VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

HODNOCENÍ RIZIK V OCHRANĚ OSOBNÍCH ÚDAJŮ
RISK MANAGEMENT IN PERSONAL DATA PROTECTION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Anna Voskárová

VEDOUCÍ PRÁCE
SUPERVISOR
JUDr. MgA. Jakub Míšek, Ph.D.

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Anna Voskárová ***ID:*** 211326
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Hodnocení rizik v ochraně osobních údajů

POKYNY PRO VYPRACOVÁNÍ:

Právní úprava ochrany osobních údajů v podobě Obecného nařízení o ochraně osobních údajů (nařízení EU č. 2016/679, dále GDPR) je postavena na principu hodnocení významnosti rizik, které zpracování osobních údajů představuje pro práva a zájmy subjektů údajů. Bakalářská práce se na tento princip zaměří a představí jeho praktické důsledky. Pozornost bude věnována rovněž posouzení vlivu na ochranu osobních údajů ve smyslu čl. 35 GDPR. V teoretické části práce autor představí roli hodnocení rizik v kontextu ochrany osobních údajů a popíše vybrané metodiky hodnocení rizik. Praktická část bakalářské práce bude spočívat v naprogramování aplikace, která pomůže správcům osobních údajů k prvotní evaluaci závažnosti rizika chystaného zpracování.

DOPORUČENÁ LITERATURA:

[1] MÍŠEK, Jakub. Moderní regulatorní metody ochrany osobních údajů. 1. vyd. Brno: Masarykova univerzita, 2020, 279 s. ISBN 978-80-210-9736-0.

[2] ŠVOLÍK, Oliver. Řízení rizik v ochraně osobních údajů [online]. Brno, 2019 [cit. 2020-09-14]. Dostupné z: <https://is.muni.cz/th/jeyno/>. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Jakub Harašta.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: JUDr. MgA. Jakub Míšek, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

Abstrakt

Bakalárska práca sa zameriava na rozbor problematiky riadenia rizík v kontexte ochrany osobných údajov pri realizácií ich spracúvania. Na základe teoretických východísk, založených na vysvetlení relevantných častí Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov), je následne predstavený koncept metodiky pre posudzovanie rizík v ochrane osobných údajov. Práca sa taktiež snaží o výklad niektorých všeobecných pojmov, ktorých pochopenie je nevyhnutné pre špecifikovanie hlavnej problematiky, ako je napr. samotný pojem rizika a proces riadenia rizík. Praktickým výstupom bakalárskej práce je webová aplikácia umožňujúca stanovenie závažnosti rizika pre práva a slobody subjektov údajov v rámci procesu všeobecného posúdenia rizík činností spracúvania osobných údajov.

Kľúčové slová

osobné údaje, ochrana osobných údajov, spracúvanie osobných údajov, riadenie rizík, posúdenie rizík, všeobecné nariadenie o ochrane osobných údajov, ochrana práv a slobôd fyzických osôb

Abstract

The bachelor thesis focuses on the issue of the risk management in the context of personal data protection in the course of the implementation of their processing. Concerning the theoretical background, based on the explanation of relevant parts of 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/EC (General Data Protection Regulation), the own methodology for risk management in personal data protection is presented. The thesis also attempts at interpretation of some general expressions, understanding of which is indispensable for the specification of the main issue, such as a risk and the process of risk management itself. The practical output of this bachelor thesis is a web application providing the determination of the severity of the risk to the rights and freedoms of data subjects in the process of the general risk assessment for personal data processing operations.

Keywords

personal data, personal data protection, processing of personal data, risk management, assessment of the risk, General Data Protection Regulation, protection of fundamental rights and freedoms of natural persons

Bibliografická citácia

VOSKÁROVÁ, Anna. *Hodnocení rizik v ochraně osobních údajů*. Brno, 2021. Dostupné tiež z: https://www.vutbr.cz/studenti/zav-prace/detail/133532. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce JUDr. MgA. Jakub Míšek, Ph.D.

Prehlásenie autora o pôvodnosti diela

Meno a priezvisko študenta:	Anna Voskárová
VUT ID študenta:	211326
Typ práce:	Bakalárska práca
Akademický rok:	2020/21
Téma záverečnej práce:	Hodnocení rizik v ochraně osobních údajů

Prehlasujem, že som svoju záverečnú prácu vypracovala samostatne pod vedením vedúceho záverečnej práce a s použitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autorka uvedenej záverečnej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto záverečnej práce som neporušila autorská práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a som si plne vedomá následkov porušenia ustanovení § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovení časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ---------- ----------

podpis autorky

Poďakovanie

Rada by som vyjadrila poďakovanie vedúcemu bakalárskej práce pánovi JUDr. MgA. Jakubovi Míškovi, Ph.D. za odbornú pomoc a usmernenie pri písaní mojej práce, za cenné rady a poznatky, užitočné pripomienky, inšpiratívne nápady a predovšetkým za čas, ktorý mi pri príprave tejto záverečnej práce venoval.

Brno ---------- ----------

podpis autorky

Obsah

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

V dnešnej, modernej spoločnosti, kedy väčšina oblastí života každého človeka prebieha na pozadí čoraz intenzívnejšieho technického pokroku, sa stretávame s narastajúcou potrebou ochrany informácií, ktoré sú pre nás istým spôsobom cenné. Ide najmä o informácie, ktoré poskytujú iným ľuďom znalosť o našej osobe – hovoríme vtedy o „osobných údajoch“. Častokrát si ani neuvedomujeme, aké následky môže poskytnutie týchto údajov o našej osobe vyvolať a bez výraznejšieho zaváhania sme pre naplnenie našich potrieb a túžob ochotní tieto informácie o sebe poskytnúť komukoľvek inému.

So spracovaním našich osobných údajov sa v dnešnej dobe stretávame doslova na každom kroku. Či už sa jedná o nákupy prostredníctvom internetu, doručovanie tovaru prepravnou spoločnosťou, rezerváciu pobytovej dovolenky alebo zriadenie študentského preukazu pre bezplatné či zvýhodnené využívanie niektorých služieb. Vo všetkých týchto situáciách, a samozrejme aj v mnohých iných, poskytujeme údaje o našej osobe. Na druhej strane stojí ako príjemca našich údajov tzv. prevádzkovateľ[1], ktorý disponuje takto získanými údajmi a môže ich ďalej spracúvať pre naplnenie definovaného účelu.

Problematiku zákonného spracúvania osobných údajov v dnešnej dobe zavádza a bližšie rozoberá Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES[2], pre mnohých známe pod pojmom GDPR. Za jeden z hlavných prínosov Nariadenia možno považovať zmenu v podobe zavedenia zásady zodpovednosti prevádzkovateľa spracúvania a prístupu založenom na hodnotení rizík[3] vyplývajúcich z realizovaného spracúvania. Táto povinnosť je chápaná v zmysle nutnosti vykonávať za každých okolností všeobecné posudzovanie rizík, ktoré v dôsledku realizovania spracovateľskej operácie môžu nastať a spôsobiť tak neočakávaný a nepriaznivý priebeh spracúvania údajov.

Popísanú všeobecnú povinnosť ďalej rozširuje článok 35 Nariadenia, ktorý zavádza pre prevádzkovateľa spracúvania osobných údajov povinnosť vykonať posúdenie vplyvu na ochranu údajov, tzv. *Data Protection Impact Assessment* – skrátene *DPIA*. Tento

[1] V českom právnom prostredí je bežne používaný pojem „správca“ osobných údajov. Avšak pre zachovanie súladu použitej terminológie s jazykom tejto práce a pre zamedzenie vzniku problému v dôsledku nejasností prekladu je tento pojem v celom rozsahu práce nahradený pojmom „prevádzkovateľ“.

[2] Ďalej len Nariadenie.

[3] Záverečná práca nesie názov „hodnotenie rizík“, avšak za účelom zamedzenia vzniku terminologických nejasností medzi jednotlivými pojmami (samotný proces hodnotenia rizík pozostáva z identifikácie, analýzy a záverečného ohodnotenia rizika, viď kap. 1.2) bude v práci nahradené toto slovné spojenie jeho synonymickým, tiež bežne používaným vyjadrením „posúdenie rizík“.

proces je realizovaný v prípadoch, kedy všeobecné posúdenie rizík spracovania odhalí skutočnosť, že pri realizácií posudzovanej spracovateľskej činnosti hrozí vysoké riziko pre práva a slobody voči subjektom spracúvaných údajov. Podrobný popis problematiky realizácie jednotlivých krokov posúdenia *DPIA* je avšak už nad rámec tejto práce. Účelom práce je popísať proces všeobecného posúdenia rizík, ktoré je prevádzkovateľ povinný realizovať vždy a za každých okolností bez ohľadu na to, či bude následne potrebné vykonať aj komplexný proces posúdenia *DPIA*.

Cieľom tejto práce je priblížiť problematiku riadenia rizík vo všeobecnosti a na základe všeobecného prístupu následne vysvetliť a analyzovať priebeh fázy hodnotenia rizík v procese spracúvania osobných údajov, ktoré má vzhľadom k svojmu špecifickému zameraniu – ochrana práv a slobôd subjektov údajov – jedinečné kroky pre realizáciu. Hodnotenie týchto rizík prináša prevádzkovateľovi spracúvania osobných údajov obraz o tom, kde a aké riziká pri spracúvaní údajov môžu vzniknúť, na základe čoho môže následne prijať potrebné opatrenia pre minimalizovanie, v ideálnom prípade odstránenie týchto rizík s cieľom zabezpečiť tak súlad spracúvania osobných údajov s podmienkami vyplývajúcimi z článku 24 Nariadenia.

Teoretická časť popisuje problematiku procesu riadenia rizík spočiatku vo všeobecnosti a následne prináša jej popis v súvislosti s realizáciou procesu hodnotenia rizík v kontexte spracúvania osobných údajov tak, ako ju chápe aj Nariadenie. Dôraz je kladený najmä na fázu posúdenia hodnôt identifikovaných rizík a ich ošetrenia, resp. odstránenia či aspoň minimalizácie na požadovanú úroveň. Pre účely realizácie praktického výstupu v podobe webovej aplikácie umožňujúcej realizovať proces posúdenia rizík spracúvania osobných údajov, v ktorom sú hlavným chráneným záujmom práva a slobody subjektov spracúvaných údajov, bude v rámci práce predstavený návrh metodiky popisujúci jednotlivé kroky tohto procesu. Navrhnutá metodika bude vytvorená s prihliadnutím na postupy doporučené francúzskym dozorným úradom CNIL a na postupy v otázke hodnotenia rizík informačnej bezpečnosti definované medzinárodnou normou ISO 27005.

Praktická časť práce je venovaná príprave koncepčných materiálov k naprogramovaniu funkčnej webovej aplikácie a samotnému naprogramovaniu jej činnosti umožňujúcej vyhodnotiť celkovú úroveň závažnosti rizika posudzovanej spracovateľskej činnosti na základe súboru jedinečných charakteristík konkrétnej činnosti, ktoré prostredníctvom dotazníkového formulára špecifikuje sám užívateľ. Rozhodovací proces pre stanovenie celkovej závažnosti rizika posudzovaného spracúvania využíva princípy navrhnutej metodiky, avšak s tým rozdielom, že management informačnej bezpečnosti nie je implementovaný ako samostatná časť posúdenia z dôvodu komplexnosti a rozsiahlosti tohto

procesu, ale je priamo súčasťou všeobecného posúdenia závažnosti rizík so zameraním na možnosť vzniku nepriaznivého zásahu do práv a slobôd subjektov údajov. Implementácia procesu hodnotenia pravdepodobnosti rizika, v súvislosti s riadením informačnej bezpečnosti, ako samostatnej jednotky by bola z dôvodu náročnosti realizácie nad rámec činností potrebných k dosiahnutiu cieľov tejto záverečnej práce.

1 RIADENIE RIZÍK

O pôvode slova „*riziko*“ je diskutované v mnohých publikáciách. Tento výraz údajne pochádza z talianskeho slova *risico*, ktoré sa v priebehu 17. storočia začalo využívať primárne v súvislosti s lodnou plavbou, kedy vyjadrovalo hroziace nebezpečenstvo pre lode, ktorému sa bolo potrebné vyhnúť. Riziko bolo teda už v tomto období ľuďmi vnímané ako situácia „vystavenia sa nepriaznivým okolnostiam“ [1, s. 90].

Formálnejší popis významu slova riziko poskytuje norma ČSN ISO 27005:2013, ktorá riziko definuje ako „*účinok neistoty na dosiahnutie cieľov*“ [2, s. 10]. Vznik rizika je teda spojený s istou mierou neistoty, pri ktorej nie je možné jasne predpovedať, kedy a či vôbec riziková udalosť nastane. Takáto udalosť nastáva len s určitou pravdepodobnosťou a spôsobuje odchýlenie sa od očakávaného výsledku, vývoja či stavu. Ak sa riziko vo forme určitej neistoty vyskytne, môže mať pozitívny a/alebo negatívny dopad na dosiahnutie jedného či viacerých vytýčených cieľov. Nakoľko výskyt rizika nie je možné vopred jednoznačne predpoklad, je teda zrejmé, že miera rizika, ktorá popisuje jeho celkový dopad, bude určená tým, či vôbec môže nastať taká udalosť, ktorá by spôsobila odklon od očakávaného priebehu činnosti, a taktiež tým, čo by táto udalosť, v prípade jej realizácie, spôsobila.

1.1 Význam riadenia rizík

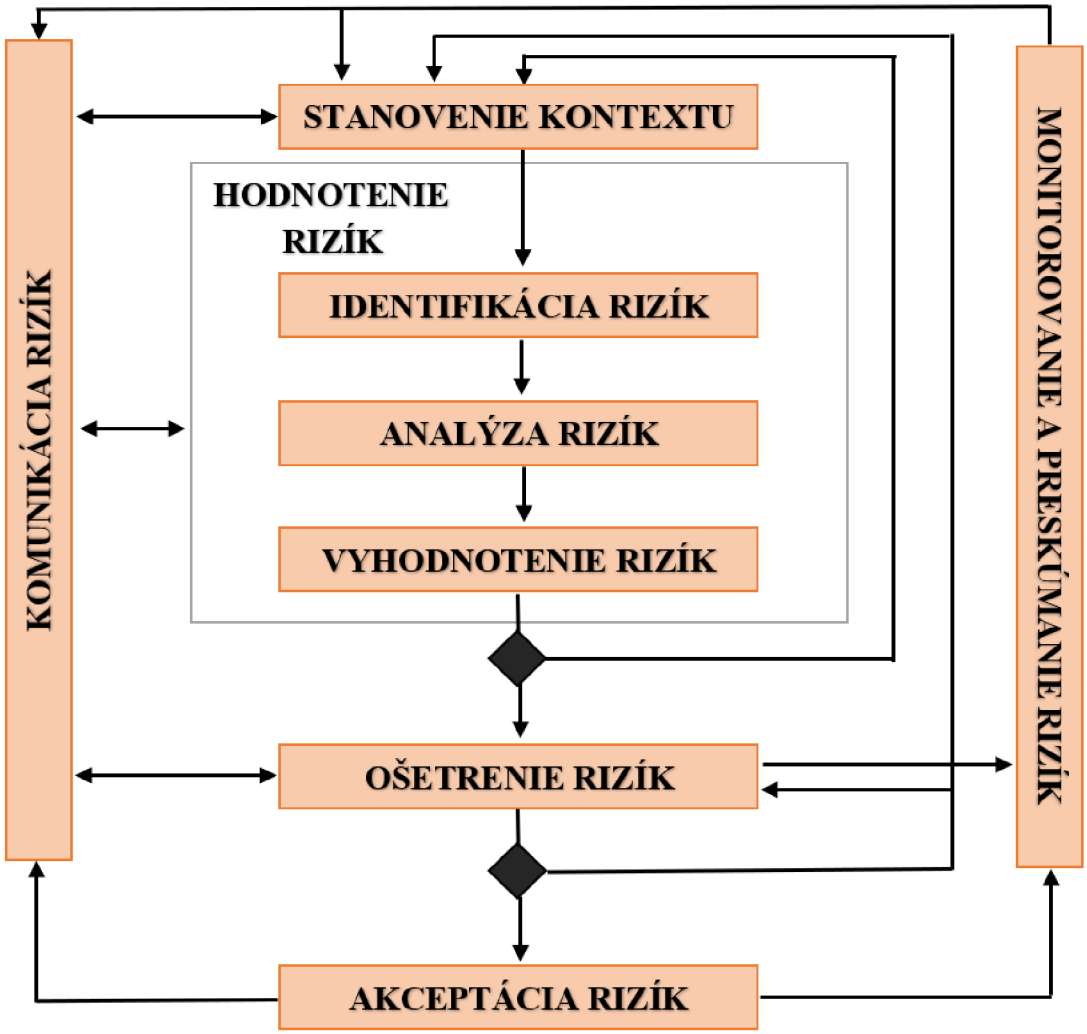
Rôzne organizácie pôsobiace v akomkoľvek odvetí súčasnej doby majú vytýčené svoje jedinečné ciele, ku ktorým sa snažia realizáciou vlastných činností dospieť. Každá takáto činnosť, ktorú organizácia počas svojho pôsobenia vykonáva, môže priniesť do plánovaného fungovania organizácie neočakávaný priebeh, čiže riziko. Počas pôsobenia musí teda organizácia čeliť mnohým neistotám, ktorých výskyt by mohol skomplikovať, prípadne úplne znemožniť dosahovanie očakávaného výsledku činností organizácie. Aby bolo možné predchádzať neočakávaným, neistým situáciám, je žiadúce, aby organizácia priebežne kontrolovala, zaisťovala a minimalizovala výskyt takýchto nežiadúcich udalostí. Kompletný proces zistení, kontroly, eliminácie a minimalizácie udalostí, ktoré môžu ovplyvňovať určitý subjekt, sa nazýva riadenie rizík [3].

