložen čl. 35 odst. 3 a 4 Nařízení GDPR (3). Je to zvláště důležité při zavádění nové technologie zpracování dat.

3.4.1 Prvotní posouzení rizikovosti zpracování osobních údajů

Pro každou zamýšlenou operaci zpracování je správce osobních údajů povinen provést prvotní posouzení, zda nespadá do některého z výše uvedených případů dle čl. 35 odst. 3.

Nařízení. Dále také jestli zamýšlená operace zpracování není uvedena na seznamu rizikových operací zpracování vydaném dozorovým úřadem (čl. 35 odst. 4 Nařízení), a případně také provést posouzení, jehož výsledkem bude stanovení, zda u zamýšleného zpracování existuje pravděpodobnost vysokého rizika či nikoliv. Jestliže správce při prvotním posouzení dojde k závěru, že zamýšlená operace zpracování nespadá ani do jedné ze jmenovaných kategorií, pak Posouzení vlivu provádět nemusí (14).

Podle čl. 35 odst. 5 Nařízení GDPR (3) dozorový úřad může ale rovněž sestavit a zveřejnit seznam druhů zpracování, u nichž není Posouzení vlivu na ochranu osobních údajů nutné. Před přijetím seznamů dle odst. 4 a 5 Nařízení GDPR (3) použije dozorový úřad mechanismus jednotnosti, pokud tyto seznamy zahrnují činnosti zpracování související s nabídkou zboží a služeb subjektům údajů, monitorováním jejich chování v několika členských státech nebo mohou zásadně ovlivnit pohyb osobních údajů v rámci Unie. Další výjimkou je dle čl. 35 odst. 10 Nařízení GDPR (3) zpracování, které již má základ v právu Unie nebo členského státu a pokud Posouzení vlivu již bylo provedeno jakožto součást obecného posouzení v souvislosti s přijetím daného právního základu, pak již není třeba provádět Posouzení vlivu na ochranu osobních údajů.

Dle WP29 (13), by měl správce při prvotním posuzování rizika také zohlednit, zda jím zamýšlená operace zpracování neobsahuje určité faktory s vysokým rizikem, zejména:

- Profilování a jiná evaluace či hodnocení (scoring) subjektů údajů.
- Automatizované individuální rozhodování, včetně profilování, které má pro subjekt údajů právní účinky nebo se ho obdobným způsobem významně dotýká.
- Systematické monitorování subjektů údajů.
- Zpracování citlivých údajů – údaje, které svou povahou představují zvýšené riziko pro práva a svobody fyzických osob.
- Zpracování osobních údajů ve velkém rozsahu.
- Kombinování osobních údajů z různých datových sad – může docházet ke zvýšení rizik spojených s výslednými daty.
- Zpracování osobních údajů týkajících se zvlášť zranitelných osob – např. pokud je subjektem údajů dítě nebo osoba se sníženou schopností rozpoznávat důsledky svého jednání.

- Inovativní užití či aplikace technologických nebo organizačních řešení.
- Bránění subjektům údajů v uplatňování svých práv v používání některé služby nebo v uzavření smlouvy – např. pokud bude banka při poskytování úvěru zjišťovat historii platební morálky a na základě špatného výsledku odmítne úvěr přiznat.

WP29 (13) uvádí, že pokud správce osobních údajů vyhodnotí, že jím zamýšlená operace zpracování splňuje alespoň dva z těchto faktorů, měl by provést Posouzení vlivu na ochranu osobních údajů.

Při provádění Posouzení vlivu na ochranu osobních údajů si správce musí vyžádat posudek pověřence pro ochranu osobních údajů (DPO), pokud ho jmenoval (čl. 35 odst. 2 Nařízení). Dále také pověřenec pro ochranu osobních údajů poskytuje informace a poradenství správcům nebo zpracovatelům, kteří dané zpracování provádějí, např. zda vůbec provádět posouzení či jakou metodiku pro provádění posouzení zvolit (čl. 39 odst. 1 Nařízení). Ve vhodných případech správce získá k zamyšlenému zpracování stanovisko od subjektů údajů nebo jejich zástupců dle čl. 35 odst. 9 Nařízení (např. interní a externí studie týkající se účelu zpracování, stanoviska zástupců zaměstnanců nebo odborových svazů). Při posuzování vlivu na ochranu osobních údajů je třeba vzít v úvahu dodržování kodexu chování správcem (čl. 40 Nařízení), v rámci kterého by měly být blíže specifikovány způsoby plnění povinností v určité oblasti a konkretizována rizika a potenciální dopady zpracování v dané oblasti. Na základě dodržování kodexu chování by měl být správce schopen lépe identifikovat potenciální dopady zpracování a také volit adekvátní opatření k jejich zmírnění (14).

Dle čl. 35 odst. 7 Nařízení GDPR (3) Posouzení vlivu na ochranu osobních údajů obsahuje alespoň:

- Systematický popis zamýšlených operací zpracování a účelu zpracování, případně včetně oprávněných zájmů správce.
- Posouzení nezbytnosti a přiměřenosti operací zpracování dle jejich účelu.
- Posouzení rizik pro práva a svobody subjektů údajů.
- Plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů pro zajištění ochrany osobních údajů a k doložení

souladu s tímto nařízením, také s přihlédnutím právům a zájmům subjektů údajů a dalších dotčených osob.

Dle čl. 35 odst. 11 Nařízení GDPR (3) Posouzení vlivu tedy zahrnuje popis, analýzu různých aspektů zamýšleného zpracování, jeho rizik a možných opatření, která je nutné přijmout pro zmírnění těchto rizik. V průběhu životního cyklu zpracování by mělo být Posouzení vlivu pravidelně aktualizováno a doplňováno a správce případně provede přezkum s cílem zjistit, zda je zpracování stále prováděno v souladu s posouzením vlivu na ochranu osobních údajů v případech, kdy dojde ke změně rizika představovaného zpracováním operace.

Výsledkem takového posouzení by měla být dokumentace, která správci umožní přijmout dostatečná opatření ke zmírnění rizika zpracování a prokazování souladu s tímto Nařízením. V případech, kdy správce při posouzení dojde k závěru, že riziko nelze vhodnými opatřeními zmírnit, slouží tato dokumentace dozorovému úřadu k tomu, aby dané zamýšlené zpracování posoudil v rámci předchozí konzultace (14).

3.5 Posouzení dopadů rizik na ochranu osobních údajů

Posouzení dopadů rizik na ochranu soukromí subjektů údajů neboli Privacy Impact Assessment (PIA) podle metodiky *Conducting privacy impact assessments, code of practise* (16) vydané britským dozorovým úřadem ICO identifikuje a pomáhá snížit rizika spojená s ochranou osobních údajů a s jejich zpracováním.

Při posuzování úrovně rizika je nutné přihlédnout k rozsahu, povaze a účelům zpracování a zhodnotit, jestli dané zpracování představuje vysokou pravděpodobnost rizika pro práva a svobody fyzických osob. Takové riziko bude dle bodu 89 odůvodnění Nařízení GDPR (3) vznikat zejména při využití nových technologií, zpracování zcela nového druhu a u nichž správce dosud neprovedl Posouzení vlivu na ochranu osobních údajů a také pokud je s ohledem na operace zpracování pro subjekty údajů obtížnější uplatnit svá práva nebo používat některé služby.

Cílem procesu posouzení rizik je identifikovat rizika týkající se práv a svobod fyzických osob, zjistit možné újmy pro subjekty údajů, včetně závažnosti a pravděpodobnosti, s jakou újma může vzniknout (viz kapitola 3.5.3). Na základě toho musí správce osobních údajů přijímat adekvátní opatření ke zmírnění závažnosti těchto rizik, která nedokáže spočítat, jelikož nemá vstupy od vlastníků údajů (subjektů údajů) - nemá ohodnocení těchto aktiv od

vlastníků údajů. Smyslem je tedy určitým objektivním měřítkem provést ohodnocení osobních údajů. Hodnota osobních údajů je sice subjektivní, přesto lze kvalitativně rizika ohodnotit. Pravděpodobnost a závažnost rizika pro práva a svobody subjektů údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelů zpracování. Riziko by mělo být ohodnoceno na základě objektivního posouzení, které následně stanoví, zda operace zpracování představují riziko či vysoké riziko (3).

Pro posuzování rizik v oblasti ochrany osobních údajů existuje více doporučovaných metodik (např. metodiky vydané francouzským dozorovým úřadem CNIL), nicméně základní principy pro určení rizik zpracování jsou následující:

a) identifikace hrozeb spojených se zpracováním,
b) identifikace potenciální újmy dotčených osob spojené se zpracováním jejich osobních údajů,
c) zhodnocení pravděpodobnosti, že újma vznikne a posouzení slabých míst systémů a procesů,
d) zhodnocení závažnosti potenciální újmy, pokud by vznikla (14).

S procesem posouzení rizik se úzce pojí princip odpovědnosti, kvůli kterému musí být správce schopen doložit soulad s Nařízením. Správce by tedy měl všechna provedená posouzení rizik a následné zvolení vhodných opatření k jejich zmírnění pečlivě odůvodnit a zdokumentovat pro potřeby prokázání souladu (14).

3.5.1 Identifikace rizik v kontextu GDPR

Hlavním cílem identifikace rizik je poskytnout vyčerpávající soubor rizikových faktorů, které by mohly mít vliv na práva a svobody fyzických osob, zejména práva na ochranu osobních údajů a jejich hodnotu. Článek 35 Nařízení GDPR (3) ukládá správci, aby identifikoval a posoudil rizika pro práva a svobody fyzických osob, která jsou se zpracováním osobních údajů spojena, a podle významu těchto rizik uplatnil adekvátní opatření k zajištění souladu s tímto Nařízením.

Následující kapitoly diplomové práce se zabývají identifikací a rozlišením aktiv a vlastníků z pohledu Nařízení GDPR (3), identifikací hrozeb a potenciální újmy, kterou může představovat dané zpracování osobních údajů fyzickým osobám, včetně následného hodnocení a zvládání rizik.

3.5.2 Identifikace aktiv a vlastníků v kontextu GDPR

Aktivum představuje určité hodnoty, které jsou pro subjekt udajů důležité a je tedy nutno je chránit. Aktivem je osobní údaj, který je již z podstaty věci klíčovým pojmem, neboť Nařízení se vztahuje pouze na zpracování informací, které lze označit za osobní údaje. Vlastníkem aktiv neboli osobních údajů jsou dotyčné subjekty údajů. Osobním údajem se rozumí jakákoliv informace, která se týká přímo či nepřímo určitelné fyzické osoby. Nejedná se pouze i identifikační údaje, které umožňují konkrétní osobu jednoznačně určit, ale o veškeré informace, jež se určitelného člověka týkají, i přestože jej jednoznačně neidentifikují (např. počet dětí, zůstatek na bankovním účtu aj.). Není rozhodující, zda je údaj zcela pravdivý nebo zda se jedná o pouhý odhad charakteristiky člověka (např. ze spotřebitelského profilu odvozený předpoklad budoucích nákupních preferencí). Stejně tak není rozhodující formát zachycené informace, tzn., jestli je v písemné podobě, nebo ve formě audio či videozáznamu (14). Dále je důležité podotknout, že dle bodu 27 odůvodnění Nařízení GDPR (3) je možno označit informaci za osobní údaj pouze, pokud se týká žijící osoby.

Nařízení GDPR (3) nově uvádí dva příklady druhů informací, jež lze považovat za identifikátory fyzické osoby, a to lokační údaje a síťové identifikátory. Lokačním údajem je informace týkající se místa pobytu či pohybu dané osoby. Síťové identifikátory jsou dle bodu 30 odůvodnění Nařízení GDPR (3) využívány při komunikaci koncových zařízení uživatelů prostřednictvím komunikačních sítí, např. IP adresa, cookies. Takto mohou být zanechány stopy, které v kombinaci s dalšími informacemi, které servery získávají, mohou být použity k profilování a identifikaci fyzických osob.

Definice osobního údaje v Nařízení GDPR (3) stejně jako definice ve směrnici 95/46/ES (17) dále obsahuje prvky lidské identity, kterých se může osobní údaj dotýkat. Jedná se o různé sféry lidské osobnosti, které mohou obsahovat popisný prvek konkrétního člověka, např. údaje o fyziologii daného člověka, společenském zařazení, informace o majetku, zdravotním stavu. Nařízení GDPR (3) nově přidává i genetickou identitu člověka (dle bodu 34 odůvodnění Nařízení se jedná o informace týkající se zděděných nebo získaných genetických znaků určité fyzické osoby – DNA, RNA aj.).

Kromě běžných typů osobních údajů je třeba rozlišit zpracování zvláštních kategorií osobních údajů. Dle článku 9 Nařízení GDPR (3) se zakazuje zpracování osobních údajů,

jež vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání, filosofickém přesvědčení, členství v odborech, dále zpracování genetických a biometrických údajů, údajů o zdravotním stavu či sexuální orientaci fyzické osoby. Výjimku tvoří zpracování těchto zvláštních osobních údajů na základě titulu plnění právní povinnosti nebo po získání explicitního souhlasu dotčeného subjektu údajů. Přítomnost těchto osobních údajů signalizuje vysoké riziko pro práva a svobody fyzických osob a vzniká tak nutnost vedení záznamů o jejich zpracování.

Nařízení GDPR (3) se netýká zpracování anonymních informací (informace, které se netýkají identifikovatelné fyzické osoby) a zpracování pro statistické a výzkumné účely. Správce se může rozhodnout určitou sadu osobních údajů anonymizovat a to tak, aby ani on, ani žádný jiný existující subjekt nemohl, ani v kombinaci s dalšími údaji, anonymizované údaje spojit s konkrétními osobami. Jestliže tedy subjekt údajů není nebo přestal být identifikovatelným, pak anonymizované osobní údaje nejsou předmětem působnosti tohoto Nařízení. Naproti tomu pseudonymní údaje, které není možné přiřadit ke konkrétním osobám bez použití dodatečných informací, uložených zvlášť a zabezpečených pomocí technických opatření, je nutno dále považovat za údaje osobní. Použití pseudonymizace osobních údajů může podle bodu 26 a 28 odůvodnění Nařízení GDPR (3) omezit rizika pro dotčené subjekty údajů a pomoct tak správcům splnit povinnosti týkající se jejich ochrany.

3.5.3 Identifikace hrozeb a potenciální újmy

V průběhu celého životního cyklu osobních údajů od jejich shromáždění až po jejich likvidaci mohou dle Nulíčka a kol. (14) vznikat různé hrozby pro práva a svobody fyzických osob viz Katalog hrozeb v Příloze č. 4. Tyto hrozby je nutné při každém zpracování osobních údajů identifikovat. Mezi takové hrozby patří zejména:

- zpracování osobních údajů v rozporu se zásadou zákonnosti;
- nevhodné zpracování osobních údajů, které překračuje očekávání subjektu údajů, dobu uchování nebo které jde nad rámec očekávání společnosti;
- nezákonné překročení stanoveného účelu zpracování;
- nadměrné shromažďování či zpracování osobních údajů – rozpor se zásadou minimalizace údajů;
- zpracování či uchování nepřesných či neaktuálních osobních údajů;

- narušení důvěrnosti či integrity osobních údajů;
- ztížení či znemožnění možnosti uplatnit práva subjektů údajů.

Poté co jsou identifikovány hrozby, které jsou s daným zpracováním osobních údajů spojeny, je potřeba identifikovat i potenciální újmu, která může nastat fyzickým osobám v důsledku vzniku hrozby. Správce by ale neměl posuzovat pouze újmu, kterou může daným zpracováním způsobit on sám, ale také újmu, která může vzniknout následným jednáním třetí strany, např. po předání nebo zveřejnění osobních údajů. Poté co je možná újma pro práva a svobody fyzických osob identifikována, je třeba posoudit její závažnost a míru pravděpodobnosti posouzením možnosti, že se zrealizuje hrozba a v jejím důsledku vznikne předvídaná újma. Také je důležité posoudit možné benefity, které dané zpracování může pro subjekt údajů znamenat – v některých případech může velká výhoda i ospravedlnit zbytkové riziko, které není možné dále zmírnit (14).

Míra pravděpodobnosti vzniku újmy bude záviset na faktorech:

- počet osob zapojených do zpracování;
- zapojení třetích stran do zpracování;
- rozdílné právní požadavky – např. při předání osobních údajů do zahraničí;
- slabá místa v procesech a systémech zpracování;
- historie předchozích incidentů, u nichž došlo ke vzniku újmy.

Mezi faktory určující závažnost potenciální újmy patří:

- citlivost a objem zpracovávaných osobních údajů;
- zranitelnost dotčených fyzických osob;
- možný dopad zpracování na významné události v životě fyzických osob;
- možný dopad zpracování na finanční a ekonomickou situaci fyzických osob (14).

3.5.4 Hodnocení a zvládání rizik

Po identifikaci potenciální újmy, posouzení pravděpodobnosti vzniku újmy a její možné závažnosti, získá správce přehled o riziku, jež dané zpracování osobních údajů představuje. Na základě zjištěného rizika pak musí s ohledem na jednotlivé hrozby volit vhodná opatření, aby riziko zmírnil. Posouzení rizika a následná implementace opatření nejsou dle čl. 24 odst. 1 Nařízení GDPR (3) jednorázovým krokem, jedná se o kontinuální proces. V případě, kdy

se okolnosti zpracování včetně možných hrozeb změní, musí správce revidovat přijatá opatření a pokud tato opatření již nepostačují, musí přijmout opatření nová, lépe odpovídající změněným hrozbám.