Riadenie rizík predstavuje proces systematického vyhľadávania, posudzovania, hodnotenia a odstraňovania neistôt [4, s. 11]. Riadenie rizík by malo byť nepretržitým procesom, počas ktorého by mal byť stanovený kontext realizácie posudzovaných činností, identifikované a vyhodnotené riziká, nadefinovaný plán ošetrenia rizík a následne ošetrené riziká predstavujúce najzávažnejší dopad. „*Riadenie rizík analyzuje, čo sa môže stať*

a aké môžu byť prípadné dôsledky, pred rozhodnutím, čo a kedy by sa malo uskutočniť za účelom redukcie rizika na prijateľnú úroveň.“ [2, s. 12]

1.2 Proces riadenia rizík

Riadenie rizík, ako ho popisuje norma ČSN ISO 31000:2009, zahŕňa nasledujúce dielčie procesy: stanovenie kontextu, posudzovanie rizík a ošetrenie rizík [4, s. 11]. Po vykonaní týchto základných krokov je následne do procesu zavedené monitorovanie a preskúmanie rizík, komunikácia rizík a vo výsledku prípadná akceptácia rizík. Celý priebeh procesu, tak ako ho popisuje vyššie spomínaná norma, je zobrazený na obr. 1.1.



Obr. 1.1: Proces managementu rizík podľa normy ČSN ISO 31000:2009. [4]

Cieľový koncept metodiky, ktorý navrhuje praktická časť tejto práce (viď kap. 3), sa obmedzuje na dve najdôležitejšie časti, a to posúdenie rizík a ich následné ošetrenie. Tieto hlavné časti je možné ďalej rozdeliť na štyri fázy, ktorými sú identifikácia, analýza, hodnotenie a ošetrenie rizika. Podrobnejšie členenie a vzájomnú nadväznosť týchto fáz tiež zachytáva obr. 1.1.

Pre splnenie hlavnej náplne tejto práce je potrebné vysvetliť všeobecný postup pri riešení problematiky posudzovania rizík. V nasledujúcich kapitolách budú preto bližšie priblížené jeho jednotlivé fázy – identifikácia, analýza a celkové ohodnotenie rizika. Ďalej bude naznačené, akými spôsobmi môže organizácia následne pristúpiť k ošetrovaniu rizík identifikovaných a ohodnotených v procese ich posudzovania. Každá z týchto štyroch fáz zahŕňa dielčie podkroky, ktoré je nutné vykonať pre kompletné naplnenie podstaty procesu posúdenia rizík. Jednotlivé kroky sa však môžu na základe špecifikácie použitej metodiky mierne líšiť, a preto na všeobecnej úrovni popísané dopodrobna nebudú. Bližšie budú rozpracované v kap. 3 venovanej návrhu vlastnej metodiky pre posudzovanie rizík v kontexte ochrany osobných údajov.

1.2.1 Posudzovanie rizík

Posudzovanie rizík definuje norma ISO 31000:2009 ako „*celkový proces identifikácie rizika a jeho analýzu a hodnotenie*“ [4]. Prvá fáza, označená pojmom identifikácia rizík, má za cieľ zostaviť zoznam rizík, ktoré by mohli nejakým spôsobom ovplyvniť priebeh posudzovanej činnosti vykonávanej organizáciou. Počas tejto etapy je potrebné definovať všetky okolnosti týkajúce sa posudzovanej činnosti. Je potrebné identifikovať čo a akým spôsobom je zapojené do realizácie posudzovanie činnosti. Organizácia venuje preto pozornosť najmä aktívam, ktoré sa akýmkoľvek spôsobom podieľajú na realizácii danej činnosti. V kontexte spracúvania osobných údajov[4] je potrebné identifikovať tie riziká, ktoré sa v posudzovanom spracúvaní osobných údajov vyskytujú, a taktiež uvážiť, aké práva a slobody by mohli byť v dôsledku výskytu týchto rizík zasiahnuté.

V rámci analýzy rizík sa stanovuje dôležitosť identifikovaných rizík z hľadiska pravdepodobnosti ich výskytu a veľkosti dopadu na konkrétnu činnosť organizácie, ktorá je predmetom prebiehajúceho posudzovania rizík. Táto fáza je obvykle chápaná ako proces definovania hrozieb, pravdepodobnosti ich uskutočnenia a dopadu na aktíva, teda vymedzenie konkrétnych rizík a stanovenie ich závažnosti.

[4] Zaradeniu a významu realizácie rizík v kontexte spracovania osobných údajov je venovaná väčšia pozornosť v ďalších častiach tejto práce (viď kap 2.4).

K analýze rizík sa dá pristupovať pomocou dvoch základných metód. Kvantitatívne metódy sú založené na matematickom výpočte rizika z frekvencie výskytu hrozby a jej dopadu. Riziká sa oceňujú číselne v prípade pravdepodobnosti vzniku udalosti aj pri oceňovaní dopadu danej udalosti [1, s. 112]. Tieto metódy je možné využiť v prípade, kedy je možné potrebné hodnoty určiť z presných dát, z určitých zaznamenaných číselných hodnôt a kedy je možné dopad takto vzniknutých rizík vyčísliť, predovšetkým vo finančných čiastkach.

Spracovanie osobných údajov je ale proces, pri ktorom do procesu hodnotenia dopadu pre práva a slobody v dôsledku pôsobenia nepriaznivého rizika vstupuje aj istá miera subjektivity, a nie je preto možné vychádzať z presných, kvantitatívnych údajov. V takomto prípade je možné využiť metódy kvalitatívne, ktoré taktiež popisujú závažnosť dopadu a pravdepodobnosť, že táto udalosť nastane, ale výslednú úroveň určujú len na základe patričného kvalifikovaného odhadu. [1, s. 112]

Na analýzu rizík nadväzuje ohodnotenie rizík. V tejto fáze sa porovnávajú úrovne rizika so stanovenými kritériami prijateľnosti, resp. neprijateľnosti. Hovoríme o tzv. kritériách pre akceptáciu rizika. Prevádzkovateľ spracúvania osobných údajov určí úroveň rizika, ktorá je pre proces spracúvania ešte prijateľná a ktorú je schopný a ochotný akceptovať. Na tvorbu kritérií a následné ohodnotenie rizík na základe ich hodnoty voči týmto kritériám má vplyv množstvo faktorov. Na jednej strane musí prevádzkovateľ zohľadniť najmä dopad na práva a slobody subjektov údajov, no na strane druhej musí zvážiť aj vlastné ekonomické možnosti pre zavedenie nových opatrení a pre prípadné plánované zmeny z dlhodobého hľadiska.

1.2.2 Ošetrenie rizík

Pre kontext tejto práce je vhodné priblížiť aj fázu ošetrenia rizík, v ktorej prevádzkovateľ uskutočňujúci posudzovanie rizík takých činností spracúvania osobných údajov, ktoré sám realizuje, na základe vytvoreného plánu opatrení potrebných pre zmiernenie identifikovaných rizík, implementuje navrhnuté opatrenia. Nakoľko je celý proces riadenia rizík procesom neustálym a iteratívnym, podobným postupom sa voči nastoleným kritériám posudzuje úroveň reziduálneho rizika[5], a to buď bude možné akceptovať a pod hrozbou tohto rizika bude možné dané spracúvanie údajov po zavedení dostupných opatrení aj naďalej realizovať, alebo bude nutné spracúvanie zamietnuť, ak už nie je možné prijať dodatočné opatrenia potrebné pre zníženie hodnoty rizika na tolerovateľnú úroveň.

[5] Jedná sa o tzv. zvyškové riziko definované takou úrovňou rizika, ktorá zostala po prijatí potrebných opatrení pre zmiernenie pôvodne identifikovaného rizika [2, s. 9].

2 RIZIKO V OCHRANE OSOBNÝCH ÚDAJOV

Spracúvanie osobných údajov je jednou z pestrej škály rôznorodých činností, ktoré sú každodenne v nezanedbateľnej početnosti realizované. Akákoľvek realizovaná činnosť, riadená stanovenou autoritou[6], má svoje určité špecifiká, ktorými sa odlišuje od ostatných prebiehajúcich činností. Ich spoločnou vlastnosťou je však to, že v dôsledku vykonávania niektorej z týchto činnosti môžu nastať také okolnosti, ktoré zapríčinia nepriaznivý odklon od jej očakávaného priebehu. Aby bolo možné výskytu týchto okolností predchádzať a ich početnosť eliminovať, je potrebné zavádzať proces riadenia rizík. Preto možno konštatovať, že, rovnako ako pre mnohé iné činnosti, má riadenie rizík dôležité postavenie aj pre činnosti spracúvania osobných údajov. Samotné spracúvanie, nakoľko ide o prácu s istým typom údajov, teda informácií, môžeme považovať za činnosť, pri ktorej je potrebné dbať na bezpečnosť týchto informácií. Hovoríme teda o riadení rizík bezpečnosti informácií [2]. Ide o systematický proces, ktorý by mal stanoviť kontext, vyhodnotiť riziká, vytvoriť plán ošetrenia nájdených a identifikovaných rizík a na základe takto vytvoreného plánu odhalené riziká následne ošetriť, resp. prijať vhodné opatrenia pre ich zmiernenie, ideálne odstránenie.

2.1 Právna úprava ochrany osobných údajov

Problematika osobných údajov a ich ochrany patrí k pomerne novým otázkam, ktoré je potrebné v súčasnej spoločnosti riešiť. Ľudia majú obmedzené možnosti ovplyvňovať vytváranie osobných údajov a taktiež následné zaobchádzanie s nimi. Z tohto dôvodu je nevyhnutná existencia zákonov, ktoré zaručia poskytnutie dostatočnej ochrany údajov.

Právnym predpisom upravujúcim oblasť ochrany osobných údajov v rámci Českej republiky bol zákon č. 256/1992 Sb.[7] V dnešnej dobe sa však stretávame s neustálym, čoraz výraznejším zdokonaľovaním počítačových technológií a verejných elektronických virtuálnych služieb, čoho dôsledkom sú aj zvýšené nároky na právnu úpravu ochrany súkromia a prevažne na úpravu ochrany osobných údajov. Vyššie spomínaná právna úprava bola prvým prameňom svojho druhu v českom právnom poriadku, avšak vedľa mnohých nesporných kladov prinášala aj isté nedostatky, v dôsledku ktorých bola pre pokrytie problematiky nedostačujúca. Hlavným problémom zmieneného zákona bol

[6] Pri všeobecnom popise, uvedenom v kapitole predchádzajúcej, bola za autoritu realizujúcu posudzovanú činnosť označená organizácia. V kontexte spracovania osobných údajov je touto zodpovednou autoritou prevádzkovateľ spracovania osobných údajov.
[7] Zákon o ochraně osobních údajů v informačních systémech.

predpoklad ustanovenia orgánu[8], ktorého poslaním by bol dozor nad prevádzkovaním informačného systému a tiež samotná ochrana osobných údajov jednotlivcov, no takýto orgán pre splnenie potrieb vyplývajúcich z vtedajšej[9] právnej úpravy nikdy nebol zriadený. Za ďalší, a pre potreby tejto práce významnejší, nedostatok je možné považovať fakt, že vtedajšia právna úprava si nezískala potrebnú „popularitu" na to, aby primäla svojich adresátov k jej striktnému dodržiavaniu, a tým pádom nedokázala naplniť svoju primárnu podstatu, a to zabezpečiť dostatočnú ochranu osobných údajov. Z tohto dôvodu bolo potrebné prijať úpravu novú, ktorá by vhodným spôsobom pokrývala všetky potrebné opatrenia vyplývajúce z potrieb modernej spoločnosti.

Podmienkou prijatia novej právnej úpravy ochrany osobných údajov bola nutnosť jej súladu s Dohovorom Rady Európy č. 108/1981 o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov. Návrh novo prijímaného zákona vyšiel zo Smernice Európskeho parlamentu a Rady Európskej únie 95/46/ES o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov. Tento návrh bol schválený a do českého právneho poriadku prijatý ako zákon č. 101/2000 Sb.[10] Zavádza tiež vysvetlenie pojmu „osobný údaj", ktorý definuje ako „*akúkoľvek informáciu týkajúcu sa určeného alebo určiteľného subjektu údajov*." V praxi to teda znamená, že pomocou takýchto informácií je možné priamo či nepriamo identifikovať fyzickú osobu, ktorú právna úprava menuje pojmom „subjekt údajov".

2.2 GDPR a povinnosti prevádzkovateľa

GDPR (anglicky *General Data Protection Regulation*) je Nariadenie Európskeho parlamentu a Rady EÚ 2016/679 o voľnom pohybe týchto dát, ktorým sa zrušuje smernica 95/46/ES. Nariadenie predstavuje nový právny rámec ochrany osobných údajov platný na celom území EÚ. V celom rozsahu nahradilo predchádzajúcu právnu úpravu danej oblasti, ktorá bola doposiaľ na úniovej úrovni regulovaná Smernicou 95/46/ES[11], preberá všetky zásady ochrany a spracúvania údajov z nej vyplývajúce, pričom ale tiež prináša a zavádza nové pravidlá ochrany fyzických osôb v súvislosti s vykonávaním spracovateľských činností, tj. určuje nové povinnosti pre prevádzkovateľa spracúvania osobných údajov, zásadným spôsobom sprísňuje pravidlá ich spracúvania, čím vo svojej hlavnej

[8] §24 zákona č. 256/1992 Sb.
[9] V súčasnosti sa problematikou ochrany osobných údajov zaoberá *Úřad pro ochranu osobních údajů* (ÚOOÚ), ktorého činnosť je vymedzená zákonom č. 110/2019 Sb. o zpracování osobních údajů.
[10] Zákon o ochraně osobních údajů a o změně některých zákonů.
[11] Na úrovni českého právneho poriadku došlo prijatím Nariadenia k nahradeniu zákona č. 101/2000 Sb., ktorý predstavoval predošlý právny rámec založený práve na Smernici 95/46/ES.

podstate poskytuje fyzickým osobám možnosť dôkladnejšej ochrany spracúvaných osobných údajov [5]. Nariadenie GDPR, nakoľko ide o právny predpis v podobe *nariadenia*, sa v rámci EÚ uplatňuje jednotne a má aplikačnú prednosť pred vnútoštátnymi predpismi upravujúcimi oblasť ochrany osobných údajov.

Pojem „osobný údaj" je v podstate veci kľúčový. Nariadenie tento pojem definuje ako „*akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Takúto osobu možno identifikovať priamo alebo nepriamo...*"[12]. Nejedná sa teda len o identifikačné údaje, na základe ktorých by bolo možné konkrétnu osobu jednoznačne určiť, ale spadajú sem všetky informácie týkajúce sa určenej alebo určiteľnej osoby, pričom ju samotné, ani v kombinácií s ďalšími informáciami neidentifikujú (napr. počet detí, dosiahnuté vzdelanie, disponibilné množstvo financií) [6, s. 77].

V oblasti európskeho práva nemožno pri diskutovaní problematiky vymedzenia pojmu „osobný údaj" opomenúť rozsudok SDEÚ vo veci C-582/14 známou tiež pod pojmom *Breyer* [29], ktorý priniesol významné rozhodnutie z hľadiska upresnenia definície kľúčového pojmu. SDEÚ v uvedenom prípade vyjadril stanovisko k dvom predbežným otázkam, z ktorých sa v jednej bližšie venoval práve problematike nepriamej identifikácie pomocou osobných údajov. V bode 41 rozsudku popisuje, že na to, aby mohla byť „*určitá informácia kvalifikovaná ako osobný údaj, nie je nutné, aby sama osebe umožňovala identifikovať dotknutú osobu*", pričom vychádza z právnej úpravy definovanej Smernicou 95/46/ES. SDEÚ v tejto veci dospel k vyjadreniu, že za „*osobný údaj je možné považovať za nepriamy identifikátor v prípade, ak má prevádzkovateľ dostatočné prostriedky k tomu, aby sa dostal k ďalším údajom, pomocou ktorých by v spojení s uvažovaným nepriamym identifikátorom bolo možné fyzickú osobu identifikovať*."[13]

Nariadenie, ako už bolo popísané vyššie, ukladá prevádzkovateľom spracúvania osobných údajov nové povinnosti a zásady pri ich spracúvaní. Nariadením sa teda musia riadiť všetky autority realizujúce spracúvanie, ktoré akýmkoľvek spôsobom zaznamenávajú a následne v rámci vymedzeného účelu spracúvajú informácie o iných subjektoch, a sú teda prevádzkovateľmi, prípadne poverenými sprostredkovateľmi spracúvania osobných údajov. Už pre zabezpečenie všeobecnej povinnosti, ktorú Nariadenie zavádza[14], je prevádzkovateľ povinný primerane riadiť riziká, ktoré by proces spracúvania údajov, s ohľadom na jeho povahu, rozsah, kontext a účely, mohol vytvoriť. Pre dodržanie tejto všeobecnej zákonnej povinnosti je potrebné, aby dochádzalo k pravidelnej identifikácií možných rizík, ktoré by mohli vzniknúť v priebehu realizácie spracovateľskej činnosti,

[12] Článok 4 odst. 1 Nariadenia.
[13] Bod 49 rozsudku SDEÚ vo veci C-582/14.
[14] Článok 24 odst. 1 Nariadenia.

a ďalej je taktiež potrebné, aby prevádzkovatelia tieto identifikované riziká následne analyzovali, hodnotili a riešili, čiže prijímali potrebné opatrenia pre ich zmiernenie na akceptovateľnú úroveň, ideálne pre ich úplné odstránenie.