Dle čl. 25 odst. 1 Nařízení GDPR (3) správce, s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, které s sebou zpracování nese, provádí záměrnou ochranu osobních údajů, jež spočívá v zavedení vhodných technických a organizačních opatření, např. pseudonymizace, minimalizace údajů, omezení přístupu nebo fyzické a síťové zabezpečení údajů, a začlení do zpracování nezbytné záruky, aby splnil požadavky tohoto Nařízení a ochránil práva subjektů údajů.

Tato opatření budou dle odst. 2 tohoto článku Nařízení GDPR (3) zavedena k zajištění toho, aby se standardně zpracovávaly jen osobní údaje, jež jsou pro daný účel zpracování nezbytné. Toto se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a dostupnosti. Opatření mají zejména zajistit, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob. Je důležité si uvědomit, že cílem hodnocení rizik není zcela vyloučit dopad zpracování na soukromí subjektů údajů. Účelem je snížit tento dopad na přijatelnou úroveň a současně umožnit realizaci užitečného projektu.

Kromě těchto opatření je správce povinen přijmout rovněž opatření k zajištění schopnosti soulad s Nařízením prokázat. Tímto je možné v praxi považovat přiměřenou dokumentaci plnění jednotlivých povinností dle Nařízení, přičemž komplexnost dokumentace bude záviset na okolnostech konkrétního zpracování (14).

Dle přílohy F ČSN ISO/IEC 27005 (1) musí být při návrhu opatření pro ošetření rizik formou jejich modifikace brána v úvahu i následující omezení:

- časová omezení,
- omezení finančními prostředky,
- technická a technologická omezení,
- provozní omezení,
- kulturní omezení,
- etnická omezení,

- ekologická omezení,
- právní omezení,
- snadnost použití,
- personální omezení,
- omezení při integraci nových a existujících opatření.

3.6 Náležitosti Posouzení vlivu na ochranu osobních údajů

Pro naplnění základních požadavků stanovených v Nařízení GDPR (3) mohou být použity různé metodiky. Aby bylo správcům osobních údajů umožněno být v souladu s Nařízením, byla stanovena společná kritéria výkladového pokynu WP29 (13). Kritéria vyjasňují základní požadavky Nařízení, ale zároveň poskytují dostatečný prostor pro různé formy provádění. Tato kritéria mohou být použita k prokázání, že je konkrétní metodika dostatečně komplexní a splňuje standardy požadované Nařízením. Kompletní kritéria pro celý proces Posouzení vlivu na ochranu osobních údajů se nachází v Příloze č. 2 této práce.

Jedná se o kompletní souhrn kritérií, na základě kterých bude v praktické části diplomové práce vytvořena metodika hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů se zaměřením na hodnocení rizik pro práva a svobody subjektů údajů.

4 Výsledky práce

4.1 Charakteristika společnosti

Společnost Taylor McCoy, s.r.o. vznikla v roce 2013 jako nástupce sdružení spolupracujících podnikatelských subjektů zaměřených na oblast bezpečnosti informací.

Na základě osobních rozhovorů s odpovědnými pracovníky (viz Příloha č. 1) byly zjištěny následující informace o činnostech a poskytovaných službách, organizační struktuře a dokumentační základně společnosti. Podnikatelské aktivity společnosti jsou orientovány na poskytování vysoce specializovaných poradenských služeb, odborného know-how v oblastech informační bezpečnosti a outsourcing rolí pro systémy řízení bezpečnosti informací a systémy řízení kontinuity podnikání. Nicméně v současné době se společnost zaměřuje především na poskytování služeb v oblasti GDPR a dosažení souladu s požadavky v rámci tohoto Nařízení. Mezi významné klienty patří společnosti v segmentech bankovnictví a finančnictví, silové resorty státní správy, státní podniky, telekomunikační společnosti, farmaceutické společnosti a formou subkontraktů i přední poradenské společnosti a ICT integrátoři.

Specialisté a konzultanti společnosti poskytují služby v následujících oblastech:

- analýza rizik souvisejících s provozem nebo změnou IT prostředí včetně doporučení, jak snížit rizikové faktory,
- vytvoření bezpečnostní politiky a procedury,
- provedení hodnocení a návrh bezpečnostní architektury,
- příprava a posouzení havarijních plánů, nastavení postupů zvládání mimořádných událostí, včetně plánováním kontinuity provozu,
- příprava na získání certifikátů ISO 27000, ISO 20000,
- provedení auditů
    - systému řízení bezpečnosti dle ISO/IEC 27001,
    - systému řízení IT služeb / ITIL dle ISO/IEC 20000-1,
    - systému řízení kvality dle ISO 9001.
- dosažení souladu s požadavky standardů a norem:
    - ISO 27001, ISO 20000,

- PCI DSS,
- Zákona o kybernetické bezpečnosti č. 181/2014 Sb.,
- GDPR.

Organizační struktura společnosti je rozdělena do dvou hlavních linií. První linii tvoří divize Obchodu a vztahu s veřejností. Druhou linii představuje divize Realizace. Divize Realizace kromě samotné realizace klientských projektů zastřešuje řízení lidských zdrojů, řízení subkontraktorů, řízení neobchodních rizik a správu interně implementovaných systémů ISO. Mezi klíčové interně implementované systémy patří vzhledem k charakteru činností společnosti systém řízení bezpečnosti informací postavený na rodině norem ISO řady 27000, především ISO 27001.

Společnost nemá kmenové zaměstnance, ale pro výkon firemních procesů zaměstnává externí kontraktory. Všichni externí kontraktoři projdou po uzavření smlouvy sadou vstupních školení, která jsou prováděna odpovědným vedoucím oddělení. Vstupní školení se týkají seznámení kontraktorů s metodikami využívaných ve společnosti a interními předpisy pro ochranu informací. Dále mohou být kontraktoři školeni v rámci mimořádných školení, která nastanou v případě změn nebo v případě reakcí na mimořádnou událost, jako je například bezpečnostní incident.

Řízení bezpečnosti informací na výkonné úrovni je zajišťováno prostřednictvím bezpečnostního manažera, který koordinuje činnosti související s bezpečností informací a rozhoduje o všech běžných záležitostech bezpečnosti informací. Zároveň také v měsíci lednu pravidelně předkládá Zprávu o stavu bezpečnosti informací za uplynulý rok poradě vedení. Zajišťování bezpečnosti informací na úrovni provozu informačního systému společnosti má na starost bezpečnostní správce. Mezi jeho hlavní odpovědnosti a pravomoci patří pravidelné informování bezpečnostního manažera o stavu bezpečnosti prostřednictvím měsíčních zpráv a průběžně v případě bezpečnostních incidentů. Další důležitou rolí v této společnosti je garant aktiva, který je odpovědný za informace spojené s aktivem. Garant aktiva má metodickou a provozní znalost daného aktiva a zodpovídá za stanovení bezpečnostních požadavků na ochranu jemu svěřených aktiv. Garant aktiva je zároveň vlastníkem rizik daného aktiva.

Dokumentační základna interních předpisů společnosti je dělena do tří úrovní. První úroveň představují strategické dokumenty vydávané vedením společnosti s rozsahem platnosti pro

celou společnost. První úroveň dokumentace obsahuje deklarace a závazky společnosti a přístup k ní není omezován.

Druhou úroveň dokumentace tvoří interní směrnice vydávané bezpečnostním manažerem, stanovující odpovědnosti rolí, procesy a opatření. Přístup k této dokumentaci je omezen na role a subjekty s uzavřeným závazkem mlčenlivosti.

Třetí úroveň dokumentace tvoří metodické pokyny, technické postupy a další dokumenty s vysokou mírou podrobností vydávané bezpečnostním manažerem. Přístup k této dokumentaci je striktně řízen a omezen na role a subjekty, kterých se dokumentace přímo dotýká a potřebují ji k výkonu svých činností.

Základním dokumentem pro řízení rizik informací zařazeným do první úrovně dokumentace je **Politika a rozsah systému řízení bezpečnosti informací**, který definuje základní cíle v bezpečnosti informací včetně cílů řízení rizik, stanovení odpovědností, rozsahu systému řízení bezpečnosti informací a jeho struktury. Dokument obsahuje závazek vedení k dosažení uvedených cílů včetně alokace potřebných zdrojů. Rozsah systému řízení bezpečnosti informací je dokumentem stanoven tak, aby pokrýval všechna informační, fyzická i další aktiva společnosti.

Druhá úroveň dokumentace je tvořena **Směrnicí bezpečnosti informací**, která obsahuje bezpečnostní cíle společnosti, bezpečnost lidských zdrojů, řízení aktiv a klasifikace informací, bezpečnost komunikací a fyzickou bezpečnost a bezpečnost prostředí.

V návaznosti na Směrnici bezpečnosti informací jsou vydány dokumenty třetí úrovně, které sestávají z metodik a postupů. Mezi ně patří **Metodika analýzy rizik, Metodika testování bezpečnosti informací, Metodická příručka bezpečnostního manažera** a další dokumenty provozního charakteru. Do této úrovně jsou zařazeny i všechny vzory a záznamy nezbytné pro fungování systému řízení bezpečnosti informací, včetně **Registru rizik, Evidence aktiv**, zpráv z přezkoumání systému řízení bezpečnosti informací, zpráv z bezpečnostních testů a dalších.

4.2 Proces řízení rizik ve společnosti

Proces řízení rizik společnosti Taylor McCoy, s.r.o. byl podrobněji analyzován v bakalářské práci „Proces řízení rizik“ (18). Ve společnosti je s ohledem na charakter podnikatelské

činnosti a způsob práce proces řízení rizik zaměřen především na řízení rizik v oblasti bezpečnosti informací. V současné době řízení rizik nepokrývá finanční, obchodní, ani jiná rizika, která jsou řízena intuitivně mimo formalizovaný proces spravovaný divizí Realizace a jsou plně v kompetenci divize Obchodu. Proces řízení rizik ve společnosti představuje kontinuální proces, ve kterém hodnocení rizik bezpečnosti informací probíhá v rozsahu pokrývajícím celý informační systém, a to pravidelně 1x za 3 roky nebo neprodleně v případě změn informačního systému, pokud to tyto změny vyžadují. Způsob a průběh hodnocení rizik je podrobněji rozpracován v Metodice analýzy rizik informací. Ve společnosti odpovídá za provedení hodnocení rizik bezpečnostní manažer. Zjištěná rizika jsou dále evidována v Registru rizik a jsou pravidelně přezkoumávána v rámci pravidelného hodnocení rizik společnosti.

Po hodnocení rizik následuje proces ošetření zjištěných rizik bezpečnosti informací, který probíhá podle Plánu ošetření rizik informací. Rizika přesahující akceptovatelnou úroveň jsou určena k redukci pomocí přijatých opatření nebo jsou přenesena na jiný subjekt. Akceptovatelná míra rizika je stanovena bezpečnostním manažerem na základě doporučení porady vedení (17).

4.2.1 Pravidla ochrany osobních údajů ve společnosti

Stav ochrany osobních údajů je ve společnosti řízen Směrnicí pro nakládání s osobními údaji (19), která obsahuje základní principy a požadavky týkající se nakládání s těmito údaji. Slouží k popsání základních pravidel pro práci s osobními údaji (klientů, zaměstnanců,..) a k ochraně společnosti a jejich klientů. Společnost zpracovává klientské, zaměstnanecké a další osobní údaje týkající se jiných subjektů údajů, za které je zodpovědná. Musí tedy stanovit a respektovat pravidla a podmínky pro zpracování osobních údajů zejména v návaznosti na právní povinnosti. Ke klíčovým principům společnosti reprezentujícím základní hodnoty ochrany osobních údajů a soukromí subjektů údajů patří:

- **Účelové omezení** - Osobní údaje jsou shromažďovány pro určité, výslovně vyjádřené a legitimní účely (důvody) a nesmějí být dále zpracovávány způsobem, který je s těmito účely (důvody) neslučitelný.
- **Zákonné zpracování - Osobní údaje** - Každé zpracování osobních údajů musí být založeno na právním titulu stanoveným zákonem.

- **Zákonné zpracování - Zvláštní kategorie osobních údajů** - Každé zpracování zvláštní kategorie osobních údajů musí být založeno na právním titulu stanoveným zákonem, přičemž nejčastějším právním titulem pro takové zpracování je výslovný souhlas.
- **Kvalita a přesnost dat** – Zpracovávané osobní údaje musí být přesné a aktuální (např. nesmí být zpracovány osobní údaje nad rámec potřebný k naplnění účelu zpracování).
- **Transparentnost** – Subjekt údajů musí být informován srozumitelným jazykem o všech účelech zpracování a musí tuto informaci obdržet ještě před začátkem zpracování jeho osobních údajů.
- **Práva subjektu údajů** - Každý subjekt údajů má zvláštní práva při zpracování jeho osobních údajů.
- **Technická a organizační opatření** – Musí být zavedena odpovídající technická a organizační opatření k ochraně osobních údajů, aby se zabránilo jakékoliv formě nezákonného zpracování.
- **Předávání osobních údajů** (v rámci i mimo skupiny) - Osobní údaje mohou být sdíleny s třetími stranami pouze tehdy, jestliže jsou splněné stanovené požadavky či právními předpisy.
- **Datová governance** (správa dat) – Je třeba definovat zodpovědné osoby i procesy, aby data a nakládání s nimi bylo řádně spravováno.
- **Monitoring a kontrolní činnost** – Kontrolní prostředí musí být řádně nastaveno.

Tyto informace ohledně pravidel ochrany osobních údajů byly získány díky možnosti nahlédnutí do Směrnice pro nakládání s osobními údaji (19) a rovněž na základě osobních rozhovorů s bezpečnostním manažerem společnosti (viz Příloha 1).

4.3 Metodika hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů

V následujících kapitolách diplomové práce je vytvořena metodika hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů, která vychází z principů uvedených v ČSN ISO/IEC 27005 (1) a ČSN ISO/IEC 29134 (20), osobních rozhovorů s odpovědnými pracovníky společnosti (viz Příloha č. 1), výkladových pokynů pracovní skupiny WP29 (13)

a s přihlédnutím k náležitostem Posouzení vlivu na ochranu osobních údajů (Příloha č. 2), jež mohou být použita k prokázání, že konkrétní metodika je dostatečně komplexní a splňuje standardy požadované Nařízením GDPR (3). Tato metodika je vytvořena ve spolupráci se společností Taylor McCoy pro jejich interní potřebu a zákaznické projekty. Dále je v kapitole 4.3.6 zpracován návrh postupu výběru opatření k řešení těchto rizik, včetně opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto Nařízením GDPR (3).

4.3.1 Harmonogram postupu vypracování metodiky

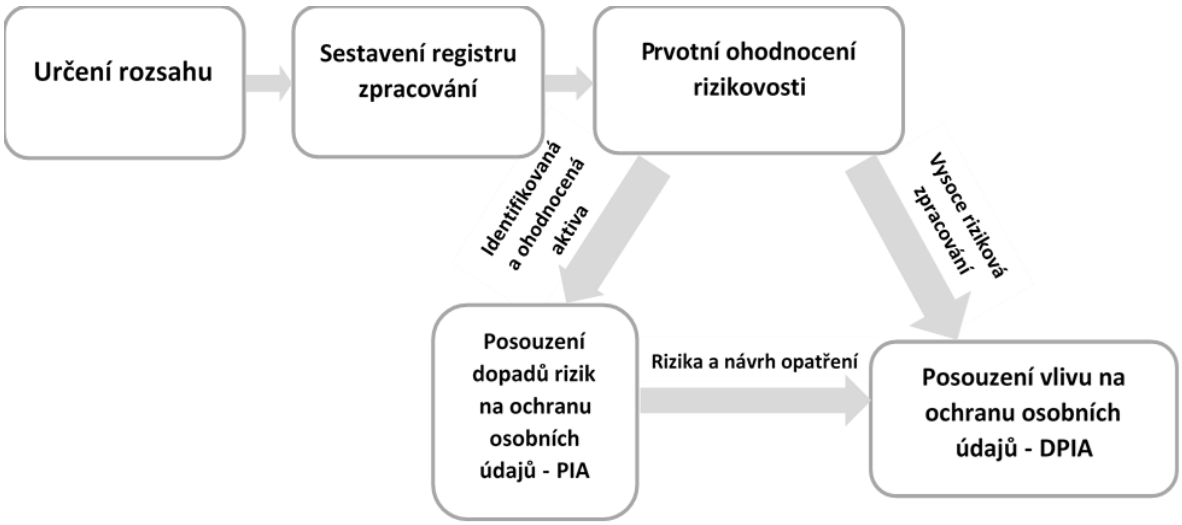
V rámci vytvoření metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů bylo třeba provést několik dílčích kroků, které jsou zobrazeny ve Schématu č. 5 a podrobněji popsány v následujícím harmonogramu postupu:

1) stanovení rozsahu GDPR pro společnost – na základě rozhovoru s bezpečnostním manažerem byly identifikovány jednotlivé oblasti (organizační části společnosti), ve kterých dochází ke zpracování osobních údajů, např. HR, účetnictví apod.
2) sestavení registru zpracování – formou rozhovorů s jednotlivými odpovědnými zaměstnanci z těch částí společnosti, které byly identifikovány v rámci předchozího kroku – určení rozsahu. Registr zpracování poskytne komplexní přehled o každém jednotlivém zpracování osobních údajů z hlediska popisu jednotlivých náležitostí DPIA, jako je popis účelu zpracování, doby uchování osobních údajů apod. (viz kapitola 4.3.3.1 a Příloha č. 5).
3) vytvoření postupu pro zjištění kritičnosti jednotlivých zpracování osobních údajů - dle kritérií WP29 (13) pro hodnocení jednotlivých zpracování osobních údajů bylo provedeno prvotní posouzení rizikovosti, jehož cílem bylo zjistit vysoce riziková zpracování, pro něž je nutné provést DPIA. Zpracování, jež nejsou zjištěna jako vysoce riziková, jsou řešena pouze v rámci PIA (viz kapitola 4.3.4).
4) vytvoření metodiky posouzení dopadů rizik pro ochranu osobních údajů (PIA) - vedle předcházejících kroků a nezávisle na nich se pro každé zpracování provede PIA, na základě kterého je určena povaha rizika, v jakých oblastech může riziko nastat a je určena jeho výše (viz kapitola 4.3.5).
5) projednání zjištěných rizik – s bezpečnostním managementem společnosti a s garanty jednotlivých zpracování proběhlo projednání zjištěných rizik, včetně

potvrzení doporučené míry akceptovatelného rizika. Dále byly projednány varianty ošetření zjištěných rizik (redukce pomocí opatření, přenesení rizika a vyhnutí se riziku).

6) návrh opatření k řešení rizik – pro pokrytí rizik, u kterých bylo společností odsouhlaseno ošetření pomocí opatření, byla navržena opatření (viz. 4.3.6)
7) projednání doporučených opatření s garanty zpracování a bezpečnostním managementem – opatření navržená v předchozím kroku byla projednána s odpovědnými zaměstnanci společnosti a odsouhlasena k realizaci.

Schéma č. 5 – Dílčí kroky metodiky Posouzení vlivu na ochranu osobních údajů



Zdroj: vlastní zpracování

Jednotlivé dílčí kroky metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů jsou popsány v následujících kapitolách.

4.3.2 Dopad požadavků DPIA na metodiku hodnocení rizik

V Příloze č. 3 je v tabulce zpracován dopad požadavků Posouzení vlivu na ochranu osobních údajů – DPIA na navrhovanou metodiku hodnocení rizik. Jestliže jednotlivé atributy požadavků DPIA ovlivňují výši rizik, pak je v tabulce uveden odkaz na kapitolu vytvořené metodiky, ve které jsou tyto atributy zohledněny a zaznamenány. Atributy požadavků jež neovlivňují výši rizik, nejsou relevantní pro zpracování této metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů a tato diplomová práce se jimi nezabývá.

4.3.3 Registr zpracování

Registr zpracování byl sestaven pro 15 typů zpracování osobních údajů. Jedná se o přehled všech zpracování, které společnost Taylor McCoy provádí. Nejprve byl stanoven rozsah, v němž bylo vymezeno 5 oblastí, ve kterých dochází ke zpracování zmíněných osobních údajů. Jedná se o oblast HR, Integrovaného systému řízení, BOZP, účetnictví a nákup. Vyplněný Registr zpracování je v Příloze č. 5. Vypracovaný Registr zpracování bude společnosti sloužit pro průběžné vedení evidence a řízení oblasti ochrany osobních údajů.

4.3.3.1 Sestavení registru zpracování

Na základě rozhovorů s odpovědnými pracovníky společnosti a studia interních dokumentů byly navrženy následující parametry pro evidenci jednotlivých zpracování, aby bylo možné identifikovat rizikovost konkrétních zpracování a posléze určit ta, která podléhají Posouzení vlivu na ochranu osobních údajů.

Účelem zpracování se rozumí důvod, pro který jsou osobní údaje zpracovávány. Osobní údaje je možno zpracovávat pouze pro vymezený účel. Obecně je účel zpracování nutno posoudit pro každé zpracování, přičemž způsob popisu účelu zpracování je zásadním určovatelem toho, jak může správce s osobními údaji nakládat.

Příklad vyplnění: „evidence uchazečů o zaměstnání“

Doplňující informace:

- zpracování může být prováděno pouze k předem stanovenému účelu;
- účel musí být:
    - určitý – aby z něj bylo jasné, jaká zpracování budou/nebudou na jeho základě probíhat (ne vágně: marketingové účely, ale spíše: zasílání nabídek nových produktů a služeb stávajícím zákazníkům),
    - výslovně vyjádřený,
    - legitimní (tedy v souladu s právním řádem);
- účely nelze kumulovat (zpracovávají se odděleně)
    - např. plnění smlouvy a současně zasílání nabídek,

    - každému účelu odpovídá jeden řádek tabulky (každý účel by měl být dostatečně konkretizován, aby nebyl identický s účelem uvedeným v jiném řádku tabulky);
- osobní údaje je možno zpracovávat pouze pro vymezený účel
    - pokud účel odpadne, zkoumá se existence jiného účelu,
    - pokud neexistuje, nutno zpracování ukončit.

Mohou být uchovávány ty samé osobní údaje, ale účel zpracování je často odlišný.

a) Vztah ke zpracování

Vztah ke zpracování je identifikací role, ve které se společnost Taylor McCoy nachází. V případě, že společnost stanovuje účel, rozsah a prostředky zpracování, je považována za „správce“. Pokud provádí zpracování dle pokynů jiného subjektu, který stanovuje dříve uvedené, pak je společnost „zpracovatelem“. Pokud účel zpracování určuje společnost i externí subjekt společně, pak se jedná o „společné správce“.

Příklad vyplnění: „správce“

Doplňující informace:

Společnost v roli správce stanovuje účel a rozsah daného zpracování osobních údajů a bude v rámci konkrétní činnosti v roli zpracovatele pouze pokud zpracovává osobní údaje pro jiného správce a na základě jeho pokynu (např. při udělování dotace požaduje třetí strana po společnosti různé údaje včetně osobních a společnost je musí shromáždit a poskytnout třetí straně, tj. zpracovat).

b) Využití externího zpracovatele pro zpracování

Tato položka určuje, jestli je zpracování prováděno s pomocí externího zpracovatele. Hodnota “ano” bude např. v případě, kdy správce osobních údajů zadá jejich zpracování externí společnosti nebo jiné fyzické osobě – podnikateli.

Příklad vyplnění: „ano“

Typem využití externího zpracovatele pro zpracování může být zpracování osobních údajů pro výpočet mezd, které je prováděno externí účetní firmou, jež jsou tyto údaje předávány.

c) Garant účelu zpracování

Garantem účelu je osoba (zaměstnanec), která je schopna určit význam zpracování osobních údajů a nese za toto zpracování odpovědnost v rámci společnosti. Většinou se jedná o vedoucí zaměstnance organizačních útvarů, případně jiné pověřené zaměstnance s odbornou znalostí daného zpracování.

Příklad vyplnění: „vedoucí ICT“

d) Právní základ zpracování

Právním základem zpracování se rozumí zákonný důvod pro provádění zpracování za uvedeným účelem. Existence právního základu je nutnou podmínkou zákonného zpracování osobních údajů.

Příklad vyplnění: „plnění právní povinnosti“

Právní základ může mít tyto varianty, které jsou podrobněji popsány níže:

- Souhlas subjektu údajů – právní jednání, jímž subjekt údajů vyjadřuje svolení k tomu, aby správce zpracovával jeho osobní údaje. Z Nařízení vyplývá požadavek, aby souhlas byl jako projev vůle zcela jednoznačný, svobodný, srozumitelný a jasný.
- Uzavření či plnění smlouvy – pokud správce zpracovává osobní údaje na základě titulu plnění smlouvy (např. poskytnutí služby), je správce oprávněn za tímto účelem osobní údaje zpracovávat a nemusí získávat další právní titul, např. souhlas. Správce může například zákonně zpracovávat jméno a adresu svého zákazníka, který si u něj objednal zboží, za účelem zaslání tohoto zboží na jeho adresu. Tento účel ale nemůže svévolně překročit a údaje podat např. třetí straně.
- Plnění právní povinnosti – pokud nějaký právní předpis (např. Zákon o účetnictví, Zákoník práce) členského státu EU po správci explicitně požaduje, aby osobní údaje zpracovával, pak správce bude moci osobní údaje zpracovávat bez souhlasu.
- Oprávněný zájem – pokud je nějaký zájem správce možné považovat za oprávněný a za účelem jeho dosažení je nezbytné osobní údaje zpracovávat, může tak učinit. Osobní údaje však zpracovávat nemůže, pokud nad oprávněným zájmem převáží zájmy nebo základní práva a svobody

subjektů údajů, jejichž osobní údaje jsou zpracovávány. Za oprávněný zájem bývá označován např. výkon svobody projevu a práva na informace, vymáhání právních nároků, ochrana před zneužitím služeb, fyzická, IT a síťová bezpečnost, vědecký výzkum apod.

- Ochrana životně důležitých zájmů subjektu údajů nebo jiné osoby – pokud je zpracování osobních údajů nutné za účelem předejití vzniku újmy na životě subjektu údajů nebo jiné osoby. Například v případech, kdy je nutné zpracovávat osobní údaje oběti nehody, která nedokáže dát souhlas.
- Plnění úkolu veřejného zájmu nebo při výkonu veřejné moci – pokud je zpracování relevantních osobních údajů nutné při plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci.

e) Kategorie subjektů osobních údajů

Kategorie subjektů osobních údajů tvoří okruh subjektů, ke kterým se osobní údaje zpracovávané za daným účelem vztahují.

Příklad vyplnění: „uchazeč o zaměstnání“

Typ subjektů údajů je role, jakou tento subjekt má ve vztahu k dané společnosti, například:

- uchazeči o zaměstnání,
- zaměstnanci,
- studenti,
- návštěvníci,
- klienti,
- rodinní příslušníci zaměstnanců aj.

f) Kategorie osobních údajů

Osobními údaji jsou veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat.

Příklad vyplnění: „číslo bankovního účtu“

Je možno uvést následující varianty osobních údajů:

- identifikační a adresní (jméno, příjmení, rodné číslo, email,..),

- identifikační IT (login, UID, přístupová oprávnění,..),
- zdravotní údaje (nemoci, duševní choroby, rekonvalescence),
- vzdělávání (diplomy, vysvědčení, osvědčení),
- biometrie (otisk prstu),
- finanční podrobnosti (cena, číslo účtu),
- popisné (rozsah, podoba a případné další členění popisných osobních údajů závisí na konkrétním účelu příslušného zpracování).

g) Zvláštní kategorie osobních údajů

Kromě běžných typů osobních údajů je třeba rozlišit a do tabulky vyznačit formou „ano/ne", zda je v rámci příslušného účelu zpracován osobní údaj zvláštní kategorie.

Příklad vyplnění: „ano"

Ke zpracování zvláštní kategorie osobních údajů patří zpracování informací vypovídajících o:

- rasovém či etnickém původu,
- politických názorech,
- náboženském vyznání či filozofickém přesvědčení,
- členství v odborech,
- genetických údajích (osobní údaje týkající se zděděných nebo získaných genetických znaků fyzické osoby, které poskytují jedinečné informace o její fyziologii či zdraví a které vyplývají zejména z analýzy biologického vzorku dotčené fyzické osoby),
- biometrických údajích (osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo vlastnoruční podpis),
- údajích o zdravotním stavu (osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu),
- údajích o sexuálním životě nebo sexuální orientaci,
- osobních údajích dítěte (fyzické osoby mladší 16 let),

- osobních údajích o trestné činnosti.

Jejich přítomnost signalizuje vysoké riziko pro dotčené subjekty údajů, což se projeví ve výsledné míře rizikovosti zpracování.

h) Zdroj osobních údajů

Zdrojem osobních údajů se rozumí zdroj, který osobní údaje k příslušnému účelu poskytl.

Příklad vyplnění: „veřejná sociální síť“

Důležité je určit, zda jsou informace získávány:

- přímo od subjektu údajů,
- z jiného zdroje:
  - od třetí osoby,
  - z jiných zdrojů a to i veřejných (Rejtřík trestů, sociální síť, soukromá detektivní kancelář apod.).

i) Způsob pořízení

Způsobem pořízení se rozumí prostředek, jakým byly osobní údaje k příslušnému poskytnuty.

Příklad vyplnění: „osobně“

K typům způsobů pořízení patří například:

- osobně,
- e-mailem,
- poštou,
- datovou schránkou,
- webovým formulářem / aplikací,
- z jiné evidence nebo IS.

j) Četnost zpracování

Zde je nutno uvést, jak často (průměrně) dochází ke zpracování osobních údajů (vyjma jejich pouhého uložení). Pokud nelze kvantifikovat ani průměrně, je třeba uvést hodnotu „nepravidelně v případě potřeby“.

Příklad vyplnění: „jednou za měsíc“

Cílem je získat přehled o tom, jak často lze aktuálnost osobních údajů kontrolovat dotazem na subjekt osobních údajů nebo porovnáním s jinou evidencí. Jedná se o naplnění zásady přesnosti osobních údajů dle čl. 5 Nařízení GDPR (3, s. 35):

„Osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny.“

k) Rozsah zpracování

Rozsah zpracování je položka rozlišující mezi malým a velkým množství zpracovávaných osobních údajů.

Příklad vyplnění: „velké“

Je třeba napsat hodnotu “velké” v případě, že je splněna alespoň jedna z následujících podmínek:

- Počet dotčených subjektů údajů po dobu jejich životnosti do doby jejich vymazání je řádově 10 tisíc a více.
    - Příklad: Ročně začne se společností spolupracovat celkem 1000 nových klientů. Některé jejich osobní údaje je třeba uchovávat 10 let z důvodu plnění právní povinnosti (např. faktury). Kumulovaný počet klientů, jejichž osobní údaje je třeba uchovávat po dobu 10 let, je 10 000. Rozsah zpracování osobních údajů je tedy “velký”.
- Jedná se o každodenní zpracování osobních údajů, např. osobní údaje zaměstnanců při běžném provozu společnosti nebo za účely behaviorálního marketingu webovým vyhledávačem.

V opačném případě je potřeba napsat hodnotu “malé”.

l) Způsob uložení

Způsobem uložení osobního údaje se rozumí forma, v jaké jsou osobní údaje uloženy při jejich zpracovávání.

Příklad vyplnění: „kartotéka“

Jednotlivé způsoby uložení osobních údajů lze rozlišit na:

- listinné – např. do spisu, kartotéky, sejfu,
- elektronické - např. na CD, společné úložiště, do speciální databáze apod.

m) Předávání třetím stranám

Zde je potřebné uvést, zda zpracovávané osobní údaje jsou předávány třetím stranám a případně jakým.

Příklad vyplnění: „Finanční úřad“

Zvláště je potřebné uvést, jestliže jsou osobní údaje předávány:

- mimo území EU,
- mezinárodním organizacím, které mají působnost mimo EU,
- za účelem dalšího komerčního zpracování.

n) Prostředek a způsob zpracování

Prostředkem zpracování osobních údajů se rozumí forma, v jaké jsou osobní údaje zaznamenány při jejich zpracovávání.

Příklad vyplnění: „webový formulář“

K dalším typům prostředků zpracování osobních údajů patří:

- písemné dokumenty (smlouvy, formuláře, žádosti,..),
- digitální média (CD),
- aplikace.

Způsobem zpracování osobních údajů se rozumí popis operace nebo činnosti v rámci uvedeného prostředku zpracování.

Příklad vyplnění: „manuálně“

K dalším typům způsobů zpracování osobních údajů lze uvést:

- předání dokumentu,
- zpřístupnění dat v aplikaci oprávněnému uživateli,
- zaslání dat prostřednictvím webového formuláře,
- manuálně/automaticky.

o) Doba uchování

Cílem je určit dobu, po kterou budou osobní údaje zpracovávány, aby tato doba mohla být zaznamenána, sledována a sdělena subjektu údajů. Po uplynutí této doby se musí osobní údaje přestat zpracovávat. Je potřebné uvést, jak dlouho jsou dané osobní údaje uchovávány, resp. jak dlouho se s nimi pracuje či jsou někde uložené před tím, než jsou zničeny, skartovány, anonymizovány. Je možné uvést časový údaj (např. 5 let apod.) nebo logickou podmínku (po dobu studia, 5 let po ukončení pracovního poměru, do ukončení výběrového řízení apod.).

Příklad vyplnění: „1 rok“

p) Informační systém

Určení v jakém informačním systému se příslušné osobní údaje uchovávají a zpracovávají. Tyto informace slouží ke zjištění, ve kterých informačních systémech jsou osobní údaje zpracovávány a které je třeba posoudit z hlediska jejich zabezpečení.

q) Název datasetu

Dataset je souhrnné označení dokumentů nebo části informačního systému, ve kterých jsou obsaženy osobní údaje zpracovávané za předem stanoveným účelem a po stanovenou dobu.

Příklad vyplnění: „návštěvní kniha“

K typům datasetů mohou patřit následující:

- za účelem plnění právní povinnosti je třeba vést evidenci pracovní doby s uvedením délky směny, práce přesčas apod.; tato evidence bude datasetem přiřazeným k danému účelu,
- za účelem zachování bezpečnosti v budově a ochrany majetku správce, požaduje recepční identifikační údaje návštěvníka, které zapisuje do návštěvní knihy; návštěvní kniha je datasetem.

4.3.4 Prvotní posouzení rizikovosti zpracování

V souladu s požadavky GDPR bylo provedeno prvotní posouzení rizikovosti zpracování dle kritérií WP248 (13) pro hodnocení jednotlivých zpracování osobních údajů, jehož cílem je zjistit vysoce riziková zpracování, pro něž je nutné provést DPIA. Zpracování, jež nejsou zjištěna jako vysoce riziková, jsou řešena pouze v rámci PIA.