2.3 Význam procesu riadenia rizík v kontexte ochrany osobných údajov

Koncept riadenia rizík neprenikol do oblasti ochrany osobných údajov až spolu s prijatím Nariadenia. Z európskeho a globálneho hľadiska sa totižto nejedná o novú povinnosť. Na európskom kontinente, napr. v britskej či francúzskej legislatíve, bolo po prevádzkovateľoch spracúvania už predtým požadované, aby pri realizácií spracúvania posudzovali možné riziká. Za najvýznamnejšie vytvorené postupy a metodiky, ktoré majú prevádzkovateľom spracúvania zjednodušiť pochopenie a zavedenie riadenia rizík ochrany údajov, je možné považovať metodiku známu pod termínom *Privacy Impact Assessment* (PIA) [7], vypracovanú francúzskym dozorným úradom CNIL v roku 2012, a taktiež príručku od britského úradu ICO [8] z roku 2007. Realizácia obdobného procesu posúdenia rizika pri spracúvaní osobných údajov za účelom eliminácie rizík voči právam a slobodám subjektom údajov je často vyžadovaná rovnako tak aj v USA. [6, s. 312]

2.3.1 Súvislosť s GDPR – čl. 24 a základné povinnosti prevádzkovateľa

Jednou z hlavných povinností, ktoré prevádzkovateľom spracúvania ukladá Nariadenie, je zabezpečenie súladu spracúvania údajov s Nariadením a následná schopnosť tento súlad preukázať, napr. prostredníctvom zodpovedne vedenej dokumentácie. S cieľom zabezpečiť adekvátnu ochranu spracovávaných osobných údajov a tým aj súlad ich spracovania s Nariadením by mal prevádzkovateľ uskutočňovať opakovane, resp. neustále analýzu rizík spracúvania údajov a následne prijímať potrebné opatrenia, ako sú napr. pseudonymizácia spracúvaných údajov[15], obmedzenie prístupu alebo fyzické či sieťové zabezpečenie údajov, s pomocou ktorých by bolo možné identifikované riziká konkrétneho procesu spracúvania zmierniť či odstrániť [6, s. 246].

Článok 24 odst. 1 Nariadenia stanovuje akýsi základ pre plnenie povinnosti prevádzkovateľa spracovania v zmysle uskutočňovania riadenia rizík spracúvania údajov:

> *„S ohľadom na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil*

[15] Bod 28 odôvodnenia Nariadenia.

a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením. Uvedené opatrenia sa podľa potreby preskúmajú a aktualizujú.“

Tento článok vymenúva všetky aspekty: *povahu, rozsah, kontext a účely spracúvania*, ktoré by mal pri prevádzkovateľ spracúvania pri posudzovaní rizík brať do úvahy. Ďalej definuje riziko ako funkciu dvoch základných hodnôt, a to *pravdepodobnosti a závažnosti pre práva a slobody fyzických osôb*. Ide o tradičné poňatie problematiky hodnotenia rizík, ktoré slúži k určeniu výslednej hodnoty rizika (viď ďalej kap. 2.4). Pri tomto hodnotení je potrebné brať do úvahy dopad, aký by mohlo mať prípadný vznik rizika na subjekty spracúvaných údajov, nie na organizáciu samotnú. Taktiež zavádza už spomínanú povinnosť prevádzkovateľa *prijať vhodné technické a organizačné opatrenia* v prípade, že bude identifikovaná taká miera rizika, ktorá by svojou závažnosťou mohla ohroziť práva a slobody subjektov údajov. Všetky opatrenia potrebné k zaisteniu dodržiavania zásad spracúvania je nutné prijímať už v dobe určovania prostriedkov, pomocou ktorých bude posudzovaná spracovateľská činnosť realizovaná, a následne je rovnako nutné ich dodržiavať počas celej doby vykonávania spracovania a uchovávania údajov až do momentu ich zlikvidovania. Nakoniec už len zvýrazňuje chápanie riadenia rizík ako systematického procesu, pri ktorom je potrebné neustále *preskúmavať a aktualizovať* už predtým ohodnotené riziká a následne prijaté ošetrujúce opatrenia, aby bolo možné preukázať vytvorenie a dodržiavanie požadovaného súladu s Nariadením zo strany prevádzkovateľa daného procesu spracovania osobných údajov.

V nadväznosti na článok 24 Nariadenia by bolo nevhodné nespomenúť jeho rozšírenie nasledujúcim článkom 25 Nariadenia, ktorý, narozdiel od článku 24 Nariadenia upravujúceho problematiku voľby vhodných opatrení pre zaistenie súladu s Nariadením, priamo špecifikuje, akým spôsobom a za akých okolností je potrebné tieto opatrenia implementovať [9, s. 504]. Prijatie primeraných technických a organizačných opatrení realizuje prevádzkovateľ za účelom dodržania všetkých zásad ochrany osobných údajov definovaných článkom 5 odst. 1 Nariadenia. V praxi teda musí prevádzkovateľ prijať v prípade potreby také organizačné a technické opatrenia, aby (i) spracovával osobné údaje len na základe právneho titulu, (ii) boli subjekty údajov o spracovaní údajov vhodne informované, (iii) nespracovával viac údajov, než je nevyhnutné, (iv) spracovával len presné a správne údaje, (v) neuchovával osobné údaje v priebehu dlhšej doby, než je nevyhnutné, (vi) a aby zaistil, že osobné údaje budú chránené pred neoprávneným či protiprávnym spracovaním a pred náhodnou stratou, zničením alebo poškodením [6, s. 260]. Posledný popísaný bod odzrkadľuje zásadu zaväzujúcu prevádzkovateľa k zabezpečeniu nenarušenia integrity a dôvernosti spracúvaných osobných údajov. Samotné Nariadenie

touto deklaráciou bezpečnosti osobných údajov ako jednej z kľúčových povinností prevádzkovateľa prináša v tomto smere rozdiel v porovnaní s predchádzajúcou zákonnou úpravou ochrany osobných údajov v zmysle zákona č. 101/2000 Sb.

Článok 5 Nariadenia zaväzuje prevádzkovateľa nielen k dodržiavaniu vyššie uvedených zásad spracúvania, ale stanovuje taktiež zodpovednosť prevádzkovateľa v zmysle jednak dodržiavania základných zásad spracúvania a rovnako tak v zmysle schopnosti preukázať ich skutočné dodržiavanie[16], kedy hovoríme o tzv. zásade zodpovednosti prevádzkovateľa. V nadväznosti na čl. 24 Nariadenia, ktorý uvádza, že *„prevádzkovateľ prijme vhodné technické a organizačné opatrenia, aby zabezpečil a bol schopný preukázať, že spracúvanie sa vykonáva v súlade s týmto nariadením“*, možno konštatovať, že sa jedná o performatívne[17] pravidlo vyplývajúce z regulácie prostredníctvom Nariadenia, nakoľko nie je činnosť prevádzkovateľa jednoznačne regulovaná, ale pokyny Nariadenia majú za cieľ prevádzkovateľa motivovať tvorbe vlastných pravidiel uskutočňovania prevádzkovaných činností takým spôsobom, aby bolo možné zabezpečiť súlad vykonávaného spracúvania údajov s Nariadením.

Podkladom pre tvorbu vlastných pravidiel rozhodných v otázke potrebnosti prijímania určitých technických a organizačných opatrení je proces riadenia rizík, ktorý dokáže poskytnúť prevádzkovateľovi dostatočnú predstavu o tom, aké riziká by mohli vzniknúť v dôsledku vykonávania spracovateľských činností, čo by bolo ich príčinou a aký zásah do práv a slobôd by mohli voči subjektom údajov spôsobiť. Realizácia riadenia rizík vo všeobecnosti by mala byť pre prevádzkovateľa jednoznačnou a neodkladnou záležitosťou, v závislosti na ktorej môže následne prispôsobiť svoje ďalšie kroky spôsobom vhodným pre zabezpečenie súladu s Nariadením. Identifikované riziko hroziace v dôsledku realizácie činností spracúvania údajov teda predstavuje istý referenčný bod umožňujúci prevádzkovateľovi rozhodnúť o tom, od akého momentu je potrebné pristupovať k prijímaniu opatrení s cieľom dodržať zásady spracúvania, a naopak kedy to nutné vzhľadom k nízkej miere hroziaceho rizika nie je [9, s. 504]. Pôsobenie performatívnej regulácie zásady zodpovednosti v tejto oblasti sa teda prejavuje spôsobom, kedy je prevádzkovateľ povinný neodkladne prijímať rozsiahlejšie a efektívnejšie opatrenia v prípadoch hrozby väčšieho rizika pre práva a slobody subjektov údajov. Naopak v prípadoch, kedy sú riziká minimálne, sa môže rozhodnúť zohľadniť náročnosť a nadbytočnosť implementácie opatrení, ktoré by vzhľadom k nízkej miere rizika už viac významne nepodporili zefektívnenie ochrany práv a slobôd subjektov údajov [11, s. 143].

[16] Článok 5 odst. 2 Nariadenia.
[17] Všeobecne k performatívnym pravidlám viď [10].

2.3.2 Súvislosť s GDPR – čl. 35 a potreba vykonania DPIA

Pre doplnenie popisu problematiky zamerania tejto práce by nemal byť opomenutý ani článok 35 Nariadenia, ktorý je ústrednou časťou popisujúcou formálne náležitosti pre podmienky a realizáciu tzv. posúdenia vplyvu na ochranu údajov (*DPIA*). V predchádzajúcom popise už bolo naznačené, že prevádzkovateľ je povinný neustále posudzovať riziká, ktoré vznikajú v dôsledku ním realizovaných spracovateľských činností. Tento pravidelne opakovaný proces všeobecného posúdenia rizík prináša prevádzkovateľovi spracúvania možnosť identifikovať tie situácie, kedy by posudzované spracúvanie mohlo prinášať riziko, ktorého hodnota by bola z istých dôvodom neprípustná. Z tohto pohľadu možno považovať ako kľúčový bod Nariadenia práve článok 35, ktorý explicitne zaväzuje prevádzkovateľa k vykonávaniu *DPIA* v prípade, kedy posudzované spracúvanie *„pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb“* [18]. Povinnosť vykonávať posúdenie vplyvu na ochranu osobných údajov bola v rámci Nariadenia zavedená ako súčasť komplexnej oblasti zabezpečenia osobných údajov. Táto povinnosť súvisí s povinnosťou prevádzkovateľa vhodným spôsobom znižovať identifikované riziká. Jedná sa o teda jednu z nových povinností zavedenú za účelom posilnenia zmyslu prístupu založenom na riziku, ktorý prevádzkovateľov spracúvania smeruje k činnostiam vyhodnocovania a minimalizácie rizikovosti z pohľadu subjektov údajov. Článok 35 Nariadenia ďalej definuje prípady, v ktorých je nevyhnutné posúdenie vykonať, čím poskytuje prevádzkovateľom akýsi návod, na základe ktorého môžu rozhodovať o tom, či je nutné samotné posúdenie *DPIA* vypracovať.

Ako problematické sa môže zdať práve určenie, kedy spracovateľská operácia môže viesť k „*vysokému riziku*“. Pracovná skupina zriadená podľa článku 29 (WP29) vypracovala pokyny k realizácií *DPIA*, v ktorých definuje deväť kritérií, ktoré je potrebné zvážiť pri posudzovaní rizikovosti spracúvania. Skúmané spracúvanie, ktoré spĺňa aspoň dve zo zmienených kritérií, je považované za proces vyžadujúci realizáciu *DPIA* [12, s. 10 – 13]. Keď nie je jasné, či sa má vyžadovať posúdenie vplyvu na ochranu údajov, WP29 odporúča, aby sa napriek tomu vykonalo, keďže *DPIA* predstavuje tiež užitočný nástroj, ako pomôcť prevádzkovateľom spracúvania dodržiavať právne predpisy o ochrane údajov. Samotné vypracovanie posúdenia je realizované vo svojej podstate len z preventívnych povinností. Ak sa však pri jeho realizácií vo fáze posudzovania rizík vyplývajúcich zo spracúvania preukáže, že daná spracovateľská operácia môže priniesť vysoké riziko pre práva a slobody fyzických osôb, tak sa z preventívnej realizácie stáva skutočné plnenie povinnosti prevádzkovateľa v zmysle zabezpečenia súladu s Nariadením [11, s. 163] .

[18] Článok 35 odst. 2 Nariadenia.

Nariadenie rovnako definuje povinnosť dozorného orgánu[19] zverejniť zoznam takých spracovateľských operácií, ktoré jednoznačne podliehajú požiadavke na vykonanie *DPIA*[20]. Rovnako tak môže aj explicitne stanoviť, ktoré operácie naopak požiadavke na vykonanie *DPIA* nepodliehajú[21]. Je nutné upozorniť, že stanovený výpis jednotlivých činností, ktoré, či už podliehajú, alebo i nepodliehajú požiadavke na vykonanie *DPIA*, sa môže s ohľadom na vývoj technológií alebo rôznych životných situácií meniť. S prihliadnutím k tejto skutočnosti sa zdá byť zrejmé, že nemožno stanoviť jednoznačný rámec pre všeobecnú klasifikáciu spracovateľských operácií, ale prevádzkovať by mal za každých okolností ním prevádzkované činnosti vždy zodpovedne zanalyzovať a na základe výsledkov všeobecného posúdenia rozhodnúť o nutnosti vykonania *DPIA*.

Pokiaľ teda prevádzkovateľ na základe realizácie všeobecného posúdenia rizík dospeje k zisteniu, že ním prevádzkované spracovateľské činnosti môžu vyústiť vo vysoké riziko pre práva a slobody subjektov údajov, je povinný neodkladne vykonať *DPIA* v spolupráci s určenou zodpovednou osobou, ak je pre realizované spracúvanie údajov určená[22]. Cieľom realizácie *DPIA* je dostatočne zhodnotiť všetky parametre realizovaného spracúvania, medzi ktoré nevyhnutne patria jeho účel, rozsah a kontext, s prihliadnutím na možné riziká pre práva a slobody fyzických osôb a rovnako tak na stav techniky za účelom stanovenia potrebných technických a organizačných opatrení. Správny postup určovania a následne prípadného odstraňovania rizík pre súkromie tých osôb, ktorých práva a slobody môžu byť zasiahnuté v dôsledku určitého spracúvania osobných údajov, je rozhodujúci pre voľbu vhodných základných parametrov spracúvania osobných údajov takým spôsobom, ktorý umožní dosiahnuť zaistenie súladu spracúvania osobných údajov s požiadavkami Nariadenia.

Podrobné vysvetľovanie problematiky realizácie jednotlivých krokov rozsiahleho a komplexného posúdenia *DPIA* je nad rámec naplnenia účelov tejto práce. Ďalšie kapitoly budú venované popisu všeobecného posúdenia rizík v kontexte spracúvania osobných údajov, ktoré možno chápať ako prvý krok získavania informácií pri rozhodovaní v otázke potreby vykonania samotného procesu *DPIA* v prípade hrozby vysokého rizika pre práva a slobody v dôsledku realizácie spracúvania osobných údajov, a pri prípadnom následnom vykonávaní *DPIA* ako jeho neoddeliteľnú súčasť.

---

[19] Na území ČR je týmto orgánom ÚOOÚ (viď kap. 2.1).
[20] Čl. 35 odst. 4 Nariadenia.
[21] Čl. 35 odst. 5 Nariadenia.
[22] Podmienky určenia zodpovednej osoby stanovuje čl. 37 odst. 1 Nariadenia. Prevádzkovateľ (príp. sprostredkovateľ) spracúvania je povinný menovať zodpovednú osobu v prípadoch spracúvania realizovaného orgánom verejnej moci alebo verejnoprávnym subjektom, ďalej pokiaľ dochádza k pravidelnému a systematickému monitorovaniu subjektov údajov vo veľkom rozsahu a/alebo pokiaľ je hlavnou činnosťou spracúvanie kategórie citlivých osobných údajov.

2.4 Proces riadenia rizík pri spracúvaní osobných údajov

Už v úvodných slovách tejto kapitoly odznelo, že spracúvanie osobných údajov je možné a potrebné zaradiť do rovnocennej roviny k akýmkoľvek iným činnostiam s rozličným zameraním. Pre všetky činnosti, za realizáciou ktorých stojí určitá autorita, by malo byť uskutočňované riadenie rizík, nakoľko môžu počas svojho chodu prinášať riziká v podobe neočakávaných udalostí, ktoré by mali za následok odklon od očakávaného výsledku danej činnosti. Pri popise problematiky spracúvania osobných údajov za činnosť, pre ktorú je potrebné vykonávať riadenie rizík, považujeme samotný proces spracúvania. Dôvody nutnosti vykonania procesu riadenia rizík spracúvania údajov boli rovnako už popísané v predchádzajúcich častiach kapitoly, no pre rýchle a jednoznačné vysvetlenie ich možno zhrnúť do formulácie „zabezpečenie súladu s Nariadením“. Základnou myšlienkou Nariadenia je chrániť spracúvané osobné údaje a tým aj fyzické osoby, ktorých sa tieto údaje týkajú. V tomto prípade by odklon od očakávanej činnosti v dôsledku vzniku rizika znamenal porušenie hlavnej podstaty uvedenej myšlienky. To znamená, že výskyt rizika pri spracúvaní osobných údajov by mal za následok porušenie ochrany týchto údajov, čo by mohlo následne vyústiť v zásah do práv a slobôd subjektov údajov.