Schopnost rozlišit ve významu jednotlivých zpracování osobních údajů z pohledu kritičnosti pro subjekt údajů je v metodice využita pro vypořádání se s problémem hodnocení aktiv v rámci analýzy rizik (pro oblast osobních údajů představovanou PIA). Analýza rizik spojená s osobními údaji principiálně obsahuje zásadní problém, a to, že lze jen velmi obtížně stanovit hodnotu aktiv (osobních údajů), neboť tato hodnota může být pro jednotlivé subjekty údajů zásadně rozdílná a nelze ji jednoduchým způsobem objektivizovat. Pro účely hodnocení aktiv bylo proto využito kritérií WP248 (13), která ve svém stanovení kritičnosti jednotlivých zpracování obsahují míru dopadu zpracování na subjekty údajů, a tedy odvozeně i obecnou představu o hodnotě těchto aktiv.

4.3.4.1 Identifikace a hodnocení jednotlivých zpracování osobních údajů

Osobní údaj (aktivum) zahrnuje zejména informace získané formou interview, dotazníků, existující dokumentace aj. Obecně jsou aktiva identifikována na úrovni jednotlivých položek mající stejný charakter nebo účel.

Pro každé aktivum je určen typ aktiva, přičemž aktiva stejného typu mohou být zařazována do skupin aktiv a následně může být pracováno pouze s touto skupinou aktiv. Všechny typy aktiv jsou rozděleny do následující kategorií:

- primární aktiva – soubory informací v různé podobě a služby,
- podpůrná aktiva – technická aktiva, např. hardware, software, datová média aj.

Hodnocení jednotlivých zpracování osobních údajů je prováděno s cílem poskytnout konkrétnější soubor zpracovatelských operací, které vyžadují provedení Posouzení vlivu na ochranu osobních údajů – DPIA z důvodu jejich vysokého rizika. Jsou aplikována kritéria obecného posouzení úrovně rizika dle WP248 (13), kdy by mělo být zváženo následujících devět kritérií s ohledem na operace zpracování s vysokou pravděpodobností, že povedou k vysokému riziku.

Tabulka 1 - Hodnocení jednotlivých zpracování osobních údajů dle WP248

Kritérium	Definice
WP248 – profilování a jiná evaluace či hodnocení (tzv. scoring) subjektů údajů	Jedná se o hodnocení nebo bodování, včetně profilování a předpovídání, a to zejména aspektů souvisejících s pracovním výkonem subjektu údajů, jeho ekonomickou situací, zdravotním stavem, osobními preferencemi nebo zájmy, spolehlivostí nebo

Kritérium	Definice
	chováním, místem pobytu či pohybu (71 a 91 bod odůvodnění Nařízení).
	Může se jednat například o finanční instituci, která prověřuje svého zákazníka v databázi úvěrových referencí nebo společnost, která vytváří behaviorální nebo marketingové profily na základě používání webových stránek nebo pohybu na nich.
WP248 - automatizované rozhodování	Automatizované rozhodování, které má právní nebo podobně závažný dopad: zpracování, jehož cílem je rozhodování o subjektech údajů, jež má ve vztahu k fyzickým osobám právní účinky nebo má na fyzické osoby podobně závažný dopad. Na zpracování, které má jen nepatrný nebo žádný dopad na jednotlivce, se toto konkrétní kritérium nevztahuje (čl. 35 odst. 3 písm. a).
	Např. zpracování může mít za následek vyloučení ze společnosti nebo diskriminaci jednotlivců.
WP248 - systematické monitorování	Zpracování, které je používáno k pozorování, monitorování nebo kontrole subjektů údajů, včetně údajů shromážděných prostřednictvím sítí nebo rozsáhlé systematické monitorování veřejně přístupných prostorů (čl. 35 odst. 3 písm. c).
WP248 – zpracování citlivých údajů	Spadají sem i zvláštní kategorie osobních údajů ve smyslu čl. 9 Nařízení (např. údaje týkající se politických názorů jedince), stejně jako osobní údaje týkající se rozsudků v trestních věcech a trestných činů vymezených v čl. 10. V posuzování může být důležité, zda subjekt údajů nebo třetí osoby údaje už zveřejnily. Skutečnost, že osobní údaje jsou veřejně dostupné, může být považována za jeden z faktorů při posouzení, zda se počítalo s dalším využitím údajů.
	Např. zdravotnická dokumentace uchovávaná ve všeobecné nemocnici nebo podrobné údaje vedené soukromým vyšetřovatelem vůči pachateli. Kromě těchto ustanovení Nařízení mohou zvyšovat možné riziko pro práva a svobody jednotlivců některé další kategorie údajů. Tyto osobní údaje jsou považovány za citlivé (v běžném smyslu toho slova), protože mají vazbu na domácnosti a soukromé činnosti (jako např. elektronické komunikace, jejichž důvěrný charakter by měl být chráněn) nebo protože mají dopad na výkon základních práv (např. lokalizační údaje, jejichž shromažďování zpochybňuje svobodu pohybu) nebo proto, že jejich porušení má jednoznačně závažný vliv na každodenní život subjektů údajů (např. finanční údaje, které by mohly vést k podvodům s platbami). Toto kritérium může zahrnovat také údaje, jako jsou např. osobní dokumenty, e-maily, osobní deníky, elektronická čtecí zařízení vybavená funkcemi poznámek a informace velmi

Kritérium	Definice
	osobní povahy obsažené v aplikacích zaznamenávajících průběh denních aktivit subjektu údajů (tzv. „lifelog“).
WP248 – zpracování velkého rozsahu	Je doporučeno, aby při určování, zda je zpracování rozsáhlé, byly zvažovány zejména tyto faktory: a) počet dotčených subjektů údajů vyjádřený konkrétním číslem, nebo jako podíl příslušné populace; b) objem údajů a/nebo rozsah jednotlivých zpracovávaných údajů; c) délka nebo trvání činnosti zpracování údajů; d) zeměpisný rozsah zpracovatelské činnosti.
WP248 – kombinování osobních údajů z různých datových sad	Pokud například pocházejí ze dvou nebo více operací zpracování údajů prováděných pro různé účely a/nebo různými správci údajů způsobem, který by přesahoval přiměřené očekávání subjektů údajů.
WP248 – zpracování osobních údajů zranitelných osob	Zpracování tohoto druhu údajů je jedním z kritérií, jestliže existuje jasná nerovnováha moci mezi subjekty údajů a správcem údajů, což znamená, že pro jednotlivce může být nemožné snadno vyslovit souhlas případně nesouhlas se zpracováním svých údajů, nebo vykonávat svá práva (75 bod odůvodnění).
	Mezi zranitelné osoby mohou patřit děti (u nichž lze mít za to, že nejsou schopny vědomě nebo promyšleně vyslovit nesouhlas popřípadě souhlas se zpracováním svých údajů), zaměstnanci, zranitelnější skupiny obyvatelstva, které vyžadují zvláštní ochranu (osoby s duševní chorobou, žadatelé o azyl nebo starší osoby, pacienti atd.) a všichni ti, v jejichž případech je možné stanovit nerovnováhu ve vztahu mezi postavením subjektu údajů a správce.

Kritérium	Definice
WP248 - inovativní užití či aplikace technologických nebo organizačních řešení	Použití nové technologie, definované v „souladu s dosaženou úrovní technických znalostí“, může zakládat potřebu provést Posouzení vlivu na ochranu osobních údajů. Použití této technologie totiž může zahrnovat nové formy sběru a použití údajů s potenciálně vysokým rizikem pro práva a svobody fyzických osob. Osobní a sociální důsledky zavedení nové technologie mohou být nepředvídatelné. Posouzení vlivu na ochranu osobních údajů pomůže správci údajů porozumět těmto rizikům a řešit je (čl. 35 odst. 1, 89 a 91 bod odůvodnění).
	Např. kombinace použití otisků prstů a rozpoznávání obličejů pro zlepšení omezení fyzického přístupu atd.
WP248 - bránění v užívání některé služby nebo uplatňování svých práv	Operace zpracování, které mají za cíl umožnit, změnit nebo zamezit subjektu údajů přístup ke službě nebo uzavření smlouvy.
	Např. banka, která prověřuje svého zákazníka v databázi úvěrových referencí, aby rozhodla, zda mu udělí úvěr, či nikoli.

Zdroj: vlastní zpracování dle (13)

Na základě zjištěných poznatků v teoretické části této práce bylo zjištěno, že pokud správce vyhodnotí, že jím zamýšlená operace zpracování obsahuje alespoň dva z těchto faktorů, měl by provést Posouzení vlivu na ochranu osobních údajů. Dle kritéria obecného posouzení rizika se zjistí kritičnost daného zpracování, např. evidence pracovních úrazů, jež je dána počtem výskytů jednotlivých kritérií:

Tabulka 2 - Kritičnost zpracování osobních údajů

Identifikace zpracování	**Kritéria obecného posouzení úrovně rizika**									
Účel zpracování osobních údajů	WP248 profilování	WP248 automat. rozhodování	WP248 system. monitorování	WP248 citlivé údaje	WP248 velký rozsah	WP248 kombinování	WP248 zranitelné osoby	WP248 inovativní užití	WP248 bránění v užívání	**Kritičnost zpracování SUMA**
Evidence pracovních úrazů				**X**	**X**					**2**

Zdroj: vlastní zpracování

Může nastat situace, kdy operace zpracování bude odpovídat výše uvedenému příkladu a správce stále považuje za nepravděpodobné, že by „mohla způsobit vysoké riziko“.

V takových případech by měl správce zdůvodnit a zdokumentovat důvod, proč neprovádí DPIA, a zahrnout či zaznamenat i názory pověřence pro ochranu osobních údajů (tzv. DPO) byl-li jmenován. Kromě toho podle Nařízení GDPR (3) v rámci zásady odpovědnosti každý správce údajů vede záznamy o zpracovatelských činnostech, za něž odpovídá, včetně účelu zpracování, popisu kategorií údajů, příjemců údajů a obecný popis technických a organizačních bezpečnostních opatření, pokud je to možné.

4.3.5 Posouzení dopadů rizik na ochranu osobních údajů – PIA

PIA představuje analýzu rizik pro oblast osobních údajů a je zpracována na základě interview s odpovědnými pracovníky společnosti. Je vytvořena za účelem naplnění odpovědnosti správce osobních údajů, definované v Nařízení GDPR (3, s. 47), kde správce „*S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto Nařízením*“.

Jelikož jdou požadavky Nařízení GDPR (3) nad rámec současného zákona 101/2000 Sb. o ochraně osobních údajů (12), tak musí být ošetřena veškerá zpracování osobních údajů týkající se fyzických osob, a to před samotným zpracováním. Z principů GDPR vychází povinnost zabývat se riziky souvisejícími se zpracováním osobních údajů prováděných správcem nebo zpracovatelem a dokladovat tento proces řízení rizik. Jsou tak výrazně posílena práva jednotlivců k ochraně jejich osobních údajů, čemuž odpovídají i nové povinnosti správců a zpracovatelů osobních údajů. Způsob provedení hodnocení rizik pro práva a svobody fyzických osob by měl být zvolen správcem osobních údajů, přičemž forma tohoto hodnocení by měla odpovídat charakteru společnosti. Jeden z možných způsobů provedení PIA je popsán normou ISO/IEC 29134 (19).

V rámci posouzení dopadů rizik na ochranu osobních údajů je třeba provést několik dílčích kroků, jež jsou zobrazeny v následujícím schématu. Nejprve jsou identifikována aktiva neboli jednotlivá zpracování osobních údajů, jejichž hodnota je určena prvotním posouzením rizikovosti dle kritérií WP248 (13). Následně jsou identifikovány a ohodnoceny hrozby a zranitelnosti z pohledu jednotlivých typů aktiv dle Katalogu hrozeb ISO/IEC 29134 (20). Na základě těchto výsledných hodnot ohodnocení aktiv, hrozeb a zranitelností je

zjištěna míra rizika jednotlivých zpracování osobních údajů. V rámci PIA jsou následně navržena opatření pro zpracování, jež nebyla shledána jako vysoce riziková. Naopak pro zjištěná vysoce riziková zpracování je třeba provést Posouzení vlivu na ochranu osobních údajů – DPIA, jež posoudí dopady konkrétního rizikového zpracování osobních údajů na soukromí a potenciální rizika takového zpracování pro práva a svobody subjektů údajů.

Schéma č. 6 – Proces posouzení dopadů rizik na ochranu osobních údajů – PIA

Zdroj: vlastní zpracování

4.3.5.1 Riziko pro práva a svobody fyzických osob

Riziko pro práva a svobody fyzických osob neboli „privacy risk" je hypotetický scénář, který popisuje:

- jak by zdroj rizika (např. zaměstnanec)
- mohl využít zranitelnosti osobních údajů v oblasti podpůrných aktiv (např. souborový systém, který umožňuje manipulaci s daty)
- v souvislosti s hrozbami (např. zneužitím zasíláním e-mailů)
- a umožnil výskyt nežádoucích událostí (např. neoprávněný přístup k osobním údajům)
- na specifické osobní údaje (např. soubor zákazníka)
- a tak způsobil dopad na soukromí subjektů údajů (např. nevyžádané obchodní sdělení, pocity invaze soukromí atd.).

4.3.5.2 Posuzování rizik zpracování osobních údajů

Cílem posuzování rizik je identifikovat, vyhodnotit rizika a správně pochopit jejich příčiny a důsledky. Před zahájením procesu posuzování rizik je třeba stanovit a zdokumentovat účel a rozsah řízení rizik, které určují podrobnost řízení rizik osobních údajů.

Hlavním účelem řízení rizik zpracování osobních údajů je:

- zajistit schopnost správce osobních údajů doložit, že zpracování osobních údajů je prováděno v souladu s Nařízením, tj. že jsou zavedena vhodná technická a organizační opatření s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob,
- identifikovat dopady na soukromí fyzických osob,
- přezkoumání rizik v oblasti ochrany soukromí také u nových technologií zpracování, projektů atd., a posouzení jejich dopadu a pravděpodobnosti,
- sdílení a snížení rizik spojených s osobními údaji se zainteresovanými stranami nebo poskytnutí důkazů týkajících se souladu s Nařízením.

Rozsah řízení rizik osobních údajů dále určuje specifické podrobnosti o tom:

- co bude v rámci řízení rizik pokryto (např. jaká zpracování osobních údajů budou do přezkoumání zahrnuty, jaké informační systémy, organizační jednotky, technická infrastruktura, atd.),
- jak se přezkoumání rizik provede,
- kdo přezkoumání rizik provede (sestavení týmu osob, který provede přezkoumání rizik),
- kdy bude přezkoumání provedeno (termín zahájení a ukončení).

Tento rozsah musí být přizpůsoben velikosti organizace (nebo její části), informačnímu systému nebo procesu, který je předmětem řízení rizik. Pro účely posuzování rizik je možná určitá forma sdružování, např. zpracování podobného typu, podobná zpracování v rámci jednoho informačního systému atd.

Identifikace a hodnocení hrozeb a zranitelností

Hrozby a zranitelnosti jednotlivých zpracování osobních údajů jsou identifikovány z pohledu hrozeb a zranitelností jednotlivých typů aktiv, na nichž jsou jednotlivá zpracování osobních údajů závislá a pro jednotlivé operace / typy operací, které jsou v životním cyklu zpracování osobních údajů prováděny, a to též s ohledem na druh typu aktiva – podpůrného média (písemnost, digitální).

Pro identifikaci hrozeb a zranitelností podpůrných aktiv je aplikován Katalog hrozeb dle ISO 29134 (20) – viz Příloha č. 4. Před provedením posuzování rizik je nutné prověřit, zda hrozby a zranitelnosti obsažené v Katalogu odpovídají specifikým podmínkám daného kontextu a rozsahu posuzování a případně Katalog upravit (např. přidat specifické hrozby, atd.). K aktivům jsou přiřazovány pouze relevantní hrozby, které je mohou poškodit, a to vše za předpokladu neexistence standardních bezpečnostních opatření.

Tyto hrozby a jejich zranitelnosti jsou hodnoceny genericky s ohledem na pravděpodobnost / četnost jejich vzniku následovně:

Tabulka 3 – Kategorizace hodnocení hrozeb operací zpracování

Úroveň	Hrozba	Popis
Nízká	0	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let
Střední	1	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	2	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	3	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Zdroj: vlastní zpracování dle (21)

Míra hrozby pro danou skupinu zpracování je dána součtem hrozeb podpůrných aktiv. Toto se provádí v Registru zpracování (viz Příloha č. 5), kde se u každého jednotlivého / skupiny zpracování provede ohodnocení hrozeb dle Katalogu hrozeb (viz Příloha č. 4), s ohledem na pravděpodobnost / četnost jejich vzniku u konkrétního zpracování.

Příklad:

Účel zpracování osobních údajů: Evidence pracovních úrazů

- **Způsob uložení: v listinné podobě**, jsou tedy aplikovány hrozby a zranitelnosti s jejich pravděpodobností pro podpůrná aktiva:
  - Papírové dokumenty
  - Kanály přenosu papíru

  A tyto jsou promítnuty do **Míry hrozby daného zpracování**: **25**

Tabulka 4 – Identifikace hrozeb a zranitelností

	Identifikace a hodnocení hrozeb a zranitelností																												
	Hardware											Software											Počítačové kanály						
Σ kritič nosti	HW 01	HW 02	HW 03	HW 04	HW 05	HW 06	HW 07	HW 08	HW 09	HW 10	HW 11	SW 01	SW 02	SW 03	SW 04	SW 05	SW 06	SW 07	SW 08	SW 09	SW 10	SW 11	CH 01	CH 02	CH 03	CH 04	CH 05		
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		

Jednotlivci									Papírové dokumenty						Kanály přenosu papíru							
HU 01	HU 02	HU 03	HU 04	HU 05	HU 06	HU 07	HU 08	PD 01	PD 02	PD 03	PD 04	PD 05	PD 06	PP 01	PP 02	PP 03	PP 04	PP 05	PP 06	Σ hrozeb	Rizikovost
0	0	0	0	0	0	0	0	1	2	3	2	2	1	2	3	2	2	3	2	25	50

Zdroj: vlastní zpracování

Následně se provede **určení úrovně rizik**, přičemž výpočet úrovně rizika je dán součinem:

Míra rizika = Kritičnost zpracování x Míra hrozby

Příklad:

Účel zpracování osobních údajů: Evidence pracovních úrazů

- **Kritičnost zpracování: 2** (dle kritéria obecného posouzení úrovně rizika)
- **Způsob uložení: v listinné podobě**, **míry hrozby daného zpracování**: **25**
- **Míra rizika: 50**

V rámci hodnocení rizik je vhodné zohlednit i případnou kumulaci rizik, kdy větší množství rizik spojených jedním typem hrozby nebo aktivem, může znamenat daleko vyšší celkové riziko.

Riziková kategorie je stanovena podle níže navrženého indexu rizika a rizikové kategorii odpovídá i způsob návrhu opatření. Hodnoty je třeba vždy přizpůsobit výslednému rozpětí rizik.

Tabulka 5 – Kategorizace rizik

Kategorie	Skóre	Riziko a způsob návrhu opatření
1	**0 - 9**	**Nízké** - riziko je považováno za přijatelné
2	**10 - 99**	**Střední** - riziko by mělo být sníženo na nejnižší možnou přijatelnou míru Dle rozhodnutí *vlastníka rizika* (odpovědný za hodnocení a zvládání rizika, za řízení životního cyklu rizika, případně za akceptaci rizika) mohou být v rámci daného rizika vyhodnoceny největší hrozby (např. dle Paretova pravidla 80 : 20) a pro ně mohou být přijata odpovídající opatření za účelem ošetření rizika, pokud je to vhodné (např. odpovídající poměr náklady na opatření vs. přínosy). Opatření je možné, dle rozhodnutí vlastníka rizika, stanovit vůči skupině hrozeb se shodným působením, nebo vůči jednotlivým hrozbám.
3	**100 -**	**Vysoké** - riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění. Opatření je nutné stanovit vůči jednotlivým hrozbám v maximální míře podrobnosti tak, aby byl doložen důkaz, že žádná klíčová hrozba nebyla opomenuta.

Zdroj: vlastní zpracování

U těchto zjištěných rizik je dále nutné stanovit prioritu pro ošetření jednotlivých rizik. Prioritizace rizik může být založena například na:

- omezených zdrojích posuzovatele (např. omezené lidské zdroje k provádění ošetření rizika),
- akceptaci určitého typu rizika (např. snaha o prioritní posouzení rizik souvisejících s pořízením nového informačního systému).

Výstupem procesu posuzování dopadů rizik na ochranu osobních údajů – PIA je výše rizik jednotlivých zpracování, na základě které jsou následně navrhována vhodná opatření pro jejich zmírnění.

Zvládání rizik zpracování osobních údajů

Vstupem pro zvládání rizik je seznam rizik zpracování osobních údajů, kterým byla přiřazena priorita pro následné ošetření. U těchto rizik je dále nutné rozhodnout, jakým způsobem s nimi bude naloženo, tj. určit způsob jejich zvládání.

Na základě studia odborné literatury a především normy ČSN ISO/IEC 27005 (1) byly stanoveny základní metody zvládání rizik viz kapitola 3.1.4:

- modifikace rizik bezpečnosti informací – tj. aplikace vhodných opatření, která riziko eliminují nebo sníží,
- podstoupení rizik bezpečnosti informací – tj. akceptování rizika bez další akce,
- vyhnutí se riziku bezpečnosti informací – pomocí vyhnutí se činnosti nebo podmínce, která dává možnost riziku vzniknout,
- sdílení rizik bezpečnosti informací – např. pomocí pojištění nebo outsourcingu.

Výstupem tohoto procesu zvládání rizik je rozhodnutí o způsobu zvládání rizik, měl by být také zpracován Plán zvládání rizik – dokument, který stanovuje, jak ošetřit rizika, jež převyšují stanovenou míru akceptovatelného rizika, a zároveň definuje pořadí priorit, v němž by měly být aplikovány vybrané způsoby zvládání rizik a to včetně jejich časových rámců. Po definování Plánu zvládání rizik by měla být určena zbytková rizika. Úroveň rizik je řízena výběrem variant pro ošetření rizik tak, aby mohlo být zbytkové riziko přehodnoceno jako akceptovatelné. Poté je třeba zjistit, zda zbytkové riziko stále nesplňuje kritéria pro akceptaci rizik, v takovém případě by bylo nezbytné opakovat další zvládání rizik, než by se mohlo přejít k akceptaci rizik.

4.3.6 Postup návrhu opatření pro ošetření rizik

V rámci návrhu opatření jsou vybírána vhodná a odůvodněná opatření, která sníží rizika při zpracování osobních údajů. Tento výběr bere v úvahu:

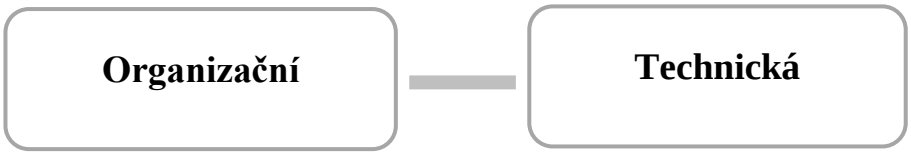
- kritéria akceptace rizik,
- požadavky právní (musí být splněny),
- regulatorní a

- smluvní požadavky.

Podrobné informace a dobrou praxi v oblasti zavádění opatření poskytuje například norma ISO/IEC 27002 (22). Během výběru opatření je třeba zvážit náklady na získání, zavedení, spravování, provozování, monitorování a údržbu opatření ve vztahu k hodnotě chráněných aktiv. Kromě toho je nutné přihlížet i k tomu, že k definování a přijetí nových opatření nebo ke změně existujících opatření mohou být zapotřebí specializované způsobilosti a odpovídající bezpečnostní povědomí.

Po konzultaci s bezpečnostním manažerem společnosti byla opatření rozdělena do následujících dvou oblastí:

Schéma č. 7 – Typy opatření pro ošetření rizik



Zdroj: vlastní zpracování

Organizační opatření

Jedná se o opatření zahrnující změny stávajících a zavedení nových procesů, především zaměřených na ochranu osobních údajů. Mezi tato opatření mohou patřit například:

- zavedení procesu řízení dodavatelů,
- vytvoření politiky bezpečnosti sítí,
- vytvoření politiky kryprografických opatření,
- zavedení pravidel ochrany zařízení mimo organizaci apod.

Technická opatření

Obsahem těchto opatření jsou návrhy technických řešení, která mají podporovat nezbytné bezpečnostní procesy, případně kompenzovat některou technickou zranitelnost. Mezi taková opatření mohou patřit:

- nástroje pro sběr, agregaci a vyhodnocování logů a bezpečnostní dohled,
- nástroje pro řízení přístupu a oprávnění,
- nástroje pro šifrování,

- webový aplikační firewall apod.

Návrh technických opatření musí být proveden v součinnosti s osobou odpovědnou za ICT společnosti.

Postup výběru opatření je takový, že po výpočtu rizika a zjištění, že se jedná o riziko přesahující míru akceptovatelného rizika, a je tudíž určeno k redukci pomocí opatření, následuje pro toto riziko dohledání, jaké hrozby ho působí. Toto je patrné z vypracovaného Registru zpracování, kde jsou hrozby týkající se jednotlivých zpracování ohodnoceny. Pro tyto hrozby jsou následně vybírána vhodná opatření z Katalogu opatření uvedeného v ISO/IEC 29151 (23). Pokud je přijato například jedno opatření, které pokryje danou hrozbu, a tím se sníží pravděpodobnost realizace této hrozby tak, že riziko klesne pod akceptovatelnou míru, pak stačí přijmout toto jedno opatření. Druhým případem je situace, kdy se jedním přijatým opatřením nepodaří snížit riziko pod akceptovatelnou úroveň, a pak je nutné přijmout další opatření, protože to znamená, že dané riziko působí ještě jiné další hrozby, které se uplatňují vůči tomuto zpracování.

Následující tabulka je přehledem možných bezpečnostních opatření a je vytvořeno jejich namapování na hrozby z Katalogu hrozeb (viz Příloha č. 4). Opatření jsou rozdělena podle typu na organizační (ID ORxx) a technická (ID TExx).

Tabulka 6 – Mapování opatření na hrozby z Katalogu hrozeb

ID opatření	Název opatření	Návaznost na hrozby
OR01	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	Všechny
OR02	Pokyny vedení pro bezpečnost informací	Všechny
OR03	Stanovení organizace ochrany osobních údajů	Všechny
TE01	Přijetí opatření pro zabezpečení mobilních zařízení a vzdáleného přístupu k informačnímu systému organizace	HW01, HW02, HW05, HW06
OR04	Stanovení pravidel pro ochranu osobních údajů před vznikem pracovního poměru	HU01, HU02, HU03, HU04
OR05	Stanovení pravidel pro ochranu osobních údajů v průběhu pracovního poměru	HU01, HU02, HU03, HU04, HU07, HU08
OR06	Stanovení pravidel pro ochranu osobních údajů během procesu ukončení pracovního poměru	HU01, HU02, HU03, HU04, HU05, HU06

ID opatření	Název opatření	Návaznost na hrozby
OR07	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	Všechny
OR08	Provedení kategorizace a ohodnocení zpracování osobních údajů	Všechny
TE02	Stanovení pravidel pro ochranu fyzických médií	HW01, HW02, HW03, HW06, HW10, HW11, PD01, PD02, PD03, PD04, PD05, PD06, PP02, PP05
OR09	Stanovení uživatelských rolí a jejich přístupových oprávnění	SW02, SW03, PD02
TE03	Zavedení opatření pro prosazování pravidel řízení přístupu	SW02, SW03
OR10	Stanovení a vynucování odpovědností uživatelů informačního systému	HW02, HW04, HW05, HW06, HW08
TE04	Zavedení řízení přístupů k systémům a aplikacím	SW02, SW03, SW06
TE05	Využití kryptografických prostředků pro ochranu dat	HW02, HW06, CH02, CH04
OR11	Zavedení zabezpečených oblastí a pravidel pro práci v nich	HW01, HW02, HW04, PD01, PD02, PD03, PD04, PD05
OR12	Zavedení fyzické ochrany ICT vybavení	HW01, HW03, HW04, HW11, CH03
OR13	Stanovení postupů a odpovědností ICT provozu	HW07, HW09, HW10, HW11, SW01, SW03, SW07, SW08, SW09, SW10, CH01, CH04
TE06	Přijetí opatření chránících před malwarem	SW02, SW04, SW05, SW08, SW09, SW10
TE07	Provádění zálohování dle zálohovacího plánu	HW01, HW03, HW10, SW01, SW03, SW11
TE08	Pořizování záznamů z přístupu k osobním údajům a bezpečnostní dohled	HW08, SW02, SW03, SW04, SW05, SW06, SW08, SW09, SW10, CH02, CH05
TE09	Zavedení pravidel správy softwarového vybavení	SW04, SW08, SW09, SW10
TE10	Zavedení procesu řízení technických zranitelností	HW01, SW04
OR14	Provádění audit informačních systémů zpracovávajících osobní údaje	SW02
TE11	Zavedení bezpečnostních opatření pro ochranu komunikačních sítí	SW02, SW05, SW06, CH01, CH02, CH04, CH05
TE12	Zabezpečení přenášených osobních údajůí	HW02, CH02, CH04

ID opatření	Název opatření	Návaznost na hrozby
OR15	Stanovení bezpečnostních požadavků na informační systémy zpracovávajících osobní údaje	HW01, SW01, SW11
OR16	Stanovení pravidel pro vývojové a podpůrné procesy	HW07, HW09, SW11
TE13	Stanovení pravidel pro testování	HW07, HW09, SW11
OR17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	HW07, HW09, HW11, SW01, SW02, SW06, SW08, SW09, SW10, CH02, CH04, CH05, PP03
OR18	Dohledování a řízení dodavatelsky zajišťovaných služeb	SW03, SW06, CH05, PP03, PP06
OR19	Zavedení procesu řízení bezpečnostních incidentů	SW05, SW06
OR20	Stanovení pravidel bezpečnosti osobních údajů v procesech řízení kontinuity	HW03, HW10, CH01, CH03, CH05, PD01
TE14	Stanovení pravidel pro vysokou dostupnost ICT prostředků	HW01, HW03, HW10, CH05
OR21	Dodržování právních a smluvních požadavků	HW09, HW11, SW01, SW02, SW07, HU03, HU04, HU05, HU06, HU07, HU08, PP01, PP04
OR22	Zavedení procesu testování bezpečnosti osobních údajů	HW04, SW02, SW05, SW06, CH02

Zdroj: vlastní zpracování dle (23) a (Příloha č. 4)

Během mapování opatření na hrozby z Katalogu hrozeb bylo zjištěno, že existuje několik opatření, které mají plošnou působnost. Nejen že působí na všechna zpracování, ale zároveň i na všechny hrozby. Tato opatření lze nazvat jako systémová, která pokud se přijmou, tak působí na všechny typy zpracování (nezáleží ani na tom, zda se jedná o papírové či elektronické zpracování). Existují tedy takováto systémová opatření a dále opatření, která sice neovliňují všechny hrozby, ale i tak jich ovlivňují větší počet. Tato by se dala nazvat jako opatření s vysokou účinností. K těmto opatřením tedy patří následující: Stanovení pravidel pro ochranu fyzických médií, Stanovení postupů a odpovědností ICT provozu, Pořizování záznamu z přístupů k osobním údajům a bezpečnostní dohled, Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby a Dodržování právních a smluvních požadavků.

Výsledkem této činnosti by měl být seznam možných relevantních opatření s jejich náklady, přínosy a prioritou uplatnění.

4.3.6.1 Stanovení plánu ošetření rizik a zbytkových rizik

V návaznosti na vypracovaný návrh opatření pro ošetření rizik by mohl být sestaven Plán ošetření rizik, a to pokud je vybráno více opatření, aby byla možná identifikace pořadí priorit, ve kterém budou aplikovány jednotlivé způsoby ošetření rizik, odpovědnosti za jejich realizaci včetně časových rámců. Priority lze stanovit za použití různých technik, včetně klasifikace rizik a analýzy nákladů a výnosů. V souvislosti se sestavením Plánu ošetření rizik jsou identifikována zbytková rizika. Tato zbytková rizika je vhodné následně přezkoumat, zda skutečně splňují kritéria organizace pro akceptaci rizik.

Je důležité formálně zaznamenat rozhodnutí vedení společnosti ke schválení Plánu ošetření rizik a rozhodnutí akceptovat zbytková rizika. V Plánu pro ošetření rizik musí být uvedeno, jak jsou rizika ošetřena a zaznamenány eventuální důvody nedbání stanovených kritérií pro akceptaci rizik. V případě akceptace rizika musí být jednoznačně dohledatelná odpovědnost za dané rozhodnutí (autor návrhu akceptace rizika, projednání, schválení atd.).

4.4 Vzorové DPIA - Evidence docházky

V rámci ověřování praktické využitelnosti vytvořené metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů byla tato metodika využita pro data společnosti a jedno zjištěné vysoce rizikové zpracování – evidence docházky dle Registru zpracování osobních údajů viz Příloha č. 5. Toto ověření není hlavním záměrem diplomové práce, ale možnost ho v součinnosti se zástupcem společnosti vytvořit byla vítanou příležitostí k prokázání funkčnosti této metodiky.