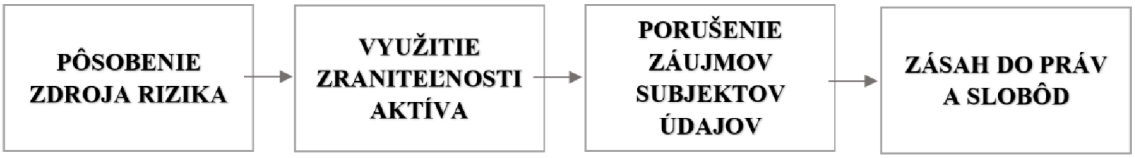
Všeobecný popis riadenia rizík, konkrétne jeho podčasti posúdenia a ošetrenia rizík, bol naznačený v kap. 1.2. Pri vnímaní problematiky realizácie riadenia rizík v kontexte spracúvania údajov zostáva základná štruktúra procesu zachovaná. Dôležité je však podotknúť, že riadenie rizík, a jeho dielčie podčasti vrátane fázy posudzovania rizík, neprebiehajú len nad rovinou zaisťovania informačnej bezpečnosti, ako ho popisuje norma ISO 27005:2013 [2]. Nad touto rovinou leží vrstva jej nadradená, ktorej úlohou je zabezpečiť práve dodržanie hlavnej povinnosti uloženej Nariadením. Ak sa teda jedná o posudzovanie rizík spracúvania osobných údajov, je potrebné systém riadenia bezpečnosti informácií doplniť ešte o špecifické prvky viažuce sa práve k problematike spracúvania osobných údajov. Výsledkom prepojenia dvoch uvedených rovín je systematický proces, ktorý by mal stanoviť kontext spracúvania, vyhodnotiť možné riziká, vytvoriť plán ošetrenia nájdených a identifikovaných rizík a na základe takto vytvoreného plánu odhalené riziká ošetriť, resp. prijať opatrenia pre ich zmiernenie či odstránenie.

Za kľúčovú fázu celého procesu riadenia rizík možno považovať fázu posudzovania rizík, konkrétne jej identifikačnú časť, počas ktorej dochádza k určovaniu troch kľúčových údajov, – čo a akým spôsobom môže byť ohrozené a aký to bude mať dopad – ktoré hrajú dôležitú rolu pri určovaní výslednej hodnoty identifikovaného rizika. Z pohľadu vnímania roviny informačnej bezpečnosti je v tomto momente vhodné definovať pojem „aktívum“. V jednoduchosti povedané, je to čokoľvek, čo má pre subjekt určitú hodnotu,

ktorá môže byť narušená a zmenšená pôsobením hrozby [1, s. 96]. Základnou charakteristikou aktíva je jeho hodnota. Tá môže byť vyjadrená objektívnym spôsobom, kedy vo väčšine prípadov odzrkadľuje všeobecne vnímanú cenu daného aktíva.

V procese riadenia rizík podľa Nariadenia za hlavné sledované aktíva považujeme informácie, konkrétne osobné údaje. Objektívne hodnotenie takýchto aktív na základe ich skutočnej ceny by bolo vskutku nemožné, preto je ich hodnota založená na subjektívnom ocenení dôležitosti aktíva pre daný subjekt [1, s. 97]. Pri určovaní hodnôt rizík spracúvania osobných údajov je teda potrebné určiť, aké nepríjemnosti by vyvolanie hrozby spôsobilo pre práva a slobody subjektov spracúvaných údajov.

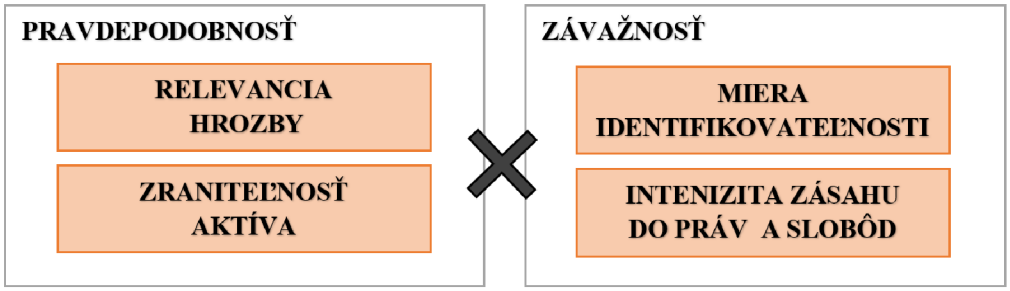
Dôležitosť riadenia rizík v ochrane osobných údajov spočíva v systematickom odhaľovaní problémov a ich následnom odstraňovaní. Aby bolo možné tieto kroky uskutočniť, je v prvom rade nutné pochopiť vzájomné prepojenie a následnosť viacerých udalostí, ktoré prebiehajú na pozadí vzniku problému, čiže skúmaného rizika. Pri stanovení úrovne rizika sa pracuje so zoznamom identifikovaných hrozieb, zraniteľností, ovplyvnených aktív, a dopadov na tieto aktíva a sledované procesy [1, s. 97]. Dopad na samotné aktíva v kontexte riadenia rizík spracúvania osobných údajov nemá až taký veľký význam. Omnoho dôležitejšie postavenie zastáva dopad na sledované procesy, ktorým je zásah do práv a slobôd subjektov údajov. Preto priebeh vzniku rizika pri spracúvaní osobných údajov možno popísať nasledovne: *existuje zdroj rizika, ktorý pôsobením hrozby využije zraniteľnosť podporného aktíva, čím dochádza k zmene očakávaného výsledku. V kontexte spracúvania osobných údajov pod touto zmenou chápeme porušenie záujmov subjektov údajov, čo má za následok zásah do ich práv a slobôd* [13, s. 31]. Slovne vyjadrený kauzálny nexus ako sled definovaných udalostí, ktorý postupne prebieha na pozadí procesu vzniku samotného rizika, je zachytený na obr. 2.1.



Obr. 2.1: Sled udalostí spôsobujúcich vznik rizika. [13]

Takto identifikovaný sled konkrétnych udalostí bude jedinečný pre každé jedno odhalené riziko vyskytujúce sa v rámci posudzovanej spracovateľskej činnosti. V ďalších fázach riadenia rizík dochádza k priradeniu hodnoty každému jedinečnému riziku, pričom je táto hodnota vyjadrená ako funkcia hodnôt pravdepodobnosti naplnenia týchto udalostí a ich následkov, teda závažnosti dopadu, ktorý sled týchto udalostí zapríčiní [1, s. 97].

Navrhovaná metodika posúdenia rizík, ktorú táto práca popisuje v kap. 3, stanovuje výslednú úroveň rizika nasledovne: pravdepodobnosť rizika vyjadruje možnosť, že vôbec vznik rizika nastane. Jeho vznik je ovplyvnený mierou zraniteľnosti podporného aktíva, ktoré je určitým spôsobom zapojené do realizácie spracúvania osobných údajov, a mierou relevancie hrozby, ktorá odzrkadľuje schopnosti zdroja rizika využiť zraniteľnosť aktíva [14, s. 46]. Hodnota závažnosti odpovedá dopadu, ktorý využitie odhalenej zraniteľnosti podporného aktíva spôsobí. Ako bolo popísané vyššie, hlavným sledovaným dopadom je zásah do práv a slobôd subjektov údajov, k čomu sa viaže aj miera identifikovateľnosti týchto subjektov. Popísané určenie výslednej hodnoty posudzovaného rizika názorne zobrazuje obr. 2.2.



Obr. 2.2: Výsledná hodnota rizika ako funkcia pravdepodobnosti a závažnosti.

2.5 Problematika akceptácie a ošetrenia rizík v kontexte spracúvania osobných údajov

Proces posúdenia rizík prináša prevádzkovateľovi spracúvania údajov kompletný zoznam ohodnotených rizík, ktoré ním vedený proces spracúvania osobných údajov prináša. Nasledujúcou fázou v celom procese riadenia rizík je fáza ošetrenia rizík. Primárnym cieľom tejto fázy je navrhnúť a aplikovať potrebné opatrenia, ktoré umožnia znížiť hodnotu rizika na akceptovateľnú úroveň. Ešte predtým je potrebné vôbec určiť, pre ktoré riziká je potrebné navrhovať a následne aplikovať nápravné opatrenia. Prevádzkovateľ preto musí určiť tzv. kritériá pre akceptáciu rizík, s ktorými bude porovnávať výsledok predchádzajúcej fázy procesu, čiže už identifikované a ohodnotené riziká.

V kontexte spracúvania osobných údajov sa zdá byť práve stanovenie vhodných a primeraných kritérií pre akceptáciu identifikovaných rizík najpodstatnejším krokom celého procesu riadenia rizík. Prevádzkovateľ spracúvania údajov je totižto postavený do situácie, kedy nemôže hodnotiť skutočnosti len na základe subjektívneho pohľadu, kedy by zvažoval prijatie nápravných opatrení najmä z pohľadu vlastnej ekonomickej straty či

zisku[23]. Pri zameraní procesu posudzovania rizík na práva a slobody fyzických osôb musí prevádzkovateľ hodnotiť dopad rizika, čiže samotný zásah do nejakého práva či slobody, z pohľadu tretej osoby a na základe tohto posudku stanoviť kritériá pre akceptáciu rizík, čo môže byť v mnohých situáciách neľahké a problematické.

Ako bolo v tejto práci už popísané, jedným z primárnych cieľov, pre dosiahnutie ktorého bolo Nariadenie uvedené do platnosti, je zabezpečiť patričnú ochranu práv a slobôd fyzických osôb spojenú so spracúvaním im príznačných osobných údajov. Avšak samotné Nariadenie v jednom zo svojich odôvodnení uvádza, že „*právo na ochranu osobných údajov nie je absolútne právo, musí sa posudzovať vo vzťahu k jeho funkcii v spoločnosti a musí byť vyvážené s ostatnými základnými právami, a to v súlade so zásadou proporcionality*“[24]. Ďalej vymenúva niekoľko základných práv, ktoré by sa mohli dostať do rozporu s právom na ochranu osobných údajov. V tomto súpise základných práv sa objavujú, okrem iných, napríklad sloboda prejavu a právo na informácie či sloboda podnikania. Je na mieste tvrdiť, že vymenované základné práva môžu v určitých situáciách odzrkadľovať isté oprávnené záujmy prevádzkovateľa spracúvania údajov. V situácií, kedy sa posudzujú dve proti sebe stojace základné práva a kedy je potrebné určiť, ktoré z týchto práv prevažuje nad druhým, sa využíva koncept proporcionality, tj. uplatňuje sa tzv. trojstupňový test pre posúdenie vzájomného pomeru proti sebe stojacich práv. Nariadenie samotné[25] priznáva uplatnenie myšlienky zavedenia proporcionality v súvislosti so sledovaním oprávnených záujmov prevádzkovateľa.

WP29 popísanú problematiku vzájomného rozporu oprávneného záujmu prevádzkovateľa spracúvania údajov a ochrany práv a slobôd fyzických osôb približuje v jednom zo svojich stanovísk [15]. Prináša v ňom prehľad záujmov, ktoré sa pri vykonávaní spracúvania v záujme zabezpečenia základných práv a slobôd prevádzkovateľa či inej tretej strany[26] môžu dostať do konfliktu so základným právom subjektov na ochranu ich osobných údajov [15, s. 27]. Je dôležité poznamenať, že do úvahy je možné brať len legitímny záujem prevádzkovateľa, tj. taký záujem, ktorý nebude v rozpore s akýmkoľvek účinným

[23] Tak by tomu bolo napr. v situácií, kedy by prevádzkovateľ realizoval posúdenie rizík so zameraním na vlastné informačné systémy, resp. vlastné aktíva. Mohol by následne objektívne zhodnotiť (vo finančných čiastkach), aké náklady by musel vynaložiť pre zavedenie potrebných opatrení a na základe toho by sa mohol, do istej miery subjektívne, rozhodnúť, či je preňho z ekonomického hľadiska vhodné a výhodné investovať do realizácie nápravných opatrení, alebo či radšej vystaví systém identifikovanému riziku, nakoľko by odstránenie či aspoň minimalizácia takého rizika predstavovala vyššie náklady v porovnaní so vznikom samotného rizika.

[24] Bod 4 odôvodnenia Nariadenia.

[25] Článok 6 odst. 1 písm. f) Nariadenia.

[26] Pod pojmom „tretia strana“ si možno v tomto kontexte predstaviť nielen inú osobu, ale aj spoločnosť ako celok. Tá môže mať taktiež v konkrétnych situáciách určitý záujem, napr. pri ochrane zdravia a bezpečnosti vybraných skupín obyvateľstva.

právnym predpisom. Len pre záujmy, ktoré splnia túto podmienku, je možné uvažovať vykonanie porovnania proti sebe stojacich základných správ prevádzkovateľa spracúvania a subjektov ním spracúvaných údajov.

Podrobný popis toho, ako má prevádzkovateľ spracúvania pristupovať k určeniu a následnému zváženiu kritérií pre vyhodnotenie nutnosti zavedenia opatrení v rámci vykonania adekvátneho ošetrenia rizika, je nad rámec naplnenia účelu tejto práce. Táto práca bližšie popisuje najmä posudzovanie rizík, ktoré v rámci celého procesu riadenia rizík predchádza fáze ošetrenia. Nasledujúca kapitola bude venovaná návrhu metodiky pre posudzovanie rizík procesu spracúvania osobných údajov s výsledkom v podobe zoznamu ohodnotených rizík, ktoré môžu v dôsledku realizácie posudzovanej spracovateľskej činnosti vzniknúť. Na základe výstupného zoznamu rizík s ich príslušným ohodnotením už potom musí sám prevádzkovateľ vyhodnotiť získané údaje a zvážiť potrebu rozsahu a vhodného spôsobu ošetrenia identifikovaných rizík.

3 NÁVRH METODIKY PRE POSUDZOVANIE RIZÍK

Pre potreby realizácie praktického výstupu záverečnej práce predstavuje táto kapitola návrh metodiky pre posudzovanie rizík v kontexte ochrany osobných údajov, ktorá bude tvoriť neoddeliteľný stavebný prvok činnosti výslednej aplikácie. Táto kapitola zároveň do istej miery predstavuje i niekoľko existujúcich metodík súvisiacich s danou problematikou, nakoľko z nich preberá určité prvky a odôvodneným spôsobom ich zlučuje do jedného fungujúceho celku. Jedným z hlavných východiskových materiálov pre tvorbu vlastnej metodiky je prístup posudzovania rizík, uvedený v norme ČSN ISO 27005:2013, zameraný na posudzovanie rizík v súvislosti s riadením informačnej bezpečnosti. Tento prístup určuje výslednú hodnotu rizika z dvoch dielčích hodnôt, a to zo závažnosti následkov vyvolaného nepriaznivého incidentu na napadnuteľné aktívum a z pravdepodobnosti výskytu tohto incidentu [2, s. 10]. Problematika určenia výslednej hodnoty identifikovaného rizika bola z teoretického hľadiska vysvetlená v kap. 2.4. Výsledná hodnota je pritom určená s prihliadnutím na predpokladaný priebeh vzniku nežiadúceho rizika, ktorý bol zachytený na obr. 2.1, tj. existuje istý zdroj rizika, ktorý realizáciou hrozby využije zraniteľnosť aktíva, čím dochádza k zmene očakávaného výsledku, a teda k vzniku nežiaducej udalosti, v dôsledku ktorej vzniknú subjektom údajov nepríjemnosti.

Súčasne táto metodika preberá isté prvky a spôsoby hodnotenia najmä z metodiky *Privacy Impact Assessment* (PIA) od francúzskeho dozorného úradu CNIL. V niektorých častiach navrhuje mierne odlišnosti od tohto referenčného postupu, pričom sú však dôvody týchto odlišností pre účely tejto metodiky primerane opodstatnené a vysvetlené.

Navrhnutá metodika je postavená na princípe kvalitatívnej metriky, čo znamená, že v procese posudzovania rizík sú výsledné riziká hodnotené v závislosti od dopadu na práva a slobody subjektov spracúvaných údajov, ktorý sa posudzuje v subjektívnom vzťahu k týmto subjektom. Na základe získaného výsledku vykonaného procesu následne na strane prevádzkovateľa posúdeného spracúvania vzniká možnosť voľby v súvislosti s riešením otázky, do akej miery a hodnoty je z ekonomického hľadiska potrebné a zároveň vhodné prijímať adekvátne opatrenia pri následnom ošetrení rizika, aby s prijatím daných opatrení bolo zároveň možné zabezpečiť súlad s požiadavkami na realizáciu činností spracúvania definovanými Nariadením.

Na realizáciu celého procesu posúdenia rizík, resp. realizáciu jeho jednotlivých etáp (identifikačnej a analytickej časti) možno nahliadať dvomi rôznymi spôsobmi, a rozložiť tak tento proces do dvoch hlavných, súčasne prebiehajúcich rovín. Nižšie popísaný dvojstranný pohľad na celú problematiku v sebe nesie aj navrhnutá metodika, pričom ich

v rámci procesu posúdenia rizík spája v jeden sledovaný výsledok, ktorým je určenie výslednej hodnoty rizika posudzovaného procesu spracúvania.