Způsob vypořádání požadavků pro DPIA dle čl. 35 odst. 7 písm. Nařízení GDPR (3) byl projednán s bezpečnostním manažerem společnosti a je pro vzorové zpracování uveden v následující tabulce:

Tabulka 7 – Způsob vypořádání požadavků pro DPIA

Požadavek	Vypořádání	Odkaz na kapitolu DPIA
Povaha, rozsah, kontext a účely zpracování jsou zohledněny	Zpracování je prováděno přesně v míře nezbytné pro plnění právní povinnosti	Viz 4.4.1
Osobní údaje, subjekty údajů a období, v rámci kterého budou osobní údaje uloženy, jsou zohledněny	Zpracování je prováděno přesně v míře nezbytné pro plnění právní povinnosti. Rizika vyplývající z doby uložení jsou vyhodnocena a jsou přijata odpovídající opatření.	Viz 4.4.2 a 4.4.3
Je poskytnut funkční popis operace zpracování	Funkční popis operace zpracování je zpracován	Viz 4.4.2
Jsou identifikována aktiva, kterých se týkají osobní údaje	Aktiva jsou identifikována	Viz 4.4.3
Dodržování schválených kodexů chování	Pro tento typ zpracování nejsou schváleny žádné závazné a relevantní kodexy chování.	Není relevantní
Výslovné vyjádření a legitimita účelu zpracování – „účelové omezení“ (čl. 5 odst. 1 písm. B),	Účel je jasně stanoven a legitimní, neboť zpracování pro daný účel je vyžadováno zákonem a jedná se tedy o plnění právní povinnosti.	Viz 4.4.1
Zákonnosti zpracování	Účel, rozsah i doba zpacování jsou v souladu s právním základem.	Viz 4.4.1
Přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány	Zpracování je prováděno pouze v rozsahu nezbytném pro plnění právní povinnosti.	Viz 4.4.2
Omezená doba uložení osobních údajů – po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány	Zpracování je prováděno pouze v rozsahu nezbytném pro plnění právní povinnosti.	Viz 4.4.2
Informace poskytnuté subjektu údajů	Informace o zpracování osobních údajů pro účely evidence pracovní doby jsou předávány zaměstnanci v rámci nástupního procesu.	Viz 4.4.1
Právo na přístup k osobním údajům a právo na přenositelnost údajů	Právo je technicky zajištěno a možnost přístupu k datům školena v rámci vstupního školení.	Viz 4.4.1
Právo na opravu, výmaz, námitku, omezení zpracování	Právo je technicky zajištěno a možnost opravy školena v rámci vstupního školení.	Viz 4.4.1

Požadavek	Vypořádání	Odkaz na kapitolu DPIA
	Přenos, výmaz a omezení zpracování není vzhledem k charakteru plnění právní povinnosti relevantní.	
Zpracovatel	Není využívána služba externího zpracovatele	Není relevantní
Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím	Údaje nejsou předávány jiným subjektům	Není relevantní
Předchozí konzultace	Předchozí konzultace nebyla vzhledem k charakteru zpracování využita	Není relevantní
Zdroje rizika jsou zohledněny	Zdroje rizik jsou řešeny v rámci provedení PIA	Viz 4.4.3
Potenciální dopady na práva a svobody subjektů údajů jsou zjištěny v případě neoprávněného přístupu, nežádoucích změn a vymizení údajů.	Potenciální dopady na práva a svobody osob jsou posouzeny v rámci provedené DPIA.	Viz 4.4.3
Jsou identifikovány nežádoucí úpravy, zmizení údajů a hrozby, které by mohly vést k nelegitimní přístupnosti,	Hrozby pro dostupnost, důvěrnost a integritu údajů jsou zohledněny v rámci provedené PIA.	Viz 4.4.3
Je posouzena pravděpodobnost a závažnost rizik pro práva a svobody subjektů údajů	Rizika jsou posouzena v rámci provedené PIA.	Viz 4.4.3
Jsou stanovena plánovaná opatření k řešení těchto rizik	Pro rizika vybraná redukci jsou navržena opatření.	Viz 4.4.4
Je požadováno poradenství pověřence pro ochranu osobních údajů	Společnost nemá a není povinna mít určeného Pověřence pro ochranu osobních údajů	Není relevantní
Jsou požadovány názory subjektů údajů nebo jejich zástupců	Vzhledem k právnímu základu zpracování (plnění právní povinností) není vyžadováno.	Není relevantní

Zdroj: vlastní zpracování

Komentář společnosti: „Pro vytvoření DPIA se ukázalo jako velmi užitečné, že v metodikou navržené tabulce jsou kromě položek relevantních pro řízení rizik i položky související s ostatními požadavky na DPIA. Položky pro řízení rizik bylo možné vyřešit díky dodané metodice, položky související s plněním právní povinnosti jsme také využili a zadali jako jednotlivé úkoly firemnímu právníkovi.“

4.4.1 Účel a rozsah zpracování

Pro účely evidence docházky do zaměstnání a plnění právní povinnosti vyplývající z pracovního zákoníku zpracovává společnost Taylor McCoy osobní údaje zaměstnanců. Zpracovávanými osobními údaji jsou jméno, příjmení, ID číslo, přítomnost, odchody, nároky na dotované jídlo, nemoc, dárcovství krve, pohřeb osoby blízké, odchod k lékaři, dovolená, sick days a nároky na benefity. O účelu a rozsahu zpracování jsou zaměstnanci informováni při nástupu do zaměstnání v rámci vstupního školení. Součástí předávaných informací je i způsob náhledu na tato data a způsob žádosti o jejich opravu.

Data jsou uložena pouze po dobu nezbytnou pro uzavření docházky daného období (1 roku). Po skončení období jsou data smazána. Při odchodu zaměstnance jsou data smazána v rámci procesu ukončení pracovního poměru.

4.4.2 Popis zpracování

Zpracování evidence docházky je prováděno elektronicky na systému provozovaném a vlastněném společností. Data zpracování poskytuje přímo zaměstnanec, který je vkládá do klientské části aplikace. Data jsou uložena na straně klienta a v okamžiku připojení do Internetu automaticky synchronizována a uložena na serverové části. Původní data na straně klienta zůstávají uložena pro případ selhání synchronizace nebo opravy chyb.

Data jsou vyhodnocována jednou týdně. Sledovanými parametry jsou informace indikující nesoulad s plněním právní povinnosti a případně nesoulad s plněním smluvního vztahu mezi zaměstnavatelem a zaměstnancem (čerpání dovolené mimo sjednaný rámec, překážky v práci v rozsahu nad rámec zákona apod.).

Tato zjištění vedou k iniciaci oprav ve vedení evidence pracovní doby, případně k zahájení kárného řízení se zaměstnancem.

Všechny operace zpracování vkládání informací jsou svázány s jedinečným identifikátorem zaměstnance.

Případné porušení zabezpečení osobních údajů tohoto zpracování je řešeno jednotným procesem řízení bezpečnostních incidentů.

4.4.3 Hodnocení rizik zpracování

Zpracování evidence docházky bylo podle kritérií WP248 (13) vyhodnoceno jako potenciálně vysoce rizikové. Zpracování naplňuje více než dvě kritéria, a to Profilování a jiná evaluace či hodnocení, Automatizované rozhodování a Systematické monitorování viz Tabulka č. 8. Ve spojení s hrozbou vůči lokálně na mobilních prostředcích ukládaným datům je výsledkem vysoké riziko, pro něž by mělo být provedeno Posouzení vlivu na ochranu osobních údajů.

Tabulka 8 – Hodnocení rizika potenciálně rizikového zpracování dle WP248

Účel zpracování	WP248 Hodnocení nebo bodování Profilování a předpovídání	WP248 Autom. rozhodování s závažným (např. právním) dopadem	WP248 Systematické monitorování	WP248 Zvláštní a citlivé údaje	WP248 Velký rozsah
Evidence docházky	Ano	Ano	Ano	Ne	Ne

WP248 Přiřazování, slučování, kombinování	WP248 Zranitelné osoby	WP248 Inovativní užití	WP248 Bránění v užívání	Rizikové zpracování	Σ kritičnosti (hodnota)
Ne	Ne	Ne	Ne	Ano	3

Zdroj: vlastní zpracování

V rámci provedení posouzení dopadu rizik na ochranu osobních údajů - PIA byly k danému zpracování, s ohledem na pravděpodobnost a četnost jejich vzniku, přiřazeny pouze relevantní hrozby a zranitelnosti dle Tabulky 3 – Kategorizace hodnocení hrozeb operací zpracování, které jej mohou poškodit. Zpracování evidence docházky je prováděno pouze elektronicky, tudíž jsou z tohoto hodnocení vyjmuty kategorie Katalogu hrozeb „PD“ – Papírové dokumenty a „PP“ – Kanály přenosu papíru, ke kterým je přiřazena nula. Ostatní kategorie hrozeb a zranitelností jsou ohodnoceny následujícím způsobem:

Tabulka 9 – Hodnocení rizika potenciálně rizikového zpracování dle Katalogu hrozeb

HW 01	HW 02	HW 03	HW 04	HW 05	HW 06	HW 07	HW 08	HW 09	HW 10	HW 11	SW 01	SW 02	SW 03	SW 04	SW 05	SW 06	SW 07	SW 08	SW 09	SW 10	SW 11	CH 01	CH 02	CH 03	CH 04	CH 05
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1

HU 02	HU 03	HU 04	HU 05	HU 06	HU 07	HU 08	PD 01	PD 02	PD 03	PD 04	PD 05	PD 06	PP 01	PP 02	PP 03	PP 04	PP 05	PP 06	∑ hrozeb
1	1	1	1	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	41

Zdroj: vlastní zpracování

Následně je určena úroveň výsledného rizika daného zpracování, která je dána součinem:

Míra rizika = Kritičnost zpracování x Míra hrozby

Účel zpracování osobních údajů: Evidence docházky

- Kritičnost zpracování: 3 (dle kritéria obecného posouzení úrovně rizika)
- Způsob uložení: v elektronické podobě**,** míra hrozby daného zpracování**:** 41
- Míra rizika: 123

Hodnota rizika byla vypočtena na 123 (Vysoké riziko). Toto vysoké riziko je tedy podle metodiky určeno k redukci pomocí opatření.

Na základě takového posouzení bylo zjišteno největší riziko vyplývající z nedostatečného fyzického zabezpečení systému obsahujícího uložené údaje o docházce – HW06 (úroveň hrozby stupeň 3, což znamená, že hrozba je velmi pravděpodobná až víceméně jistá, a její předpokládaná realizace je častější než jednou za měsíc), jež je popsáno v následující tabulce.

Tabulka 10 – Popis hrozeb a zranitelností rizikového zpracování dle Katalogu hrozeb

HW06	Hardware	Ztráta	Nezákonné přístupy k OÚ	Krádež laptopu z hotelového pokoje, krádež profesionálního mobilního telefonu kapsářem, získání vyhozeného úložného zařízení nebo hardwaru, ztráta elektronického úložného zařízení, atd.

Zdroj: vlastní zpracování

4.4.4 Návrh opatření

Pro redukci zjištěného rizika zpracování evidence docházky bylo ve spolupráci s bezpečnostním manažerem společnosti navrženo a přijato následující opatření (dle Tabulky č. 6 se jedná o opatření technického typu: TE05).

Tabulka 11 – Návrh opatření pro vzorové zpracování

Využití kryptografických prostředků pro ochranu dat	
ID zpracování	ZP04 – evidence docházky
Odpovědnost za zavedení	Bezpečnostní manažer Taylor McCoy, s.r.o.
Typ opatření	Technické
Souvislost s jinými opatřeními	Není
Doporučený termín realizace	Duben 2018

Zdroj: vlastní zpracování

Vzhledem ke skutečnosti, že data předmětného zpracování se vyskytují na mobilní stanici, bylo vhodné nasadit šifrování dat této stanice. Na stanici je použit operační systém Microsoft Windows, takže bylo možné využít vestavěnou technologii pro šifrování. První variantou byla technologie BitLocker. Touto metodou je možné šifrovat jak celé disky, tak případně přenosná média.

Další možností bylo využití EFS (Encrypted File System), což je funkce NTFS souborových systémů. Toto šifrování bylo možné nastavit na úrovni jednotlivých adresářů nebo souborů na disku. Pro zašifrování byl využit klíč, který je přítomný v uživatelském certifikátu.

Pro tuto mobilní stanici bylo šifrování celých disků pomocí technologie BitLocker z hlediska uživatelského komfortu vhodnější a poskytlo tak nejlepší zabezpečení pro případ fyzické krádeže.

5 Výsledky a diskuse

Hlavní cíle diplomové práce a samotné metodiky hodnocení rizik byly formulovány v době, kdy přes všeobecnou znalost požadavků Obecného nařízení pro ochranu osobních údajů nebylo zcela zřejmé, jaký bude způsob naplňování těchto požadavků. Díky minimálním omezením ze strany regulačních orgánů byl při návrhu metodiky velký prostor pro kreativní přístup. S ohledem na charakter společnosti Taylor McCoy, s.r.o. byl cíl práce dosažen novým využitím existujících a uznávaných standardů doplněných o vlastní postupy a poznatky. Díky tomu by výsledná metodika měla umožňovat plnění požadavků GDPR s přiměřeným úsilím a náklady, a zároveň demonstrovat své fungování založené na obecně uznávaných postupech. Díky spolupráci se společností Taylor McCoy bylo možné funkčnost metodiky ověřit na několika praktických realizovaných projektech. Z pozitivní zpětné vazby z analýz podle této metodiky lze usuzovat, že metodika je přijímána společností jako funkční.

V průběhu zpracování se ukázal jako nejvíce problematický návrh hodnocení osobních údajů. Úkol objektivně ohodnotit osobní údaje fyzických osob je svým způsobem netradiční v pojetí řízení rizik, neboť běžně používané metodiky počítají se schopností stanovit hodnotu aktiv z informací přímo dostupných dané společnosti. Hodnocení rizik spojených se zpracováním osobních údajů nicméně předpokládá stanovení hodnoty informačních aktiv bez přímého zapojení dotčených subjektů údajů, přičemž hodnota těchto aktiv se může zcela zásadně lišit v závislosti na subjektivním vnímání jednotlivými osobami. Řízení rizik je navíc v tomto případě prováděno nikoliv v zájmu společnosti, ale v zájmu jednotlivých fyzických osob. S tímto zásadním problémem se do okamžiku dokončení této diplomové práce obtížně potýká většina státních i komerčních organizací. Postup zvolený na začátku zpracování diplomové práce se ukázal svým způsobem šťastný, protože do okamžiku jejího dokončení nebyly k dispozici dříve očekávaná vodítka a metodické pokyny ze strany odpovědných orgánů, a to i přes blížící se termín nabytí účinnosti GDPR.

Při praktickém ověřování metodiky byla tato zařazena do celkové koncepce GDPR projektů realizovaných společností Taylor McCoy. Tyto projekty zahrnovaly fáze stanovení rozsahu GDPR ve společnosti, provedení srovnávací analýzy s požadavky GDPR a vytvoření Registru zpracování osobních údajů. Průběžné výstupy z diplomové práce byly využity v těchto projektech již pro fázi vytvoření Registru zpracování a především následného ohodnocení rizikovosti zpracování a provedení analýzy rizik. Hlavním cílem, ke kterému se

každá společnost snaží co nejrychleji dostat, je přehled opatření, která musí realizovat. Jako součást diplomové práce byl navržen postup výběru opatření pro pokrytí zjištěných rizik zpracování osobních údajů. Postup návrhu opatření byl zvolen tak, aby byla prioritizována opatření s krátkou dobou implementace a pokrývající co největší množství zpracování osobních údajů a s nimi spojená rizika, a tím bylo dosaženo co nejvyšší účinnosti v co nejkratší době. Časové hledisko navrhovaných opatření se ukázalo jako velmi významné s ohledem na ubývající čas k jejich implementaci.

V závěru zpracování diplomové práce byl proveden pokus o srovnání této vypracované metodiky s jinými zvěřejněnými metodikami tohoto typu. Při srovnávání metodik bylo zjištěno, že vzhledem k volnosti pravidel pro tvorbu této metodiky jsou veřejně dostupné metodiky natolik vzájemně rozdílné, že nelze provést žádné srovnání se smysluplným závěrem a lze očekávat, že kvalitu výstupů z těchto metodik prověří až výkladová praxe Úřadu na ochranu osobních údajů a soudů.

Vyjádření společnosti k vytvořené metodice:

„Z pohledu společnosti Taylor McCoy je pro nás předložená vypracovaná metodika velice užitečná, jelikož je klíčovou komponentou pro vyřešení souladu s požadavky GDPR, jak pro naši společnost, tak pro naše klienty, kterým poskytujeme poradenství v oblasti ochrany informací, jež zahrnuje i oblast ochrany osobních údajů. Po diskusi s autorkou metodiky bylo dohodnuto její následné využívání jak pro naši interní potřebu, tak pro naše zákaznické projekty. Vzhledem k charakteru GDPR stojícího mimo jiné na principech řízení rizik, je pro nás správná a funkční metodika nezbytným předpokladem pro úspěšnou realizaci projektů. Vytvořená metodika je na jedné straně srozumitelná pro široký okruh typově zcela odlišných organizací a jejich vedoucích zaměstnanců, a současně umožňuje integraci s metodikami pro systémy řízení bezpečnosti informací, ať již existujících nebo nově vytvářených. Využití této metodiky nám pravděpodobně usnadní situaci v okamžiku, kdy většina podobných společností tápe, jak problematiku řízení rizik pro účely Posouzení vlivu na ochranu osobních údajů uchopit.“

6 Závěr

Ochrana soukromí je ústavně chráněnou hodnotou a v současné době se díky vytěžování dat a jejich zvyšujícímu se komerčnímu užití a sdílení osobních údajů, jedná o jednu z priorit. Ochrana soukromí se skládá z několika částí a aspektů a nedílnou součástí je řízení rizik osobních údajů. S nástupem digitální doby, kdy se z dat stala surovina, jež je základem nejednoho byznysu, vzrostla potřeba zdokonalit systém zavádějící řád do nakládání s citlivými daty a chránit soukromí fyzických osob. Obecné nařízení o ochraně osobních údajů (GDPR) je novou a do značné míry revoluční legislativou EU, která podstatnou měrou zvýší ochranu osobních údajů občanů. V souvislosti se zaváděním GDPR je zapotřebí do systému řízení rizik promítnout nové požadavky hodnocení rizik působících na osobní údaje fyzických osob. Cílem vytvořené metodiky hodnocení rizik pro Posouzení vlivu na ochranu osobních údajů je odhalit rizika a navrhnout postup výběru účinných a efektivních opatření k minimalizaci potenciálních škod hrozících informačním aktivům v podobě osobních údajů.

S ohledem na předpokládaný způsob využívání a minimální omezení ze strany regulačních orgánů byla vytvořena metodika hodnocení rizik tak, aby umožňovala plnění požadavků GDPR a zároveň byla srozumitelná pro různé typy a velikosti společností. Prvním krokem v rámci procesu hodnocení rizik osobních údajů je stanovení rozsahu GDPR pro společnost, v němž jsou vymezeny jednotlivé oblasti, ve kterých dochází ke zpracování osobních údajů. Následně je sestaven Registr zpracování, jenž poskytne komplexní přehled o každém jednotlivém zpracování osobních údajů z hlediska popisu jednotlivých požadavků GDPR. Registr zpracování je vyplňován formou rozhovorů s pracovníky společnosti, kteří jsou odpovědní za procesy, ve kterých probíhají daná zpracování osobních údajů.

V dalším kroku je potřeba provést identifikaci a hodnocení jednotlivých aktiv (v tomto případě osobních údajů) formou prvotního posouzení rizikovosti zpracování osobních údajů. Při návrhu tohoto kroku se jako nejvíce problematické ukázalo ohodnocení osobních údajů, jelikož lze jen velmi obtížně stanovit hodnotu aktiv (osobních údajů), neboť tato hodnota může být pro jednotlivé fyzické osoby zásadně rozdílná a nelze ji jednoduchým způsobem objektivizovat. Pro tyto účely ohodnocení aktiv bylo proto využito kritérií obecného posouzení úrovně rizika dle pracovní skupiny WP248, která ve svém stanovení kritičnosti jednotlivých zpracování obsahují míru dopadu daného zpracování na fyzické osoby, a tedy odvozeně i obecnou představu o hodnotě těchto aktiv.

Po identifikaci a ohodnocení aktiv je dalším krokem provedení posouzení dopadů rizik na ochranu osobních údajů (tímto je představována analýza rizik pro oblast osobních údajů), což zahrnuje identifikaci hrozeb a zranitelností ve spojitosti s osobními údaji fyzických osob a rovněž posouzení pravděpodobnosti a dopadů těchto hrozeb na osobní údaje. Na základě výsledných hodnot aktiv, hrozeb a zranitelností je zjištěna míra rizika jednotlivých zpracování osobních údajů. Cílem vytvořené analýzy rizik je odhalit rizika, určit jejich výši a následně navrhnout účinná opatření k eliminaci potenciálních škod, jež by v případě realizace hrozby mohly ohrozit osobní údaje fyzických osob.

Dílčím cílem diplomové práce bylo navržení postupu výběru opatření pro pokrytí zjištěných rizik zpracování osobních údajů. V rámci tohoto kroku byla zjištěna existence několika opatření, jež mají plošnou působnost a tato opatření byla rozdělena do dvou kategorií. Prvním typem jsou opatření systémová, která působí nejen na všechny typy zpracování, ale zároveň na všechny hrozby. K těmto systémovým opatřením patří stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat a provedení kategorizace a ohodnocení zpracování osobních údajů. Druhým typem jsou opatření s vysokou účinností, jež sice neovliňují všechny hrozby, ale i tak jich ovlivňují větší počet. K těmto patří například stanovení pravidel pro ochranu fyzických médií, stanovení postupů a odpovědností ICT provozu či dodržování právních a smluvních požadavků.

Vytvořená metodika byla představena vedení společnosti Taylor McCoy, s.r.o. a z pozitivní zpětné vazby z analýz podle této metodiky lze usuzovat, že metodika je přijímána společností jako funkční. Výsledná metodika umožňuje plnění požadavků GDPR s přiměřeným úsilím a náklady, a zároveň demonstruje své fungování založené na obecně uznávaných postupech.

7 Seznam literatury

(1) ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(2) ČSN ISO/IEC 29100. *Informační technologie - Bezpečnostní techniky – Rámec soukromí.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

(3) Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

(4) MERNA, Tony a F- Al Thani FAISAL. *Risk management*. Brno: Computer Press, 2007. ISBN 978-80-251-1547-3.

(5) TICHÝ, Milík. *Ovládání rizika: analýza a management*. Vyd. 1. Praha: C.H. Beck, 2006, 396 s. ISBN 80-7179-415-5.

(6) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. ISBN 978-80-247-4644-9.

(7) HNILICA, Jiří a Jiří FOTR. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování*. 1. vyd. Praha: Grada, 2009, 262 s. Expert (Grada). ISBN 978-80-247-2560-4.

(8) ZUZÁK, Roman a Martina KÖNIGOVÁ. *Krizové řízení podniku*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2009, 253 s. ISBN 978-80-247-3156-8.

(9) ŘEHÁK, David. *Úvod do problematiky řízení rizik* [online]. [cit. 2017-10-25]. Dostupné z: http://www.researchgate.net/profile/David_Rehak/publication/261437852_vod_do_problematiky_zen_rizik/links/54cfa1280cf298d65664cee0.pdf.

(10) GUBALOVÁ, Karin. *Ako na riadenie informačnej bezpečnosti: Data Security Management.* Praha: TATE International, s.r.o., únor 2008, ISSN 1211-8737.

(11) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualiz. a rozš. vyd. Praha: Grada Publishing, 2006, 296 s. ISBN 80-247-1667-4.

(12) Zákon o ochraně osobních údajů a o změně některých zákonů (Zákon č. 101/2000 Sb.) [online]. [cit. 2018-01-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101

(13) Article 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk“ for the purposes on Regulation 2016/679*. Brusel, Belgie: Working Party 29, 2016.

(14) NULÍČEK, Michal a kol., *GDPR – obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.

(15) One Trust. *The Ultimate PIA and DPIA Handbook for Privacy Professionals*. London: One Trust, 2017.

(16) GRAHAM, Christopher. *Conducting privacy impact assessments, code of practise.* Information Commissioner´s Office, 2014.

(17) Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

(18) JANIŠOVÁ, Pavlína. *Proces řízení rizik.* Praha, 2016. Bakalářská práce (Bc.). Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, katedra řízení, 2016-05-20. 67 s.

(19) Taylor McCoy, s.r.o. *Směrnice pro nakládání s osobními údaji*. 2015. Praha

(20) ISO/IEC 29134. *Information Technology – Security Techniques – Guidlines For Privacy Impact Assessment*. London: British Standards Institutions, 2017.

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

(22) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(23) ISO/IEC 29151. *Information technology – Security techniques – Code of practise for personally identifiable information protection.* Geneva: ISO copyright office, 2017.

8 Přílohy

Seznam příloh

Příloha č. 1 – Seznam otázek pokládaných bezpečnostnímu manažerovi a bezpečnostnímu správci společnosti

Příloha č. 2 – Náležitosti Posouzení vlivu na ochranu osobních údajů

Příloha č. 3 – Dopad požadavků DPIA na metodiku hodnocení rizik

Příloha č. 4 – Katalog hrozeb

Příloha č. 5 – Registr zpracování

Příloha č. 1 – Seznam otázek pokládaných bezpečnostnímu manažerovi a bezpečnostnímu správci společnosti

1. Jaké jsou činnosti Vaší společnosti a jaká je její organizační struktura v souvislosti se zpracováním osobních údajů?
2. Jakým způsobem je ve Vaší společnosti zajišťováno řízení rizik bezpečnosti informací?
3. Konají se ve Vaší společnosti pravidelná školení zabývající se aktualizací rizik či interními předpisy pro ochranu informací/osobních údajů?
4. Pořádáte ve Vaší společnosti nějaká mimořádná školení jako reakci na vznik bezpečnostního incidentu nebo jiné mimořádné události?
5. Jak je ve Vaší společnosti členěna dokumentační základna interních předpisů?
6. Jakým způsobem máte ve společnosti zajištěn proces řízení rizik?
7. Řídí se Vaše společnost nějakými pravidly ochrany osobních údajů? Existuje ve společnosti nějaká směrnice pro nakládání s osobními údaji?
8. Máte ve společnosti stanovenou odpovědnou osobu pro oblast ochrany osobních údajů? Pokud ano, jaké je její organizační zařazení a její pracovní náplň?
9. Máte vytvořenou evidenci jednotlivých procesů a zpracování osobních údajů?
10. S jakými typy a jakým rozsahem osobních údajů pracujete?
11. Máte externího zpracovatele osobních údajů?

Příloha č. 2 – Náležitosti Posouzení vlivu na ochranu osobních údajů

a) Je poskytován systematický popis zamýšlených operací zpracování (čl. 35 odst. 7 písm. A Nařízení GDPR (3)):
   - povaha, rozsah, kontext a účely zpracování jsou zohledněny (bod 90 odůvodnění),
   - osobní údaje, subjekty údajů a období, v rámci kterého budou osobní údaje uloženy, jsou zohledněny,
   - je poskytnut funkční popis operace zpracování,
   - jsou identifikována aktiva, kterých se týkají osobní údaje (HW, SW, sítě, lidé, paper transmission channels),
   - dodržování schválených kodexů chování (čl. 35 odst. 8).

b) Posouzení nezbytnosti a přiměřenost zpracování (čl. 35 odst. 7 písm. B Nařízení GDPR (3)):
   - Jsou stanovena opatření, jež mají být v souladu s Nařízením (čl. 35 odst. 7 písm D a bod 90 odůvodnění), s ohledem na:
     - Opatření přispívající k proporcionalitě a nezbytnosti zpracování na základě:
       - výslovně vyjádřeného a legitimního účelu zpracování – „účelové omezení“ (čl. 5 odst. 1 písm. B),
       - zákonnosti zpracování (čl. 6),
       - přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány – „minimalizace údajů“ (čl. 5 odst. 1 písm. C),
       - omezená doba uložení osobních údajů – po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány – „omezení uložení“ (čl. 5 odst. 1 písm E).
     - Opatření přispívající k právům subjektů údajů:
       - informace poskytnuté subjektu údajů (čl. 12, 13 a 14),
       - právo na přístup k osobním údajům a právo na přenositelnost údajů (čl. 15 a 20),
       - právo na opravu, výmaz, námitku, omezení zpracování (čl. 16 až 19 a 20),

- zpracovatel (čl. 28),
- předávání osobních údajů do třetích zemí nebo mezinárodním organizacím (kapitola V),
- předchozí konzultace (čl. 26).

c) Rizika pro práva a svobody subjektů údajů (čl. 35 odst. 7 písm C Nařízení GDPR (3)):
   - původ, povaha, zvláštnost a závažnost rizik z pohledu subjektů údajů (viz bod 84 odůvodnění),
     - zdroje rizika jsou zohledněny (bod 90 odůvodnění),
     - potenciální dopady na práva a svobody subjektů údajů jsou zjištěny v případě neoprávněného přístupu, nežádoucích změn a vymizení údajů,
     - jsou identifikovány nežádoucí úpravy, zmizení údajů a hrozby, které by mohly vést k nelegitimní přístupnosti,
     - je posouzena pravděpodobnost a závažnost rizik pro práva a svobody subjektů údajů (bod 90 odůvodnění),
   - jsou stanovena plánovaná opatření k řešení těchto rizik (čl. 35 odst. 7 písm D a bod 90 odůvodnění).

d) Podílejí se zainteresované strany, především:
   - Je požadováno poradenství pověřence pro ochranu osobních údajů, tzv. DPO (čl. 35 odst. 2),
   - Jsou požadovány názory subjektů ůdajů nebo jejich zástupců (čl. 35 odst. 9).

Příloha č. 3 – Dopad požadavků DPIA na metodiku hodnocení rizik

Tabulka 12 - Dopad požadavků DPIA na metodiku hodnocení rizik

Náležitosti DPIA	Požadavek	Význam pro metodiku	Odkaz na kapitolu metodiky
Je poskytován systematický popis zamýšlených operací zpracování (čl. 35 odst. 7 písm. A)	povaha, rozsah, kontext a účely zpracování jsou zohledněny,	Tyto atributy zpracování by měly být zaznamenány v jednotném Registru zpracování a popsány samostatnou kapitolou DPIA (např. Účel a rozsah zpracování). Jednotlivé atributy pak ovlivňují výši rizik.	Registr zpracování v Příloze č. 5
	osobní údaje, subjekty údajů a období, v rámci kterého budou osobní údaje uloženy, jsou zohledněny,	Tyto atributy zpracování by měly být zaznamenány v jednotném Registru zpracování a popsány samostatnou kapitolou DPIA (např. Účel a rozsah zpracování). Jednotlivé atributy pak ovlivňují výši rizik.	Registr zpracování v Příloze č. 5
	je poskytnut funkční popis operace zpracování,	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.
	jsou identifikována aktiva, kterých se týkají osobní údaje,	Identifikace aktiv je identifikace kategorií osobních údajů pro jednotlivá zpracování, přičemž za základní aktivum pro účely metodiky DPIA se považuje každé dílčí zpracování a jemu příslušející atributy. Identifikovaná aktiva jsou zachycena v Registru zpracování.	Viz 4.3.4.1
	dodržování schválených kodexů chování.	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.
Posouzení nezbytnosti a přiměřenosti	výslovné vyjádření a legitimita účelu	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.

Náležitosti DPIA	Požadavek	Význam pro metodiku	Odkaz na kapitolu metodiky
zpracování (čl. 35 odst. 7 písm. B): **Jsou stanovena opatření, jež mají být v souladu s Nařízením (čl. 35 odst. 7 písm D a bod 90 odůvodnění), s ohledem na:** **a) Opatření přispívající k proporcionalitě a nezbytnosti zpracování na základě:**	zpracování – „účelové omezení“,		
	zákonnosti zpracování,	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.
	přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány – „minimalizace údajů“,	Tyto atributy zpracování by měly být zaznamenány v jednotném Registru zpracování. Rozsah zpracování má přímý dopad na výši rizik.	Registr zpracování v Příloze č. 5
	omezená doba uložení osobních údajů – po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány – „omezení uložení“.	Tyto atributy zpracování by měly být zaznamenány v jednotném Registru zpracování. Doba uložení má přímý dopad na výši rizik.	Registr zpracování v Příloze č. 5
Opatření přispívající k právům subjektů údajů:	informace poskytnuté subjektu údajů,	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.
	právo na přístup k osobním údajům a právo na přenositelnost údajů,	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.
	právo na opravu, výmaz, námitku, omezení zpracování,	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.
	zpracovatel,	Využití externího zpracovatele pro zpracování by mělo být zaznamenáno v jednotném Registru zpracování. Vazba na externího zpracovatele má dopad na výši rizik.	Registr zpracování v Příloze č. 5
	předávání osobních údajů do třetích zemí nebo mezinárodním organizacím,	Předávání osobních údajů do třetích zemí nebo mezinárodním organizacím by mělo být zaznamenáno v jednotném Registru zpracování. Předávání má dopad na výši rizik.	Registr zpracování v Příloze č. 5
	předchozí konzultace.	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.

Náležitosti DPIA	Požadavek	Význam pro metodiku	Odkaz na kapitolu metodiky
		Předchozí konzultace je následný krok po hodnocení rizik a přijetí opatření, pokud se nepodaří riziko redukovat na akceptovatelnou úroveň.	
Rizika pro práva a svobody subjektů údajů (čl. 35 odst. 7 písm C): **a) Původ, povaha, zvláštnost a závažnost rizik z pohledu subjektů údajů (viz bod 84 odůvodnění)**	zdroje rizika jsou zohledněny,	Pro zohlednění zdroje rizika by měla být vypracována samostatná kapitola Posouzení dopadů rizik na ochranu soukromí – PIA.	Viz 4.3.5
	potenciální dopady na práva a svobody subjektů údajů jsou zjištěny v případě neoprávněného přístupu, nežádoucích změn a vymizení údajů,	Pro zohlednění dopadů by měla být vypracována samostatná kapitola Posouzení dopadů rizik na ochranu soukromí – PIA.	Viz 4.3.5
	jsou identifikovány nežádoucí úpravy, zmizení údajů a hrozby, které by mohly vést k nelegitimní přístupnosti,	Pro zohlednění hrozeb pro dostupnost, důvěrnost a integritu údajů by měla být vypracována samostatná kapitola Posouzení dopadů rizik na ochranu soukromí – PIA.	Viz 4.3.5
	je posouzena pravděpodobnost a závažnost rizik pro práva a svobody subjektů údajů.	Pro posouzení závažnosti rizik by měla být vypracována samostatná kapitola posouzení dopadů rizik na ochranu soukromí – PIA.	Viz 4.3.5
Jsou stanovena plánovaná opatření k řešení těchto rizik (čl. 35 odst. 7 písm D a bod 90 odůvodnění).	jsou stanovena plánovaná opatření k řešení těchto rizik.	Pro stanovení plánovaných opatření k řešení rizik by měla být vypracována samostatná kapitola posouzení dopadů rizik na ochranu soukromí – PIA.	Viz 4.3.6
Podílejí se zainteresované strany, především:	je požadováno poradenství pověřence pro	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.

Náležitosti DPIA	Požadavek	Význam pro metodiku	Odkaz na kapitolu metodiky
	ochranu osobních údajů,		
	jsou požadovány názory subjektů údajů nebo jejich zástupců.	Požadavek nemá dopad na metodiku hodnocení rizik.	Není relevantní.

Zdroj: vlastní zpracování dle (13)

Příloha č. 4 – Katalog hrozeb

Následující katalog hrozeb je využíván při posuzování účinků hrozeb vůči aktivům (osobním údajům) a je platný pro všechny typy a velikosti organizací, včetně veřejných i soukromých společností, vládních subjektů a neziskových organizací.