Prvá oblasť je zameraná na posúdenie tých prvkov, ktoré sú špecifické práve pre problematiku spracúvania osobných údajov, tj. vymedzenie kontextu posudzovaného spracúvania a všetkých parametrov preň príznačných a hodnotenie ujmy v podobe zásahu do ľudských práv a slobôd, ktorá môže v dôsledku výskytu rizika pri vykonávaní spracúvania fyzickým osobám vzniknúť. V tejto časti sa navrhnutá metodika opiera z veľkej časti o postup, ktorý poskytuje spomínaná metodika PIA [16]. V oblasti riešenia otázky ochrany osobných údajov sa metodika taktiež mnohokrát opiera o odporúčania a stanoviská Pracovnej skupiny zriadenej podľa článku 29 (WP29). Na druhej strane je potrebné venovať pozornosť taktiež tým prvkom, ktoré realizujú samotný proces spracúvania osobných údajov. V tomto smere dochádza k posudzovaniu podporných aktív zapojených do vykonávania posudzovanej spracovateľskej činnosti, ďalej zraniteľností, ktoré sa na týchto aktívach môžu vyskytnúť a v neposlednom rade je taktiež potrebné identifikovať a analyzovať hrozby, ktoré by využitím identifikovaných zraniteľností podporných aktív mohli vyvolať incident a spôsobiť tým nepriaznivý následok v podobe zásahu do práv a slobôd subjektov údajov. Posudzovanie hrozieb a zraniteľností identifikovaných na podporných aktívach je do istej miery inšpirované myšlienkami obsiahnutými v už spomínanej metodike PIA [16], niektoré prvky preberá tiež z normy ISO 27005:2013 [2], no oba tieto prístupy z veľkej časti dopĺňa o vlastné znalosti, úvahy a názory.

3.1 Identifikácia parametrov spracovania osobných údajov

Pre posúdenie nepriaznivého zásahu do práv a slobôd subjektov spracúvaných údajov je v prvom rade dôležité pochopiť a analyzovať kontext posudzovaného procesu spracúvania. Musia byť preto známe odpovede na otázky aký je účel spracúvania údajov, aké osobné údaje a v akom rozsahu sa spracúvajú. Identifikácia uvedených druhov informácií o konkrétnom spracúvaní je nevyhnutná pre vyhodnotenie pravdepodobnosti a závažnosti hrozby, ktorá pre subjekty údajov predstavuje riziko v rámci daného procesu spracúvania.

3.1.1 Kontext spracovania

Rizikovosť konkrétneho spracúvania údajov závisí na mnohých faktoroch, ktorých spojenie robí túto spracovateľskú operáciu jedinečnou v porovnaní s inými. Pri posudzovaní a hodnotení rizikovosti je potrebné brať do úvahy to, koho sa spracúvané údaje, zaznamenávané v posudzovanom procese, týkajú, aké kategórie údajov sú o danom subjekte spracúvané, v akom rozsahu sú tieto údaje spracúvané a aký je účel ich spracúvania.

Z týchto vymenovaných faktorov je následne možné aspoň odhadnúť, aký nepriaznivý dopad by mohol byť spôsobený výskytom rizika, tj. akejkoľvek neočakávanej situácie, ktorá by odklonila proces spracúvania údajov od jeho pôvodne vytýčeného zámeru. Ako príklad dopadu je možné uviesť napríklad jednoznačné identifikovanie subjektu údajov.

Viesť záznamy o vymenovaných parametroch spojených s daným spracúvaním by mal prevádzkovateľ už len z povinností vyplývajúcich z Nariadenia, ktoré stanovuje určovanie hodnoty rizika spracúvania pre práva a slobody subjektov údajov „*na základe povahy, rozsahu, kontextu a účelu spracúvania*“ [27]. Identifikácia týchto vlastností spracúvania je preto neoddeliteľnou súčasťou posudzovania rizík.

Subjekt údajov

Pracovná skupina WP29 zahŕňa medzi spracovateľské operácie, ktoré môžu predstavovať vysoké riziko, aj tie situácie, kedy sa spracúvajú údaje o tzv. zraniteľných osobách. Pri tejto úvahe vychádza z bodu 75 odôvodnenia Nariadenia, ktoré uvádza, že vyššie riziko hrozí v prípade, „*ak sa spracúvajú osobné údaje zraniteľných fyzických osôb, najmä detí*“[28]. WP29 medzi zraniteľné osoby zahŕňa aj ďalšie skupiny ľudí, akými sú napríklad zamestnanci, mentálne postihnuté osoby, staršie osoby atď. Ich spoločným znakom je, že sa nachádzajú v nerovnovážnom postavení voči prevádzkovateľovi spracúvania ich osobných údajov, kedy buď nemôžu vyjadriť nesúhlas so spracúvaním (napr. zamestnanci), alebo sa nachádzajú pozícií, kedy nie sú schopné na základe vlastného uváženia namietať voči spracúvaniu svojich údajov (ako napr. deti či mentálne postihnuté osoby) [12, s. 12].

Kategórie a rozsah osobných údajov

Zákonná definícia pojmu osobný údaj bola už v teoretickej časti vysvetlená, viď kap 2.2. Z hľadiska dôležitosti jednotlivých prvkov procesu posudzovania rizík konkrétne údaje možno považovať za kľúčový prvok celého procesu posudzovania. V prípade výskytu určitého rizika pri spracúvaní osobných údajov vzniká dotknutým subjektom istá ujma, ktorá sa prejaví v dôsledku zásahu do ich práv a slobôd. Ujma nemusí byť nutne viazaná na konkrétny spracúvaný osobný údaj o danom subjekte. V niektorých prípadoch užitie samostatného údaju nebude mať priamo za následok vysoké riziko a s ním súvisiaci vznik ujmy, no následná kombinácia jednotlivých údajov už zvýšené riziko spôsobiť môže. To, do akých práv a slobôd bude fyzickým osobám zasiahnuté a aká bude miera a intenzita

[27] Bod 76 odôvodnenia Nariadenia.
[28] Bod 75 odôvodnenia Nariadenia.

tohto nepriaznivého zásahu, závisí, okrem iných faktorov, taktiež na tom, aké osobné údaje (resp. aká kombinácia spracúvaných údajov) boli postihnuté. Na základe povahy spracúvaných osobných údajov je taktiež možné určiť, či s využitím týchto údajov (resp. akoukoľvek ich kombináciu) možno dosiahnuť jednoznačnú identifikáciu fyzickej osoby. To, s akou ľahkosťou či obťažnosťou možno danú fyzickú osobu identifikovať, odzrkadľuje tzv. mieru identifikovateľnosti, ktorá, rovnako ako spôsobený dopad v podobe zásahu do práv a slobôd, značne ovplyvňuje rizikovosť posudzovaného spracúvania.

WP29 označuje za rizikové spracúvanie tie činnosti, v ktorých sa operuje s „*citlivými údajmi alebo údajmi osobnej povahy*“ [12, s. 12]. Medzi citlivé údaje[29] sú radené najmä údaje uvedené v čl. 9 odst. 1 Nariadenia, ktorý sa venuje spracúvaniu tzv. zvláštnych kategórií údajov, ktoré odhaľujú: „*rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby*“, podobne sú popisované aj v bode 75 odôvodnenia Nariadenia, no zároveň sem spadajú aj údaje, ktoré sa považujú za citlivé v dôsledku ich prepojenia na súkromné aktivity osoby alebo údaje, ktorých napadnutie by malo vážny dopad na život dotknutej osoby.

V závislosti na rozsahu spracúvaných údajov aj samotné Nariadenie definuje niekoľko príkladov konkrétnych spracovateľských operácií, ktoré môžu viesť k vyššiemu riziku pre práva a slobody fyzických osôb. Čl. 35 Nariadenia odst. 3 písm. a) hovorí o „*systematickom a rozsiahlom hodnotení osobných aspektov*“. K pojmu „rozsiahle spracúvanie“ poskytuje vysvetlenie bod 91 odôvodnenia Nariadenia, ktorý stanovuje, že sa jedná o prípady „*spracúvania značného množstva osobných údajov na regionálnej, celoštátnej alebo nadnárodnej úrovni, ktoré by mohli mať dopad na veľký počet subjektov údajov*“. V nadväznosti na slová vyplývajúce z Nariadenia, WP29 odporúča pri posudzovaní rozsahu zohľadniť najmä faktory ako počet dotknutých osôb, ktorých sa spracúvanie týka, objem údajov, ktoré sa spracúvajú, doba trvania či stálosť procesu spracúvania a geografický rozsah realizovaného spracúvania [12, s. 11].

Účel spracovania

Posledným, no taktiež veľmi dôležitým faktorom, ktorý musí prevádzkovateľ brať pri posudzovaní rizík do úvahy, je účel, za ktorým je posudzované spracúvanie osobných

[29] V samotnom Nariadení sa pojem „citlivé údaje“ nepoužíva, no v českom i slovenskom právnom prostredí sa jedná o ustálenú terminológiu.

údajov realizované. Opäť ide o faktor, ktorý bude špecifický pre každý jedinečný proces spracúvania, čo znamená, že pri rôznom kontexte spracúvania nemusí určité napadnutie, či už v zmysle kompromitácie, modifikácie alebo zneprístupnenia spracúvaných osobných údajov spôsobiť vždy rovnakú ujmu.

Z hľadiska účelu teda možno jednotlivé spracovateľské operácie rozlíšiť na menej či viac rizikové. Príkladom spracúvania s vyššou mierou rizikovosti môže byť zaznamenávanie osobných údajov pre zabezpečenie zdravotnej starosti. Inou situáciou z bežného života môže byť taktiež spracúvanie osobných údajov za účelom riešenia rôznych otázok v oblastí financií fyzických osôb. Naopak za menej rizikové možno považovať spracúvanie údajov pre potreby marketingových spoločností, ktoré v záujme realizácie rôznych prieskumov či predstavovania komerčných produktov prejavujú snahu o kontaktovanie širokého okruhu ľudí.

3.1.2 Ujma

Proces posúdenia rizika poskytuje komplexnú analýzu zameranú na zistenie *možnej ujmy* z pohľadu subjektov údajov a *pravdepodobnosti*, s akou ujma môže vzniknúť [6, s. 249]. Po zohľadnení týchto dvoch identifikovaných parametrov sa ako výsledok procesu posudzovania získa výsledná hodnota rizika, ktorú dané spracúvanie predstavuje. Pod ujmou v kontexte tejto práce rozumieme porušenie záujmov subjektov údajov, tj. určité neželané výsledky spracúvania, ktoré budú mať za následok vznik zásahu do práv a slobôd subjektov spracúvaných údajov. Je dôležité podotknúť, že vznik ujmy nie je nutne viazaný na jeden konkrétny subjekt údajov, ktorého osobné údaje sú zahrnuté do procesu konkrétneho spracúvania s vysokou mierou rizikovosti. Vznik problému, ktorý rizikové spracúvanie prináša, sa môže preniesť medzi viaceré subjekty a prejaviť sa v podobe ujmy pre širšiu spoločnosť. Za názorný príklad možno označiť predvolebné obdobie, počas ktorého typicky dochádza k ovplyvňovaniu verejnosti šírením kandidačných kampaní vďaka dostupnosti osobných údajov širokého okruhu fyzických osôb. Z nedávnej praxe možno spomenúť situáciu, kedy došlo k odkúpeniu údajov, získaných prostredníctvom tretích strán zo sociálnej siete Facebook o desiatkach miliónov Američanov bez ich vedomia, spoločnosťou Cambridge Analytica [17][18], ktorá sa analýzou takto získaných údajov podieľala na profilovaní amerických voličov za účelom ovplyvnenia ich rozhodovania pri hlasovaní v amerických prezidentských voľbách v roku 2016.

Nariadenie vo svojom článku 5 postupne vymenúva základné zásady ochrany osobných údajov, ktoré je potrebné pre zabezpečenie zákonnosti spracúvania dodržať. Z hľadiska všeobecného posudzovania vzniku možnej nepriaznivej ujmy hroziacej v dôsledku

realizácie rizikového spracúvania osobných údajov má význam zamerať sa najmä na hodnotenie zabezpečenia a dodržania dôvernosti, integrity a dostupnosti systémov a služieb, zapojených do procesu spracúvania, a tým aj samotných spracúvaných údajov. Dokonca aj WP29 v jednom zo svojich usmernení venovanému riešeniu problematiky súvisiacej s ohlasovaním porušenia ochrany osobných údajov označuje túto trojicu vlastností za „*všeobecné zásady bezpečnosti informácií*“ [19, s. 7].

Dôvernosť

Narušenie dôvernosti spracúvaných údajov možno zaradiť do skupiny veľmi závažných spôsobov porušenia záujmov subjektov údajov, ktorý v dôsledku realizácie spracovateľských činnosti môže nastať. Pod narušením dôvernosti rozumieme situáciu, kedy dôjde k neoprávnenému alebo náhodnému poskytnutiu či prístupu k osobným údajom neoprávneným osobám [19, s. 7]. V závislosti na tom, aká osoba a s akým úmyslom získa neoprávnene alebo náhodne prístup k zaznamenaným údajom, musí následne dotknutá osoba zniesť rôzne závažné ujmy v podobe zásahu do jej práv či slobôd.

Integrita a presnosť

Pre zaistenie integrity musia byť osobné údaje chránené pred neoprávneným zničením, stratou či pozmenením [6, s. 293]. Zabezpečenie integrity osobných údajov je úzko späté s ďalšou zásadou spracovania osobných údajov, a to so zásadou dodržania ich presnosti[30]. Podľa tejto zásady musia byť spracúvané údaje presné, majú odpovedať skutočnosti a v prípade akejkoľvek zmeny je potrebná ich neodkladná aktualizácia.

Narušenie integrity spočíva v neoprávnenej alebo náhodnej zmene osobných údajov, čo by malo taktiež za následok narušenie presnosti spracúvaných údajov. V dôsledku toho môžu byť napr. o dotknutej osobe vedené nepravdivé informácie, ktoré môžu vyústiť v zníženie kvality jej bežného života. Ako príklad je možné uviesť situáciu, kedy by zamestnávateľ pri evidencii dochádzky nepresne zaznamenával časy príchodu a odchodu a v dôsledku takto chybne vedených informácií by mohlo zamestnancovi hroziť, na základe informácií zachytených v omylnom zázname o neplnení si povinností vyplývajúcich z pracovne-právneho vzťahu, zníženie platového ohodnotenia.

[30] Článok 5 odst. 1 písm. d) Nariadenia.

Dostupnosť

Za porušenie dostupnosti osobných údajov sa považuje ich strata alebo zničenie. WP29 považuje za v celku problematické určiť to, či je možné za narušenie dostupnosti považovať aj spôsobenú dočasnú nedostupnosť, ktorá bude mať za následok iný dopad, narozdiel od trvalého zničenia osobných údajov a tým pádom aj ich dostupnosti.

Nariadenie v čl. 32 odst. 2 písm. c) kladie dôraz na schopnosť prevádzkovateľa „*obnoviť dostupnosť osobných údajov a prístup k nim včas*“[31]. Z tejto formulácie je zrejmé, že v niektorých prípadoch môže mať čo i len dočasné narušenie dostupnosti za následok zásah do práv a slobôd subjektov údajov. Opäť je však potrebné analyzovať konkrétnu situáciu v rámci jedinečného kontextu spracúvania údajov. Príkladom vzniku kritických následkov v dôsledku narušenia dostupnosti údajov je oblasť zdravotníctva, kedy môže v prípadoch, kedy nie sú, čo i len dočasne, dostupné kritické lekárske údaje o pacientoch, dôjsť k ohrozeniu života týchto pacientov. [19, s. 8]

Zásah do práv a slobôd subjektov údajov

Nariadenie, ako jednotný prameň práva EÚ, mnohokrát hovorí o „*riziku pre práva a slobody fyzických osôb*“[32] a kladie si za cieľ zabezpečiť ochranu týchto fyzických osôb, čiže subjektov spracúvaných údajov. Pojem „práva a slobody“ však nie je v rámci Nariadenia bližšie konkretizovaný. Z tohto dôvodu umožňuje Nariadenie chrániť prakticky akékoľvek práva a slobody fyzických osôb. Vo všeobecnosti je akékoľvek nariadenie prijaté ako právny predpis v rámci EÚ takým právnym aktom, ktorý sa vo všetkých členských štátoch uplatňuje automaticky a jednotne ihneď po nadobudnutí svojej účinnosti bez nutnosti transponovania do národného právneho poriadku [20]. S odvolaním sa na túto skutočnosť je oprávnené tvrdiť, že Nariadenie, ako sekundárny prameň práva EÚ, sa snaží o ochranu všetkých tých práv a slobôd, ktoré sú garantované na rovnakej úrovni, tj. v rámci EÚ, vyššie postaveným, čiže primárnym právnym predpisom. Všeobecne aplikovaným „interným“ právnym predpisom na úrovni únioového práva je na základe článku 6 odst. 1 Zmluvy o Európskej únií Charta základných práv a slobôd, ktorá bola prijatá[33] v roku 2000 s cieľom zabezpečiť, súbežne s „vonkajším“ kontrolným mechanizmom v podobe akceptácie Európskeho dohovoru o ochrane ľudských práv a základných slobôd zo strany členských štátov EÚ, súlad právnych predpisov a politík s ochranou základných práv v rámci EÚ.

[31] Článok 32 odst. 2 písm. c) Nariadenia.
[32] Uvádza tak napr. bod 74 odôvodnenia Nariadenia.
[33] Charta EÚ nadobudla účinnosť až v roku 2009 spolu s prijatím Lisabonskej zmluvy.