ID hrozby	Podpůrná aktiva	Akce	Riziko s dopadem na soukromí	Příklady hrozeb
HW01	Hardware	Abnormální/neobvyklé použití	Zmizení osobních údajů (dále jen OÚ)	Skladování/uložení osobních souborů, osobní užití, atd.
HW02	Hardware	Abnormální/neobvyklé použití	Nezákonné přístupy k OÚ	Použití USB flash disků nebo disků, které nejsou vhodné pro citlivost informací, Použití nebo přeprava tajného/citlivého hardware pro osobní účely, atd.
HW03	Hardware	Poškození	Zmizení OÚ	Záplavy, požár, vandalismus, poškození přirozeným opotřebením, poškození paměťového zařízení, atd.
HW04	Hardware	Špionáž	Nezákonné přístupy k OÚ	Sledování člověka na obrazovce bez jeho vědomí, focení obrazovky, geolokace hardwaru, dálková detekce elektromagnetických signálů, atd.
HW05	Hardware	Ztráta	Zmizení OÚ	Krádež laptopu nebo mobilního telefonu, zbavení se/odstranění zařízení nebo hardwaru, atd.
HW06	Hardware	Ztráta	Nezákonné přístupy k OÚ	Krádež laptopu z hotelového pokoje, krádež profesionálního mobilního telefonu kapsářem, získání vyhozeného úložného zařízení nebo hardwaru, ztráta elektronického úložného zařízení, atd.
HW07	Hardware	Pozměnění	Zmizení OÚ	Přidání nekompatibilního hardwaru vedoucího k poruchám, vyjmutí komponentů nezbytných pro správné fungování systému, atd.
HW08	Hardware	Pozměnění	Nezákonné přístupy k OÚ	Sledování hardware-based keyloggerem, vyjmutí hardwarových komponentů, připojení zařízení (jako je USB flask disk) pro spuštění OS nebo načtení dat, atd.

ID hrozby	Podpůrná aktiva	Akce	Riziko s dopadem na soukromí	Příklady hrozeb
HW09	Hardware	Pozměnění	Nežádoucí změny v OÚ	Přidání nekompatibilního hardwaru vedoucího k poruchám, vyjmutí komponentů nezbytných pro správné fungování aplikace, atd.
HW10	Hardware	Přetížení/Zahlcení	Zmizení OÚ	Skladovací jednotka je plná, výpadek proudu, provozní přetížení kapacity, přehřátí, nadměrné teploty, atd.
HW11	Hardware	Ztráta pevného disku	Nezákonné přístupy k OÚ	Špatné smlouvy o likvidaci nebo údržbě mohou mít za následek neoprávněný přístup k OÚ, atd.
SW01	Software	Abnormální/neobvyklé použití	Zmizení OÚ	Vymazání dat, používání padělaného nebo kopírovaného softwaru, chyba operátora, která smaže data, atd.
SW02	Software	Abnormální/neobvyklé použití	Nezákonné přístupy k OÚ	Skenování obsahu, nelegitimní odkazování na data, zvyšování oprávnění, maskování stop použití, posílání spamů přes e-mail, zneužití síťových funkcí, atd.
SW03	Software	Abnormální/neobvyklé použití	Nežádoucí změny v OÚ	Nechtěné pozměnění dat v databázi, vymazání souborů potřebných pro správný chod softwaru, chyby operátora, které pozmění data, atd.
SW04	Software	Poškození	Zmizení OÚ	Vymazání běžících spustitelných nebo zdrojových kódů, logická bomba, atd.
SW05	Software	Špionáž	Nezákonné přístupy k OÚ	Skenování síťových adres a portů, shromažďování konfiguračních dat, analýza zdrojových kódů za účelem nalezení využitelných nedostatků/vad, testování jak databáze reagují na škodlivé dotazy, atd.
SW06	Software	Špionáž	Nezákonné přístupy k OÚ	Skenování síťových adres a portů, napadení zranitelností při poslechu, analýze, podávání zpráv nebo zprostředkovatelských portů a služeb.
SW07	Software	Ztráta	Zmizení OÚ	Neobnovení licence pro software používaný pro přístup k datům, atd.

ID hrozby	Podpůrná aktiva	Akce	Riziko s dopadem na soukromí	Příklady hrozeb
SW08	Software	Pozměnění	Zmizení OÚ	Chyby během updatů, konfigurace údržby, zavirování malware, nahrazení komponentů, atd.
SW09	Software	Pozměnění	Nezákonné přístupy k OÚ	Sledování software-based keyloggerem, zavirování malware, instalace dálkového/vzdáleného administračního nástroje, substituce komponentů, atd.
SW10	Software	Pozměnění	Nežádoucí změny v OÚ	Chyby během updatů, konfigurace údržby, zavirování malware, nahrazení komponentů, atd.
SW11	Software	Přetížení/Zahlcení	Zmizení OÚ	Překročení velikosti databáze, vkládání dat mimo normální rozsah hodnot, atd.
CH01	Počítačové kanály	Poškození	Zmizení OÚ	Odpojená kabeláž/elektrické rozvody, špatný příjem wi-fi, atd.
CH02	Počítačové kanály	Špionáž	Nezákonné přístupy k OÚ	Zastavení provozu/přenosu Ethernetu, získávání dat odeslaných přes wi-fi síť, atd.
CH03	Počítačové kanály	Ztráta	Zmizení OÚ	Krádež měděných kabelů, atd.
CH04	Počítačové kanály	Pozměnění	Nežádoucí změny v OÚ	"Man-in-the middle" nebo "man in the browser" útok pro pozměnění nebo přidání dat do síťové komunikace, opakovaný útok (znovuposlání zachycených dat), atd.
CH05	Počítačové kanály	Přetížení/Zahlcení	Zmizení OÚ	Zneužití rozsahu/šířky, neoprávněné stahování, ztráta internetového připojení, atd.
HU01	Jednotlivci	Abnormální/neobvyklé použití	Nezákonné přístupy k OÚ	Ovlivňování (phishing, sociální inženýrství, podplácení/korupce atd.), vyvíjení nátlaku (vydírání, psychické obtěžování atd.), atd.
HU02	Jednotlivci	Abnormální/neobvyklé použití	Nežádoucí změny v OÚ	Ovlivňování (drby/fámy, dezinformace atd.), atd.
HU03	Jednotlivci	Poškození	Zmizení OÚ	Pracovní nehoda/úraz, nemoc z povolání, jiné zranění a nemoci, smrt, neurologické, psychické nebo psychiatrické onemocnění, atd.
HU04	Jednotlivci	Špionáž	Nezákonné přístupy k OÚ	Neúmyslné vyzrazení informací během hovoru,

ID hrozby	Podpůrná aktiva	Akce	Riziko s dopadem na soukromí	Příklady hrozeb
				použití poslechových zařízení k odposlechu na setkáních, atd.
HU05	Jednotlivci	Ztráta	Zmizení OÚ	Přemístění/přiřazení, ukončení smlouvy nebo propuštění, převzetí celé nebo části organizace, atd.
HU06	Jednotlivci	Ztráta	Nezákonné přístupy k OÚ	Přetahování zaměstnanců, změny přiřazení, převzetí celé nebo části organizace, atd.
HU07	Jednotlivci	Přetížení/Zahlcení	Zmizení OÚ	Vysoký pracovní tok, stres nebo negativní změny pracovních podmínek, přiřazení zaměstnanců k úkolům mimo jejich schopnosti, špatné používání dovedností, atd.
HU08	Jednotlivci	Přetížení/Zahlcení	Nežádoucí změny v OÚ	Vysoký pracovní tok, stres nebo negativní změny pracovních podmínek, přiřazení zaměstnanců k úkolům mimo jejich schopnosti, špatné používání dovedností, atd.
PD01	Papírové dokumenty	Poškození	Zmizení OÚ	Stárnutí archivovaných dokumentů, spálení souborů během požáru, atd.
PD02	Papírové dokumenty	Špionáž	Nezákonné přístupy k OÚ	Čtení, Fotokopie/kopírování, fotografování, atd.
PD03	Papírové dokumenty	Ztráta	Zmizení OÚ	Krádež dokumentů, ztráta šanonů/desek během přesunu, likvidace, atd.
PD04	Papírové dokumenty	Ztráta	Nezákonné přístupy k OÚ	Krádež šanonů/desek z kanceláře, krádež pošty z poštovní schránky, znovuzískání vyřazených dokumentů, atd.
PD05	Papírové dokumenty	Pozměnění	Nežádoucí změny v OÚ	Změny údajů v šanonech/deskách, nahrazení originálu padělkem, atd.
PD06	Papírové dokumenty	Přetížení/Zahlcení	Zmizení OÚ	Postupné vymazávání v průběhu času, dobrovolné vymazávání částí dokumentu, atd.
PP01	Kanály přenosu papíru	Poškození	Zmizení OÚ	Ukončení pracovního postupu po reorganizaci, doručení pošty zastaveno stávkou/útokem, atd.
PP02	Kanály přenosu papíru	Špionáž	Nezákonné přístupy k OÚ	Čtení oběžníkových podpisových archů, reprodukce dokumentů při přepravě, atd.

ID hrozby	Podpůrná aktiva	Akce	Riziko s dopadem na soukromí	Příklady hrozeb
PP03	Kanály přenosu papíru	Ztráta	Zmizení OÚ	Eliminace procesu následujícího po reorganizaci, ztráta společnosti pro doručování dokumentů, atd.
PP04	Kanály přenosu papíru	Pozměnění	Zmizení OÚ	Změna v tom jak je pošta zasílána, reorganizace kanálů pro přenos papíru, změna v pracovních postupech, atd.
PP05	Kanály přenosu papíru	Pozměnění	Nežádoucí změny v OÚ	Změny ve zprávě/interním sdělení bez vědomí autora, změna z jedné podpisové knihy na jinou, posílání několika konfliktních dokumentů, atd.
PP06	Kanály přenosu papíru	Přetížení/Zahlcení	Zmizení OÚ	Přetížení poštovní a kurýrní služby, přetížení validačního procesu, atd.

Zdroj: vlastní zpracování dle (20)

Příloha č. 5 – Registr zpracování

IDENTIFIKACE ZPRACOVÁNÍ

Účel zpracování	Vztah ke zpracování	Využití externího zpracovatele pro zpracování	Garant účelu	Právní základ zpracování
Integrovaný systém řízení (IMS)				
Školení zaměstnanců na dokumentační systém	Správce	Ne	IMS	oprávněný zájem
Zprávy z provedených auditů	Správce	Ne	IMS	oprávněný zájem
Podklady pro provedení externího / certifiikačního auditu	Správce	Ne	IMS	oprávněný zájem
HR				
Evidence docházky	Správce	Ne	HR	plnění právní povinnosti
Mzdový systém	Správce	Ne	HR	plnění právní povinnosti
BOZP				
Preventivní zdravotní prohlídky	Správce	Ne	BOZP	plnění právní povinnosti
Účetnictví				
Zpracování mezd	Správce	Ne	FD	plnění právní povinnosti
Fakturace od fyzických osob	Správce	Ne	FD	plnění právní povinnosti
Cestovní příkazy	Správce	Ne	FD	plnění právní povinnosti
Údaje pro dokladování bankovních transakcí	Správce	Ne	FD	plnění smlouvy
Podklady pro výpočet daní	Správce	Ne	FD	plnění právní povinnosti
Vyúčtováná soukromého užívání firemních prostředků	Správce	Ne	FD	plnění právní povinnosti
Vyúčtování naturálních příjmů	Správce	Ne	FD	plnění smlouvy
Nákup				
Zpracování smluv	Správce	Ne	PUD	plnění právní povinnosti, oprávněný zájem

Kategorie subjektů	Kategorie osobních údajů	Zvláštní kategorie	Zdroj
Integrovaný systém řízení (IMS)			
zaměstnanci	jméno, příjmení, ID číslo zaměstnance, datum narození, podpis	Ne	subjekt OÚ
zaměstnanci	jméno, příjmení, podpis	Ne	subjekt OÚ
zaměstnanci	jméno, příjmení, podpis	Ne	subjekt OÚ
HR			
zaměstnanci / agenturní zaměstnanci	jméno, příjmení, ID číslo, přítomnost, odchody, nároky na dotované jídlo, nemoc, dárcovství krve, pohřeb osoby blízké, odchod k lékaři, dovolená, sick days, nároky na benefity	Ne	subjekt OÚ, nadřízený zaměstnanec
zaměstnanci	Jméno, Příjmení, rodné číslo, bydliště, pohlaví, datum narození, místo narození, číslo občanského průkazu, číslo pasu , rodinný stav, rodinní příslušníci, státní příslušnost, dosažené, vzdělání, národnost, fotografie, bankovní účet, odvody, soc a zdrav pojištění, zdravotní pojišťovna, výše mzdy, zdravotní stav, osobní číslo, druh pracovního poměru, datum nástupu, datum ukončení pracovního poměru, srážky ze mzdy (insolvence, exekuce)	Ne	subjekt OÚ
BOZP			
zaměstnanci	ID číslo, jméno, příjmení, datum narození, datum nástupu, pracovní zařazení, zdravotní omezení, pracovní režim	Ano	subjekt OÚ
Účetnictví			
zaměstnanci / studenti	ID číslo, jméno, příjmení, číslo oddělení, údaje o srážkách, náhrady	Ne	Helios
externisté / dodavatelé	jméno, příjmení, IČ, DIČ, adresa, číslo bankovního účtu	Ne	subjekt OÚ
zaměstnanci	ID zaměstnance, oddělení, jméno, příjmení, adresa	Ne	subjekt OÚ
zaměstnanci	ID zaměstnance, jméno, příjmení, číslo bankovního účtu, částka	Ne	Helios
zaměstnanci	jméno, příjmení, adresa, číslo ePKP, finanční údaje	Ne	HR, Axapta
zaměstnanci	ID zaměstnance, jméno, příjmení, oddělení, RZ vozidla, telefonní číslo	Ne	HR
zaměstnanci	ID zaměstnance, jméno, příjmení, číslo bankovního účtu, částka, forma naturálního příjmu	Ne	subjekt OÚ
Nákup			
statutární zástupci, OSVČ	jméno, příjmení, adresa, IČ, DIČ, podpis	Ne	subjekt OÚ, obchodní rejstřík

			Kritičnost (hodnota) zpracování			
Doba uchování	Informační systém	Název datasetu	WP248 Hodnocení nebo bodování Profilování a předpovídání	WP248 Autom. rozhodování s závažným (např. právním) dopadem	WP248 Systematické monitorování	WP248 Zvláštní a citlivé údaje
Integrovaný systém řízení (IMS)						
papír - do scanování, elektronicky neomezeně	fileserver	adresář IMS	Ne	Ne	Ne	Ne
neomezeně	n/a	n/a	Ne	Ne	Ne	Ne
neomezeně	fileserver	adresář IMS	Ne	Ne	Ne	Ne
HR						
neomezeně	PowerKey	n/a	Ano	Ano	Ano	Ne
podle legislativy	Helios	n/a	Ne	Ne	Ne	Ano
BOZP						
neomezeně	Riscon	n/a	Ne	Ne	Ne	Ano
Účetnictví						
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
10 let	Axapta	n/a	Ne	Ne	Ne	Ne
Nákup						
neomezeně	fileserver	disk K	Ne	Ne	Ne	Ne

Kritičnost (hodnota) zpracování							
WP248 Velký rozsah	WP248 Přiřazování, slučování, kombinování	WP248 Zranitelné osoby	WP248 Inovativní užití	WP248 Bránění v užívání	Rizikové zpracování	∑ kritičnosti (hodnota)	Hodnoceno
Integrovaný systém řízení (IMS)							
Ne	Ne	Ano	Ne	Ne	Ne	**1**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
HR							
Ne	Ne	Ne	Ne	Ne	Ano	**3**	**Ano**
Ne	Ne	Ano	Ne	Ne	Ano	**2**	**Ano**
BOZP							
Ne	Ne	Ne	Ne	Ne	Ne	**1**	**Ano**
Účetnictví							
Ne	Ne	Ano	Ne	Ne	Ne	**1**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
Ne	Ne	Ano	Ne	Ne	Ne	**1**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**
Nákup							
Ne	Ne	Ne	Ne	Ne	Ne	**0**	**Ano**

Identifikace a hodnocení hrozeb a zranitelností																												
Hardware											Software										Počítačové kanály							
HW 01	HW 02	HW 03	HW 04	HW 05	HW 06	HW 07	HW 08	HW 09	HW 10	HW 11	SW 01	SW 02	SW 03	SW 04	SW 05	SW 06	SW 07	SW 08	SW 09	SW 10	SW 11	CH 01	CH 02	CH 03	CH 04	CH 05	HU 01	H U0 2
Integrovaný systém řízení (IMS)																												
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
HR																												
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
BOZP																												
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
Účetnictví																												
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
Nákup																												
1	1	1	1	2	3	1	1	1	1	1	1	1	3	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1

Identifikace a hodnocení hrozeb a zranitelností																			
Jednotlivci						Papírové dokumenty						Kanály přenosu papíru							
HU 03	HU 04	HU 05	HU 06	HU 07	HU 08	PD 01	PD 02	PD 03	PD 04	PD 05	PD0 6	PP 01	PP 02	PP 03	PP 04	PP 05	PP 06	∑ hrozeb	Rizikovost
Integrovaný systém řízení (IMS)																			
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	55	55
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	24	0
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	56	0
HR																			
1	1	1	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	41	123
1	1	1	1	1	2	0	0	0	0	0	0	0	0	0	0	0	0	41	82
BOZP																			
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	55	55
Účetnictví																			
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	56	56
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	56	0
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	56	0
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	55	0
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	55	55
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	55	0
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	55	0
Nákup																			
1	1	1	1	1	2	1	1	3	2	1	1	1	1	1	1	1	1	57	0

Zdroj: vlastní zpracování