Komplexný proces posúdenia rizík by bolo prakticky nemožné plnohodnotne vykonať pre všetkých 50 základných práv, ktoré sú Chartou EÚ garantované. Preto je na mieste opäť stanoviť istý spôsob kategorizácie práv, do ktorých by mohlo byť v dôsledku vzniku nepriaznivého rizika zasiahnuté. Taktiež Nariadenie v bode 75 odôvodnenia vymenúva dopady, ku ktorým by mohlo rizikové spracúvanie osobných údajov viesť, ako napríklad diskriminácia, krádež či zneužitie identity, poškodenie dobrého mena atď. Pre navrhovanú metodiku bola preto zo všetkých popísaných skutočností a s prihliadnutím na zoznam základných práv garantovaných Chartou EÚ nakoniec zvolená podľa vlastného uváženia kategorizácia práv do troch základných skupín, ktoré zahŕňajú základné práva vzhľadom k ich zaradeniu do príslušnej oblasti života človeka. Sú nimi:

- osobnosť človeka, kam spadá právo na:
  - život,
  - nedotknuteľnosť osoby,
  - súkromie človeka[34]
    - rešpektovanie súkromného a rodinného života,
    - právo človeka na informačné sebaurčenie,
    - právo na ochranu listového tajomstva apod.;
- postavenie človeka v spoločnosti, kam spadá právo na:
  - nediskrimináciu,
  - vlastníctvo majetku,
  - prístup k službám zamestnanosti,
  - zdravotnú starostlivosť;
- verejnoprávne politické práva, kam spadá právo na:
  - slobodné voľby.

Uvedené práva sú tými, k porušeniu ktorých dochádza pri bežných činnostiach prevádzkovateľa najčastejšie. Každý jeden proces spracúvania osobných údajov je však do istej miery jedinečný a na základe príslušného kontextu spracúvania špecifický, a preto by sám prevádzkovateľ mal zvážiť, na aké práva a slobody bude prihliadať. Všeobecným odporučením môže byť nahliadnutie na práva z hľadiska oblastí ľudského života, ktoré sú definované názvami prvých 6 hláv Charty EÚ[35].

[34] Hlavnou podstatou uplatňovania práva na ochranu súkromia je zabezpečenie ochrany identity človeka. Tu možno vidieť prepojenie s problematikou výskytu rizika pri spracúvaní osobných údajov. Pochybenie v ochrane spracúvaných údajov by mohlo mať za následok napr. ich kompromitáciu (ako jeden z možných dôsledkov rizikového spracúvania) a po úniku týchto údajov by bolo napr. možné dotknutú fyzickú osobu identifikovať, čím by bolo narušené právo na ochranu jej súkromia.

[35] Patria sem dôstojnosť, slobody, rovnosť, solidarita, občianstvo a spravodlivosť.

3.2 Rovina posúdenia informačnej bezpečnosti

Za rovinou spracúvania osobných údajov, ktorá je v kontexte tejto práce prioritnou, prebiehajú na pozadí procesy sprostredkujúce samotnú realizáciu jednotlivých činností spracúvania. V tomto kontexte je potrebné venovať pozornosť povinnosti prevádzkovateľa viažucej sa k dodržiavaniu opatrení nevyhnutných pre zaistenie bezpečnosti ním prevádzkovaných informačných systémov. Aj v tejto rovine musí prevádzkovateľ uskutočniť proces posúdenie rizík a na základe jeho výsledkov prijať potrebné opatrenia, aby nedochádzalo k prelomeniu samotného zabezpečenia, ktorého úlohou je, okrem iného, poskytovať ochranu zaznamenaných osobných údajov.

3.2.1 Identifikácia rizík

ČSN ISO 27005:2013 poskytuje definíciu rizika bezpečnosti informácií, ktoré je pre túto prácu kľúčové. Riziko bezpečnosti informácií sa vyjadruje ako *„kombinácia následkov udalosti bezpečnosti informácií a s ňou súvisiacou pravdepodobnou možnosťou výskytu*“ [2, s. 10]. Je teda zrejmé, že miera rizika bude z jednej časti ovplyvnená tým, či vôbec môže nastať udalosť, ktorá by spôsobila odklon od očakávaného priebehu činnosti[36].

Za hlavný cieľ identifikačnej fázy v oblasti riadenia informačnej bezpečnosti možno považovať určenie toho, čo by sa muselo stať, aby bola spôsobená potenciálna strata, a taktiež porozumieť tomu, ako, kde a prečo môže táto strata nastať [2, s. 19]. V rámci kap. 2.4 bol uvedený podrobný popis priebehu vzniku nepriaznivého rizika. Vo fáze identifikácie rizík je teda potrebné zamerať sa na existujúce zdroje rizika a podporné aktíva, ktorých zraniteľnosti by mohli zdroje rizika využiť pre realizáciu hrozby.

3.2.2 Zdroj rizika a hrozba

Za zdroj rizika sa považuje akýkoľvek prvok, ktorý môže sám alebo spoločne s inými prvkami zapríčiniť vznik rizika [21, s. 12]. Takýto prvok môže teda pôsobením na zraniteľnosť aktíva (viď ďalej) realizovať hrozbu. Zdrojom rizika môže byť prakticky čokoľvek, a tak nie je možné definovať jeho konkrétnu podobu. Zoznam identifikovaných zdrojov rizík bude pre každú organizáciu jedinečný z dôvodu špecifického zamerania jej činnosti. Pre univerzálnosť navrhovanej metodiky je vhodné zaviesť aspoň všeobecnú klasifikáciu zdrojov rizika a nimi realizovaných hrozieb. Podľa úmyslu zdroja rizika realizovať hrozbu ich možno rozdeliť na (i) úmyselné (napr. špionáž, odposluch, krádež),

[36] Očakávaným priebehom činnosti v kontexte tejto práce je taký priebeh spracúvania, v rámci ktorého je dodržané zabezpečenie ochrany spracúvaných osobných údajov s cieľom zamedziť vzniku nepríjemností v zmysle nepriaznivého zásahu do práv a slobôd subjektov údajov.

(ii) náhodné (napr. náhle zlyhanie funkčnosti zariadenia) a (iii) environmentálne (rôzne prírodné udalosti) [2, s. 43 – 44]. Zdroj rizika môže teda hrozbu realizovať z vnútorného (zamestnanci) alebo vonkajšieho (adresáti spracúvaných údajov, tretie strany) prostredia organizácie, alebo môže mať hrozba aj takú podobu, za ktorej realizáciou nestojí žiadna konkrétna osoba (malware a iné hrozby pre prevádzkovaný software; ohrozenie hardware prírodným živlom – požiar, záplava) [16, s. 3].

Po realizácií tohto kroku by mala každá organizácia dospieť k vytvoreniu katalógu zdrojov rizík, ktoré by mohli využiť zraniteľnosti podporných aktív. Vo vytvorenom katalógu by mali byť zdroje rizika popísané čo najpodrobnejšie. Najmä pre úmyselné hrozby je potrebné viesť záznamy o tom, aká je motivácia pre realizáciu takejto hrozby a aké rôzne akcie a nepriaznivé dôsledky môžu byť výsledkom jej realizácie [22, s. 13].

3.2.3 Podporné aktíva a ich zraniteľnosti

Pod pojem „podporné aktívum“ možno zaradiť čokoľvek, čo má pre organizáciu určitú hodnotu, ktorá môže byť narušená a zmenšená pôsobením hrozby, a preto je potrebná jeho ochrana [1, s. 96], [2, s. 19]. Ide o všetky také prvky informačného systému, ktoré sa určitým spôsobom podieľajú na procese spracúvania údajov [16, s. 2].

Podporné aktíva organizácie je možné rozklasifikovať podľa ich typu do viacerých kategórií, napr.: hardware, software, siete a informačné kanály, zamestnanci a pracovníci, lokalita, samotná organizácia a jej štruktúra [2, s. 35]. Metodika PIA od dozorného úradu CNIL ďalej zavádza aj ďalšie kategórie, ktorých význam je pri spracúvaní osobných údajov neopomenuteľný. Sú nimi napríklad dokumenty v papierovej podobe nesúce osobné údaje, pričom tiež berie do úvahy možné spôsoby prenosu týchto papierových dokumentov. Pri návrhu metodiky tejto práce boli zohľadnené aj kategórie podporných aktív uvádzané metodikou PIA, no po ich prepojení s odporúčaniami normy ISO 27005:2013 bolo navrhnuté rozdelenie do dvoch hlavných kategórií, ktorými sú (i) technické podporné aktíva (tj. prevádzkovaný informačný systém) a (ii) organizačné podporné aktíva. Každá z týchto kategórií je následne rozčlenená na konkrétnejšie podskupiny podporných aktív. Navrhnuté rozdelenie prevádzkovaných podporných aktív zobrazujú tab. 3.1 a tab. 3.2.

Tab. 3.1: Kategorizácia technických podporných aktív.

TECHNICKÉ PODPORNÉ AKTÍVA	
hardware	zariadenia realizujúce spracúvanie dát
	podporné zariadenia
	nosiče dát
	úložiská dát
software	operačný systém
	serverová infraštruktúra
	softwarové balíky využívané pre spracúvanie dát
prostriedky umožňujúce prenos dát	siete
	informačné kanály
bezpečnostné prvky	zabezpečovacie a kamerové systémy

Tab. 3.2: Kategorizácia organizačných podporných aktív.

ORGANIZAČNÉ PODPORNÉ AKTÍVA	
pracovníci[37]	osoby realizujúce spracúvanie dát
	užívatelia
	vývojári a technická podpora
	osoby realizujúce dohľad nad zabezpečením
papierové dokumenty obsahujúce zaznamenané dáta	operácie spojené s tvorbou, údržbou a likvidáciou papierových dokumentov
	spôsoby prenosu papierových dokumentov
lokalita	vonkajšie prostredie organizácie
	budovy a priestory

[37] Pod pojmom „pracovníci“ si možno predstaviť kategóriu zahŕňajúcu všetky také osoby, ktorým môže byť akýmkoľvek spôsobom umožnený prístup k spracúvaným údajom.

3.3 Analýza rizík

Riziko ako výsledný produkt vzniká prepojením oboch popísaných oblastí – roviny spracúvania osobných údajov a roviny riadenia rizík informačnej bezpečnosti. V nasledujúcich fázach posúdenia rizík činností spojených so spracúvaním osobných údajov budú už obe roviny popisované viac-menej súčasne. Stále je však potrebné vnímať samotné spracúvanie ako akýsi „povrchový" proces, za ktorým ale musí byť zo strany prevádzkovateľa zaisťovaná taktiež bezpečnosť ním prevádzkovaných informačných systémov.

V kapitole 2.4 bolo popísané, akým spôsobom sa pristupuje k stanoveniu výslednej hodnoty rizika. Táto hodnota, resp. veľkosť rizika je vyjadrená ako funkcia hodnôt *pravdepodobnosti* naplnenia nepriaznivých udalostí a ich následkov, teda *závažnosti* dopadu, ktorý sled takýchto udalostí zapríčiní.

Identifikačná fáza, popísaná v predchádzajúcej kapitole, poskytuje prevádzkovateľovi uskutočňujúcemu proces posudzovania rizík prehľad o tom, aké riziká môže sledované spracúvanie údajov vyvolať. Každé riziko vzniká ako jedinečný sled udalostí: zdroj rizika realizuje hrozbu pôsobením na zraniteľnosť podporného aktíva, čím vyvolá určitý dopad, ktorým je v kontexte tejto práce ujma spôsobená subjektom spracúvaných údajov, teda zásah do ich práv a slobôd (táto skutočnosť bola zachytená na obr. 2.1). Všetky vymenované prvky reťazca, ktoré stoja za vznikom rizika, boli identifikované už vo fáze predchádzajúcej. Cieľom analytickej fázy je teda takto identifikovanému riziku priradiť konkrétnu úroveň v závislosti na jeho pravdepodobnosti a závažnosti. Pravdepodobnosť vzniku rizika je pritom zložená z hodnôt miery zraniteľnosti podporného aktíva a miery relevancie hrozby, ktoré sa viažu k posudzovaniu a zaisteniu informačnej bezpečnosti, a závažnosť tohto rizika závisí na miere identifikovateľnosti subjektov údajov a tiež na intenzite zásahu do ich práv a slobôd.

Táto práca, z dôvodu primeranej subjektivity pri hodnotení dopadu rizika (viď tiež kap. 1.2.1), využíva kvalitatívnu metriku analýzy rizík. Dielčie hodnoty pravdepodobnosti a závažnosti nebudú získané z presných hodnôt vyplývajúcich z činností organizácie, ale budú stanovené vo forme slovného vyjadrenia na základe určitého opodstatneného kvalifikovaného odhadu.

3.3.1 Pravdepodobnosť rizika

Pravdepodobnosť – relevancia hrozby

Každý potenciálny zdroj rizika zaradený do katalógu, ktorý je produktom identifikačnej fázy riadenia informačnej bezpečnosti, môže využiť nejakú zraniteľnosť podporného

aktíva a týmto spôsobom realizovať hrozbu. Je preto potrebné odhadnúť, aká je pravdepodobnosť toho, že táto skutočnosť bude realizovaná. Parameter, ktorý túto hodnotu udáva, je označovaný pojmom relevancia hrozby. Táto metodika navrhuje tri základné úrovne pre ohodnotenie relevancie hrozby, ktoré sú zobrazené v tab. 3.3.

Tab. 3.3: Relevancia hrozby.

Relevancia hrozby	Vysoká	Očakáva sa výskyt hrozby, je veľmi pravdepodobné, že dôjde k realizácií hrozby pôsobením na zraniteľnosť podporného aktíva; v minulosti boli prítomné incidenty alebo štatistiky alebo ďalšie informácie, ktoré indikujú, že sa táto hrozba pravdepodobne vyskytne, alebo existujú vážne dôvody alebo motivácie pre útočníka vykonať túto hrozbu.
	Stredná	Výskyt hrozby je pravdepodobný; v minulosti boli incidenty alebo štatistiky, alebo ďalšie informácie, ktoré indikujú, že táto alebo podobné hrozby sa vyskytli niekedy v minulosti, alebo existuje indikácia že by mohli existovať pre útočníka nejaké dôvody vykonať takúto hrozbu.
	Nízka	Je nepravdepodobné, že sa hrozba objaví, nevyskytli sa incidenty, štatistiky , motívy atď. ktoré by indikovali, že hrozba nastane.

Popisovaný spôsob ohodnotenia hrozby je možné použiť v prípade neúmyselných, čiže náhodných a environmentálnych hrozieb. V prípade druhej skupiny, a to hrozieb úmyselných, je potrebné, aby prevádzkovateľ spracúvania pri posudzovaní zvážil navyše ešte aj motiváciu zdroja hrozby úmyselne zapôsobiť na zraniteľnosť podporného aktíva.

Pravdepodobnosť – zraniteľnosť aktíva

Druhou z potrebných hodnôt pre určenie pravdepodobnosti výskytu rizika je miera zraniteľnosti podporného aktíva. Všetky potenciálne zraniteľné aktíva zapojené do procesu spracúvania a ich identifikované zraniteľnosti sú taktiež výstupom predchádzajúcej identifikačnej fázy. Rovnako ako aj v prípade určovania relevancie hrozby navrhuje táto metodika tri základné úrovne kvalitatívneho ohodnotenia zraniteľnosti aktíva zapojeného do realizácie činností spracúvania údajov, ktoré sú zobrazené v tab. 3.4.

Tab. 3.4: Zraniteľnosť aktíva.

Zraniteľnosť aktíva	Vysoká	Je jednoduché využiť zraniteľnosť; sú implementované slabé alebo žiadne opatrenia pre zabezpečenie aktíva.
	Stredná	Zraniteľnosť by mohla byť využitá; sú implementované isté bezpečnostné opatrenia.
	Nízka	Je obtiažne zraniteľnosť využiť; sú implementované kvalitné bezpečnostné opatrenia.

Určenie výslednej hodnoty pravdepodobnosti

Metodika PIA od CNIL [16, s. 6] navrhuje štyri základné úrovne pre kategorizáciu pravdepodobnosti na základe jej istého kvantitatívneho ohodnotenia. Táto práca nemá dôvod zavádzať inú stupnicu, nakoľko rozdelenie hodnôt pravdepodobnosti realizácie incidentu, v ktorého dôsledku by bolo zasiahnuté do práv a slobôd subjektov údajov, do štyroch oddelených úrovní sa zdá byť postačujúce. Tab. 3.5 zachytáva spôsob určenia výslednej hodnoty pravdepodobnosti identifikovaného rizika v závislosti na rôznych kombináciách hodnôt priradeným parametrom relevancie hrozby a zraniteľnosti aktíva. Na základe priradenej hodnoty pravdepodobnosti je možné každé identifikované riziko zaradiť do jednej zo štyroch základných úrovní. Rozčlenenie na jednotlivé úrovne približuje tab. 3.6, každej z týchto úrovní potom pripadá príslušný popis v tab. 3.7.

Tab. 3.5: Určenie výslednej hodnoty pravdepodobnosti rizika.

	Zraniteľnosť aktíva	N	S	V
Relevancia hrozby	Nízka	1	2	3
	Stredná	2	3	4
	Vysoká	3	4	5

Tab. 3.6: Pravdepodobnosť rizika.

Výsledná hodnota relevancia hrozby x miera zraniteľnosti	**Pravdepodobnosť incidentu**
≤ 2	Zanedbateľná (1)
3	Nízka (2)
4	Stredná (3)
5	Vysoká (4)

Tab. 3.7: Pravdepodobnosť rizika.

Pravdepodobnosť	Zanedbateľná (1)	Pre identifikované zdroje rizika sa javí ako nemožné využiť zraniteľnosť podporných aktív, a spôsobiť tak hrozbu.
	Nízka (2)	Pre identifikované zdroje rizika sa je náročné využiť zraniteľnosť podporných aktív, a spôsobiť tak hrozbu.
	Stredná (3)	Je možné, že identifikované zdroje rizika dokážu využiť zraniteľnosť podporných aktív, a spôsobiť tak hrozbu.
	Vysoká (> 3)	Pre identifikované zdroje rizika sa je jednoduché využiť zraniteľnosť podporných aktív, a spôsobiť tak hrozbu

V rámci posudzovanej spracovateľskej operácie bude, veľmi pravdepodobne, odhalená možnosť vzniku rizika na viacerých podporných aktívach, pričom každé z týchto aktív môže mať jednu či viac zraniteľností, ktoré môžu byť využité rozličnými identifikovanými hrozbami. Určenie hodnoty pravdepodobnosti, ako funkciu hodnôt zraniteľnosti aktíva a relevancie hrozby, je potrebné realizovať pre každé jedno zo zoznamu identifikovaných rizík. Pre každé z týchto rizík je následne potrebné určiť ešte aj hodnotu závažnosti dopadu v dôsledku jeho uskutočnenia, aby bolo nakoniec možné získať ako výstup procesu posudzovania rizík kompletný zoznam rizík s im priradenými výslednými hodnotami. Proces určenia jednotlivých dielčích hodnôt pravdepodobností rizika pre konkrétne identifikované zraniteľnosti a možné hrozby znázorňuje tab. 3.8.

Tab. 3.8: Určovanie pravdepodobnosti rizika realizáciou hrozby na identifikovanú zraniteľnosť podporného aktíva.

Aktívum	Hrozba	Relevancia hrozby	Najpravdepodobnejšia zraniteľnosť	Miera zraniteľnosti	Pravdepodobnosť
Aktívum 1	Hrozba 1A	N/S/V	Zraniteľnosť A	N/S/V	P_{1A}
	Hrozba 1B	N/S/V	Zraniteľnosť B	N/S/V	P_{1B}
Aktívum 2	Hrozba 2A	N/S/V	Zraniteľnosť A	N/S/V	P_{2A}
	Hrozba 2B	N/S/V	Zraniteľnosť B	N/S/V	P_{2B}
	Hrozba 2C	N/S/V	Zraniteľnosť C	N/S/V	P_{2C}
Aktívum 3	Hrozba 3A	N/S/V	Zraniteľnosť A	N/S/V	P_{3A}
…	…	…	…	…	
Aktívum *n*	Hrozba *n*A	N/S/V	Zraniteľnosť A	N/S/V	P_{nA}

3.3.2 Závažnosť rizika

Závažnosť odzrkadľuje dopad, ktorý vyvolaný incident, tj. situácia, kedy zdroj rizika zapôsobí na zraniteľnosť podporného aktíva, čím vyvolá hrozbu, spôsobí. Metodika PIA od CNIL [7, s. 12 – 13] navrhuje určovať potenciálny dopad na základe dvoch hlavných faktorov. Prvým z nich je miera jednoduchosti (resp. obťažnosti) identifikácie subjektu na základe dotknutých spracúvaných dát. Ako druhý faktor je uvedený dopad, ktorý vyvolaný incident spôsobí. V kontexte spracúvania osobných údajov hovoríme o závažnosti ujmy, ktorú budú pociťovať dotknuté subjekty údajov v dôsledku zásahu do ich práv a slobôd. K popísanému dvojzložkovému určeniu hodnoty závažnosti rizika sa prikláňa aj navrhovaná metodika, a preto bude preberať postupy pri určovaní miery identifikovateľnosti a intenzity zásahu z uvedených východiskových materiálov.

Závažnosť – miera identifikovateľnosti

Pri spracúvaní akýchkoľvek kategórií osobných údajov je vždy nutné posúdiť, či vôbec, a ak áno, tak do akej miery, je zo znalosti spracúvaných údajov možné identifikovať konkrétnu fyzickú osobu. Pri posudzovaní možnosti identifikácie konkrétnej osoby je pritom

nutné uvažovať nielen jednotlivé osobné údaje ako samostatné identifikátory, ale taktiež ich rôzne kombinácie, pomocou ktorých je možno jednoznačne určiť danú dotknutú osobu. Vytvorená metodika, s prihliadnutím na odporúčania stanovené metodikou PIA, zavádza kvalifikované ohodnotenie miery identifikovateľnosti do štyroch úrovní, ako je naznačené aj v tab. 3.9.

Tab. 3.9: Miera identifikovateľnosti subjektov údajov. [7]

Identifikácia	Zanedbateľná (1)	Identifikovať subjekt s využitím spracúvaných údajov je takmer nemožné; získanie ďalších potrebných údajov k identifikácii je takmer nemožné.
	Nízka (2)	Identifikovať subjekt s využitím spracúvaných údajov je takmer nemožné; získanie ďalších potrebných údajov k identifikácii by bolo možné s vynaložením väčšieho úsilia.
	Stredná (3)	Identifikovať subjekt s využitím spracúvaných údajov je takmer nemožné; získanie ďalších potrebných údajov k identifikácii by bolo možné a jednoduché.
	Vysoká (4)	Identifikovať subjekt s využitím spracúvaných údajov je možné bez vynaloženia akéhokoľvek dodatočného úsilia.

Závažnosť – intenzita zásahu do práv a slobôd

Pri posudzovaní dopadu na práva a slobody subjektov údajov posudzujeme mieru ujmy, ktorá im v dôsledku nekorektného priebehu spracúvania osobných údajov vznikla. Táto metodika[38] navrhuje zohľadniť tri základné druhy ujmy, ktoré môže poškodený subjekt údajov, v prípade zásahu do jeho práv a slobôd, znášať:

- fyzická ujma (materiálne straty, škody spôsobené na fyzickom majetku);
- materiálna ujma (vznik straty alebo ušlého zisku vzhľadom na zapojené aktíva);
- psychická ujma (fyzické či emocionálne ťažkosti).

[38] Opäť podobne ako metodika PIA od CNIL [7, s. 13].

Tab. 3.10: Intenzita dopadu na práva a slobody subjektov údajov. [7]

Dopad	Zanedbateľný (1)	Dotknuté subjekty nebudú ovplyvnené alebo môžu pociťovať isté nepríjemnosti, ktoré ale dokážu bez problémov prekonať.
	Nízky (2)	Dotknuté subjekty môžu pociťovať značné nepríjemnosti, ktoré ale dokážu po vynaložení úsilia prekonať.
	Stredný (3)	Dotknuté subjekty môžu pociťovať výrazné nepríjemnosti, ktoré ale dokážu po vynaložení veľkého úsilia prekonať.
	Vysoký (4)	Dotknuté subjekty môžu pociťovať výrazné, dokonca až nezvratné nepríjemnosti a následky, ktoré nemusia byť schopné prekonať ani po vynaložení nadmerného úsilia.

Určenie výslednej hodnoty závažnosti

Výsledná hodnota závažnosti vzniknutého incidentu je určená kombináciou hodnôt určených v predchádzajúcich krokoch. Určenie hodnoty závažnosti v závislosti na miere identifikácie konkrétnej fyzickej osoby a nepriaznivého dopadu na práva a slobody zobrazuje tab. 3.11. Následná klasifikácia možných hodnôt závažnosti, opäť do štyroch ohraničených úrovní, na základe pridelenej hodnoty je zachytená v tab. 3.12.

Tab. 3.11: Určenie výslednej hodnoty závažnosti rizika.

	Dopad	Z	N	S	V
Identifikácia	Zanedbateľná	1	2	3	4
	Nízka	2	3	4	5
	Stredná	3	4	5	6
	Vysoká	4	5	6	7

Tab. 3.12: Závažnosť rizika.

Výsledná hodnota identifikácia x dopad	Závažnosť incidentu
≤ 3	Zanedbateľná (1)
4	Nízka (2)
5	Stredná (3)
> 5	Vysoká (4)

3.4 Výsledné riziko

Výsledným produktom navrhnutej metodiky pre posudzovanie rizík je zoznam všetkých identifikovaných rizík s príslušnou hodnotou, ktorá im je priradená v poslednom kroku popísaného procesu aplikáciou tzv. súčtovej matice rizík (viď tab. 3.13) na stanovené hodnoty závažnosti a pravdepodobnosti vzniku jednotlivých rizík získaných v predchádzajúcich krokoch posúdenia. Súčtové matice sú v riadení rizík považované za štandard a ich využitie je doporučené aj mnohými medzinárodnými normami, akou je napríklad ISO 31010:2010 [21, s. 82]. Táto riziková matica sa aplikuje na každé jedno identifikované riziko, ktoré bolo v priebehu celého procesu posudzované, a pre každé z týchto rizík zobrazuje jeho konečné ohodnotenie stanovené ako súčin identifikovaných hodnôt jeho pravdepodobnosti a závažnosti. Na základe takto určenej hodnoty možno jednotlivé riziká kategorizovať do štyroch hlavných skupín, ktoré možno ďalej konkrétnejšie deliť, tak, ako je zobrazené v tab. 3.14, a každému riziku možno taktiež priradiť slovný popis odzrkadľujúci jeho závažnosť (viď tab. 3.15).

Tab. 3.13: Určenie výslednej hodnoty rizika pomocou rizikovej matice.

závažnosť					
	V (4)	4	8	12	16
	S (3)	3	6	9	12
	N (2)	2	4	6	8
	Z (1)	1	2	3	4
		Z (1)	N (2)	S (3)	V (4)
		pravdepodobnosť			

Tab. 3.14: Klasifikácia rizík.

			Hodnota rizika
Zaradenie rizika	Vysoké riziko	Veľmi vysoké riziko	> 15
		Vysoké riziko	13 – 15
	Stredné riziko	Vyššie riziko	10 – 12
		Stredné riziko	8 – 9
	Nízke riziko	Nízke riziko	4 – 7
	Veľmi nízke riziko	Veľmi nízke riziko	2 – 3
		Zanedbateľné riziko	1

Tab. 3.15: Popis rizika na základe výslednej hodnoty tohto rizika.

Úroveň rizika	**Hodnota rizika**	**Popis**
Vysoké riziko	13 – 16	Riziko je neprípustné a musia byť okamžite zahájené kroky k jeho odstráneniu, tj. je potrebné okamžite zaviesť opatrenia pre odstránenie rizika.
Stredné riziko	8 – 12	Riziko je dlhodobo neprípustné a musia byť zahájené systematické kroky k jeho odstráneniu, tj. je potrebné zaviesť opatrenia pre odstránenie rizika.
Nízke riziko	4 – 7	Riziko môže byť znížené zavedením menej náročných opatrení alebo v prípade vyššej náročnosti zavedených opatrení môže byť riziko považované za prijateľné.
Veľmi nízke riziko	1 – 3	Riziko je považované za prijateľné

3.5 Porovnanie navrhnutej metodiky s metodikou PIA

Ako už v predchádzajúcom texte odznelo, výsledným produktom posudzovania rizík je kompletný zoznam identifikovaných rizík, ktorým bolo v priebehu procesu posúdenia pridelené príslušné ohodnotenie odzrkadľujúce ich pravdepodobnosť a závažnosť. Táto výsledná hodnota rizika je pre prevádzkovateľa posudzovaného spracúvania osobných údajov referenčným ukazovateľom, na základe ktorého vyhodnocuje nutnosť prijímania adekvátnych opatrení pre ošetrenie možných rizík. Navrhnutá metodika kategorizuje ohodnotené rizika do štyroch hlavných skupín (viď tab. 3.14) a z popisu jednotlivých kategórií je zrejmé, kedy a v akom rozsahu je nutné nápravné opatrenia zavádzať.

V úvode kapitoly, ešte pred samotným popisom navrhnutej metodiky, bolo poznamenané, že jedným z hlavných východiskových materiálov pre jej zostavenie bola metodika PIA od CNIL. Táto metodika taktiež zavádza štyri hlavné kategórie rizík, do ktorých sú jednotlivé riziká zaradené podľa výslednej hodnoty [7, s. 21]. Avšak nutnosť prijímania nápravných opatrení pri realizácii ošetrení rizík definuje rôzne jednak v závislosti na

miere pravdepodobnosti rizika a inak v závislosti na jeho závažnosti, tak ako naznačuje tab. 3.16. Nutnosť prijímania nápravných opatrení potom korešponduje s popisom jednotlivých kategórií rizík uvedeným v tab. 3.15, ktorá bola vytvorená špeciálne pre navrhovanú metodiku tejto práce.

Tab. 3.16: Klasifikácia rizík podľa metodiky PIA. [7]

<table>
<tr><td rowspan="4">závažnosť</td><td>V (4)</td><td colspan="2" rowspan="2">Riziko s nízkou pravdepodobnosťou ale vysokou závažnosťou</td><td colspan="2" rowspan="2">Riziko s vysokou pravdepodobnosťou a vysokou závažnosťou
(„vysoké riziko“)</td></tr>
<tr><td>S (3)</td></tr>
<tr><td>N (2)</td><td colspan="2" rowspan="2">Riziko s nízkou závažnosťou a nízkou pravdepodobnosťou
(„veľmi nízke riziko“)</td><td colspan="2" rowspan="2">Riziko s nízkou závažnosťou, ale vysokou pravdepodobnosťou</td></tr>
<tr><td>Z (1)</td></tr>
<tr><td></td><td></td><td>Z (1)</td><td>N (2)</td><td>S (3)</td><td>V (4)</td></tr>
<tr><td colspan="2"></td><td colspan="4">pravdepodobnosť</td></tr>
</table>

4 APLIKÁCIA METODIKY NA KONKRÉTNU ČINNOSŤ SPRACÚVANIA ÚDAJOV

Nasledujúca časť uvádza názorný príklad práce s navrhnutou metodikou. Nejedná sa o komplexné posúdenie rizík v konkrétnom procese spracúvania osobných údajov. Jedná sa len o jednoduchú ukážku slúžiacu pre lepšie pochopenie realizácie jednotlivých krokov posúdenia, ktoré boli podrobne popísané v predchádzajúcej kapitole.

4.1 Popis situácie

Zamestnávateľ spracúva osobné údaje svojich zamestnancov pre účely zabezpečenia *Bezpečnosti a ochrany zdravia pri práci* v zmysle plnenia vlastnej zákonnej povinnosti vyplývajúcej zo zákona č. 309/2006 Sb. o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci.

Pre naplnenie daného účelu sú zaznamenávané nasledovné osobné údaje – meno a priezvisko zamestnanca, titul, pridelené identifikačné číslo, pracovná pozícia. Evidencia pracovnej doby zamestnancov prebieha prostredníctvom softwarovej aplikácie, zamestnanci zaznamenávajú svoj príchod a odchod do zamestnania priložením zamestnaneckej karty na elektronický terminál pri hlavnom vchode do objektu výkonu povolania. Záznamy sú uložené centralizovane na serverovom úložisku zamestnávateľa.

V prípade výskytu incidentu v podobe pracovného úrazu sa spisuje záznam o úraze, ktorý je zamestnanec povinný potvrdiť svojím podpisom. Následne je záznam o pracovnom úraze postúpený ďalším príslušným inštitúciám.

4.2 Identifikácia rizík

Nakoľko ide len o názornú ukážku aplikácie navrhnutej metodiky, nebude záverom tejto fázy kompletný zoznam identifikovaných rizík, akoby tomu bolo v skutočnosti pri posudzovaní obdobnej situácie. Pre naplnenia primárneho účelu, ktorým je priblížiť čitateľovi jednotlivé kroky posudzovania rizík, bude uvedených v každej dielčej časti identifikačnej fázy len niekoľko vybraných príkladov.

Kontext spracovania údajov

V prípade, že nastane pracovný úraz zamestnanca pri vykonávaní jeho povinností vyplývajúcich z pracovne-právneho vzťahu uzavretého so zamestnávateľom, je podľa § 269

odst. 1 zákona č. 262/2006 Sb.[39] zamestnávateľ povinný nahradiť zamestnancovi vzniknutú škodu alebo nemajetkovú ujmu. Preto je nutné viesť evidenciu o pracovných úrazoch zamestnancov, ktoré nastanú pri plnení ich pracovných povinností počas pracovnej doby.

Táto práca si nekladie za cieľ vysvetliť celý priebeh kompenzačného procesu, od vzniku pracovného úrazu až po úhradu vzniknutej škody. Pre účely tejto práce budú dôležité len niektoré významné body celého procesu. Prvým významným krokom je spísanie záznamu ihneď po vzniku pracovného úrazu. Tento záznam obsahuje nasledujúce osobné údaje poškodeného zamestnanca, ktorému sa pracovný úraz stal: meno a priezvisko, adresa bydliska a identifikačný údaj, tj. rodné číslo zamestnanca, ďalej presný čas vzniku pracovného úrazu a jasne zrozumiteľný priebeh a popis úrazu[40].

Pre stanovenie kontextu spracúvania je taktiež potrebné vymedziť tretie strany, tj. ďalšie subjekty, ktorým budú zaznamenané osobné údaje komunikované. Pri bežnom postupe ohlasovania vzniku pracovného úrazu je záznam o tomto úraze, spolu s príslušnými údajmi o zamestnancovi, komunikovaný ďalším príslušným inštitúciám, ako sú inšpektorát práce, sociálna poisťovňa a zdravotná poisťovňa.

Možná ujma

Zamestnanec má po vzniku pracovného úrazu nárok na odškodnenie primerané k povahe ujmy, ktorú v dôsledku pracovného úrazu utrpel. Pre potreby tejto práce uvažujme situáciu, kedy nastal pracovný úraz, ktorým bola spôsobená práceneschopnosť zamestnanca bez smrteľných úrazov a úrazov s ťažkou ujmou na zdraví. V tejto situácií má zamestnanec nárok na primerané odškodnenie v podobe finančnej kompenzácie od príslušnej zákonnej poisťovne, s ktorou má zamestnávateľ uzavretý poistne-právny vzťah na základe Vyhlášky č. 125/1993. Sb.[41] Príslušnej poisťovni musí byť doručený záznam o pracovnom úraze a tá následne presne vymedzeným postupom preverí okolnosti, na základe ktorých obdržanú žiadosť o priznanie odškodného potvrdí alebo zamietne. [23]

Jednou z podstatných skúmaných okolností je čas vzniku incidentu, ktorý zapríčinil pracovný úraz. Za pracovný úraz je možné považovať len taký úraz, ktorý nastal počas pracovnej doby. Pri elektronickej evidencii dochádzky zamestnancov je preto potrebné zabezpečiť nastavenie správneho aktuálneho času pre potreby presného záznamu pracovnej doby jednotlivých zamestnancov.

---

[39] Tzv. zákoník práce.

[40] Pri preverovaní pracovného úrazu pre priznanie odškodnenia zamestnancovi je príslušná zákonná poisťovňa oprávnená zisťovať aj ďalšie osobné údaje zamestnanca, napr. údaje o zdravotnom stave.

[41] Vyhláška ministerstva financí, kterou se stanoví podmínky a sazby zákonného pojištění odpovědnosti organizace za škodu při pracovním úrazu nebo nemoci z povolání.

V prípade nedodržania tejto povinnosti môže nastať situácia, kedy by zdokumentovaný záznam o pracovnom úraze obsahoval isté, správne údaje o čase vzniku incidentu, no vzhľadom na nepresnosť systému pre evidenciu dochádzky by to bolo práve v čase, kedy by z dôvodu chybného nastavenia času v systéme nebol zamestnanec evidovaný v dochádzke. Tým pádom by poisťovňa pri overovaní incidentu usúdila, že incident sa nestal počas pracovnej doby zamestnanca. Zamestnancovi by v tejto situácií vznikla ujma v podobe nepriznania odškodného za utrpený pracovný úraz.

Podporné aktíva, ich zraniteľnosti a možné hrozby

Evidencia dochádzky zamestnancov prebieha prostredníctvom elektronického terminálu, ktorý využíva istý typ softwarovej aplikácie určenej priamo pre zaznamenávanie časov príchodu a odchodu zamestnancov z miesta výkonu práce.

Z popisu situácie je zrejmé, že pre zabezpečenie funkčnosti takto zostaveného systému, je potrebné zabezpečiť v prvom rade nepretržitú dostupnosť elektrickej energie pre samotné terminálové zariadenie. Dôležitý je aj použitý software, mal by byť pravidelne aktualizovaný, čím sa zabezpečí eliminácia možných nedostatkov[42]. V prípade výskytu pracovného úrazu sa do protokolu zaznamenáva, okrem iných údajov, aj presný čas úrazu[43]. Terminál je potrebné pred spustením správne nakonfigurovať, čas evidencie musí korešpondovať s aktuálnym časom platným v časovej zóne sídla firmy. Táto konfigurácia je uskutočnená povereným zamestnancom, a teda do celého procesu zabezpečenia správnosti evidencie dochádzky je zapojený aj ľudský faktor.

Pre všetky kategórie aktív existuje zoznam zraniteľností, ktoré sa na nich môžu v prípade nedostatočného zabezpečenia vyskytnúť. Rovnako tak platí aj pre hrozby. Samozrejme, s prihliadnutím na individualitu a špecifickosť rôznych spracovateľských operácií, ktoré môžu byť s osobnými údajmi vykonávané, sa tieto parametre vždy identifikujú v kontexte konkrétnej spracovateľskej operácie. Príklad možných aktív zapojených do realizácie modelovej spracovateľskej činnosti, ich zraniteľností a potenciálnych hrozieb, zobrazuje tab. 4.1.

[42] V modelovej situácií uvažujeme, že poskytovateľ software, s ktorým má firma uzavretú licenčnú zmluvu pre poskytovanie tohto software, neustále monitoruje, kontroluje a ďalej rozvíja činnosť poskytovaného produktu. V prípade nedostatkov prináša zákazníkom vylepšenia v podobe dostupných aktualizácií.

[43] Ide o údaj vyžadovanými inštitúciami, ktoré ďalej posudzujú, či môže byť skutočne zaznamenaná udalosť považovaná za pracovný úraz, a či má teda poškodený zamestnanec vôbec právo na uplatnenie nárokov v dôsledky ujmy spôsobenej počas tohto úrazu.

Tab. 4.1: Identifikované aktíva, ich zraniteľnosti a možné hrozby v rámci konkrétnej spracovateľskej operácie.

Identifikované aktívum	Možná hrozba	Najpravdepodobnejšia zraniteľnosť
Software pre evidenciu dochádzky zamestnancov	Porucha a chyba software	Nedostatočné riadenie a overovanie zmien (aktualizácie)
	Poškodenie databázy obsahujúcej evidenciu dochádzky	Nevhodná manipulácia (napr. pri kontrole údajov poverenýmzamestnancom[44])
Terminál slúžiaci pre zaznamenávanie dochádzky zamestnancami	Výpadok energie	Nestabilná dodávka energie
	Chyba personálu pri konfigurácií zariadenia	Nesúlad zaznamenaných časových údajov s realitou

4.3 Analýza rizík

V analytickej časti sa riziku vyplývajúcemu zo spracovateľskej činnosti prisudzuje hodnota jeho pravdepodobnosti a závažnosti. Hodnota pravdepodobnosti v sebe zahŕňa relevanciu vzniku hroby a mieru zraniteľnosti podporného aktíva. Závažnosť je výsledkom posúdenia dopadu rizika na práva a slobody subjektov spracúvaných údajov.

Pravdepodobnosť

Pre určenie pravdepodobnosti výskytu rizika je potrebné priradiť identifikovaným zraniteľnostiam podporných aktív a hrozbám, ktoré môžu tieto zraniteľnosti zneužiť, určitú hodnotu. Ohodnotenie konkrétnej zraniteľnosti poskytuje odpoveď na otázku, aké jednoduché, resp. náročné je zraniteľnosť využiť. Je pritom potrebné zvážiť aktuálne implementovaný bezpečnostný systém na ochranu aktív. Naopak hodnota relevancie hrozby odzrkadľuje pravdepodobnosť využitia identifikovanej zraniteľnosti konkrétnou posudzovanou hrozbou. Ohodnotenie identifikovaných zraniteľností a možných hrozieb súvisiacich s modelovou situáciou zobrazuje tab. 4.2.

[44] V prípade potreby prebieha pravidelná kontrola zaznamenaných údajov v evidencii dochádzky. Jedná sa o bežný spôsob kontroly zamestnancov, ktorý uskutočňuje poverená osoba, zväčša personalista/-tka.

Tab. 4.2: Ohodnotenie identifikovaných zraniteľností a možných hrozieb konkrétnej spracovateľskej operácie.

Možná hrozba	Chyba personálu pri konfigurácií zariadenia	Výpadok energie	Poškodenie databázy obsahujúcej evidenciu dochádzky	Porucha a chyba software
Relevancia hrozby	Nízka	Nízka	Nízka	Stredná
Odôvodnenie	Túto činnosť uskutočňuje špeciálne školený zamestnanec; nastavená konfigurácia je následne kontrolovaná iným povereným zamestnancom.	V prípade výpadku energie je zaistený záložný zdroj energie, ktorý zabezpečí činnosť zariadení až do príchodu povereného zamestnanca, ktorý obdržal informáciu o výpadku energie.	Prístup k údajom v databáze majú len vybraní zamestnanci špeciálne školení pre túto činnosť; pre prístup do databázy používajú jedinečné autentizačné údaje.	Kontroly software sú uskutočňované v stanovených intervaloch, ktoré nemusia presne korešpondovať s intervalom vývoja nových aktualizácií daného software.
Zraniteľnosť	Nesúlad zaznamenaných časových údajov s realitou	Nestabilná dodávka energie	Nevhodná manipulácia (napr. pri kontrole údajov povereným zamestnancom)	Nedostatočné riadenie a overovanie zmien (aktualizácie)
Miera zraniteľnosti	Nízka	Nízka	Stredná	Nízka
Pravdepodobnosť	1	1	2	2

Závažnosť – miera identifikovateľnosti

Pri posudzovaní závažnosti rizika je potrebné určiť mieru identifikovateľnosti, čiže ako jednoduché, resp. ako náročné je zo spracúvaných osobných údajov identifikovať konkrétny subjekt údajov (tj. konkrétneho zamestnanca).

Z popisu uvažovanej modelovej situácie je zrejmé, že pre priznanie patričného odškodnenia musí byť jednoznačne určiteľné, komu má byť odškodnenie priznané. Tento subjekt musí byť teda jednoznačne identifikovateľný. V systéme evidencie dochádzky síce zamestnanec figuruje pod prideleným identifikačným číslom, ktoré ho odlišuje od ostatných zamestnancov, no práve vďaka tomuto jedinečnému identifikátoru môže byť konkrétny zamestnanec jedinečne rozpoznaný.

Taktiež bolo v predchádzajúcej časti popísané, že záznam o pracovnej úraze poskytnutý príslušnej poisťovni musí obsahovať meno a priezvisko, rodné číslo a adresu bydliska zamestnanca. Pomocou tejto kombinácie údajov je možné konkrétny subjekt jasne identifikovať, miera identifikovateľnosti je preto vysoká.

Závažnosť – intenzita zásahu do práv a slobôd

V identifikačnej časti modelovej situácie bolo ako príklad zásahu do práv a slobôd uvedené odoprenie uznania primeraného odškodnenia zamestnanca v dôsledku chybe v systéme evidencie dochádzky. V takejto situácií by zamestnanec v priebehu zotavovania sa z úrazu nemal nárok na príspevok z práceneschopnosti, pravdepodobne by situáciu musel vyriešiť čerpaním neplateného voľna, čo by sa odzrkadlilo na znekvalitnení jeho finančnej situácie a tým aj celkovej kvality života. Takto postihnutý subjekt môže pociťovať výrazné nepríjemnosti, ktoré ale dokáže pri vynaložení veľkého úsilia (napr. finančná pôžička či pomoc od blízkych) prekonať. Dopad rizika na práva a slobody môžeme teda klasifikovať ako stredný.

Určenie výslednej hodnoty závažnosti

Výsledná hodnota závažností vzniknutého incidentu je určená kombináciou hodnôt určených v predchádzajúcich krokoch, tj. ako kombinácia vysokej miery identifikovateľnosti a stredného dopadu na práva a slobody dotknutého subjektu spracúvaných údajov. Hodnota závažnosti rizika v uvažovanej modelovej situácií je, po aplikácií uvedených hodnôt dvoch dielčích parametrov, práve 6, čo odpovedá vysokej závažnosti uvažovaného incidentu. Túto skutočnosť zobrazuje tab. 4.3 spolu s tab. 4.4.

Tab. 4.3: Výsledná hodnota závažnosti rizika modelovej spracovateľskej operácie.

	Dopad	Z	N	**S**	V
Identifikácia	Zanedbateľná	1	2	3	4
	Nízka	2	3	4	5
	Stredná	3	4	5	6
	Vysoká	4	5	**6**	7

Tab. 4.4: Klasifikácia závažnosti v závislosti na jej hodnote.

Výsledná hodnota identifikácia x dopad	**Závažnosť incidentu**
< 3	Zanedbateľná (1)
4	Nízka (2)
5	Stredná (3)
> 5	**Vysoká (4)**

4.4 Určenie výslednej hodnoty rizika

Po zaradení získaných hodnôt pravdepodobnosti a závažnosti rizika do súčtovej matice, zobrazenej v tab. 4.5, získavame výslednú hodnotu rizika modelového procesu spracúvania údajov. Jeho hodnota je 8, čo podľa navrhnutej metodiky odpovedá strednému[45] riziku posudzovanej činnosti spracúvania údajov. Takéto identifikované riziko je z dlhodobého hľadiska neprípustné a musia byť zahájené systematické kroky k jeho odstráneniu.

[45] Stredné riziko spracovania je klasifikované v rozmedzí hodnôt 8 – 12 výsledného rizika (viď tab. 3.14).

Tab. 4.5: Výsledné riziko modelovej spracovateľskej činnosti.

závažnosť	**V (4)**	4	**8**	12	16
	S (3)	3	6	9	12
	N (2)	2	4	6	8
	Z (1)	1	2	3	4
		Z (1)	**N (2)**	S (3)	V (4)
		pravdepodobnosť			

5 PRAKTICKÁ ČASŤ

Hlavnou náplňou praktickej časti tejto záverečnej práce je naprogramovanie aplikácie, ktorá poskytne jej užívateľom možnosť realizovať proces posúdenia rizík za účelom prvotného stanovenia závažnosti rizika uskutočňovaných spracovateľských operácií s osobnými údajmi. Aplikácia je realizovaná vo forme webovej aplikácie a jej základným stavebným prvkom je dotazníkový formulár, v rámci ktorého užívateľ bližšie charakterizuje rozličné aspekty vykonávaného spracúvania. Na základe zvolených parametrov aplikácia následne vyhodnotí závažnosť rizika posudzovanej činnosti spracúvania údajov. Priebeh procesu vyhodnocovania je pre užívateľa celkom transparentný.

5.1 Realizácia informačného portálu a webovej aplikácie

Pri tvorbe webovej aplikácie bola realizovaná myšlienka, že vytvorená webová stránka by mala užívateľovi hneď na prvý pohľad poskytnúť odpoveď na dôležitú základnú otázku – čo sa užívateľ môže na danej stránke dozvedieť, resp. čomu je venovaná jej obsahová náplň. Z tohto dôvodu nie je webová stránka len jednoduchou aplikáciou, ale možno ju označiť pojmom „informačný portál“, nakoľko obsahuje základné informácie súvisiace s ochranou osobných údajov a tiež so samotným Nariadením za účelom oboznámenia užívateľa s aspektami danej problematiky. Pokiaľ má teda užívateľ záujem, vie sa o problematike ochrany osobných údajov dozvedieť všetky dôležité informácie, nakoľko tie sú v rámci informačného portálu interpretované takým spôsobom, aby boli ľahko zrozumiteľné a pochopiteľné aj pre užívateľa neznalého v danej oblasti.

V rámci sekcie informačného portálu venovanej posudzovaniu rizík má užívateľ možnosť pristúpiť k aplikácii, ktorá ho prevedie procesom posúdenia rizík pre užívateľom realizovanú činnosť spracúvania osobných údajov. Tento proces je realizovaný s využitím dotazníkového formulára, v ktorom užívateľ postupne vyberá možnosti obsahujúce popis rozličných aspektov spracúvania osobných údajov tak, aby čo najpresnejšie pomocou zvolených možností charakterizoval posudzovanú spracovateľskú činnosť. Následne je z užívateľom vybraných hodnôt stanovená závažnosť rizika, ktoré v dôsledku vykonávania posudzovaných činností môže vzniknúť pre práva a slobody subjektov údajov.

5.1.1 Použitý framework a implementačné nástroje

Pre vytvorenie základnej podoby webovej stránky bol využitý framework Bootsrap [24]. Jedná sa o voľne dostupné rozhranie, ktoré poskytuje jeho užívateľom prostriedky pre vytváranie moderných webových stránok s prihliadnutím najmä na vizuálne aspekty

vytvorenej stránky. Poskytuje množstvo preddefinovaných funkcionalít a elementov, akými sú napr. zoznamy a formuláre, čím užívateľovi uľahčuje prácu so zložitými štruktúrami. Je založený na písaní zdrojového kódu s využitím značkovacieho jazyka HTML (*Hypertext Markup Language*), ktorý je po vzhľadovej stránke rozšíriteľný pomocou jazyka CSS (*Cascading Style Sheet*). Pre programovanie funkcionality je v rámci frameworku Bootstrap používaný primárne programovací jazyk Javascript.

Hlavným dôvodom, prečo bol využitý práve popísaný framework, je iba okrajová skúsenosť s tvorbou webových stránok. Počas svojho stredoškolského štúdia sa autorka už stretla s kombináciou jazykov HTML a CSS, avšak bez akéhokoľvek hlbšieho zamerania či tvorby konkrétnych stránok. Framework Bootstrap a všetky jeho oficiálne komponenty je licencovaný pod permisívnou MIT licenciou, vďaka čomu autorka mohla využiť dostupné šablóny [25] pre prvotný návrh vzhľadu webovej stránky, ktorý následne už len upravila podľa svojich potrieb a preferencií. Príslušné zdrojové kódy použitej šablóny sú patrične uvedené copyright doložkou o pôvode originálneho diela a taktiež odkazom na pôvodnú licenciu použitého prvku. Ďalším z dôvodov je možnosť využitia programovacieho jazyka Javascript pre doplnenie funkcionality webovej aplikácie. S týmto programovacím jazykom autorka síce pred tvorbou webovej aplikácie k bakalárskej práci žiadnu skúsenosť nemala, avšak nakoľko sa jedná o rozšírený a využívaný programovací jazyk, tak nebol problém získať z bohatej dokumentácie dostupnej naprieč celým internetom informácie užitočné k implementácii funkcionality vytvorenej webovej aplikácie.

Ďalšou využitou implementačnou pomôckou je open-source Javascriptová knižnica pre vytváranie webových komponentov s názvom React. React bol vytvorený spoločnosťou Facebook už v roku 2013 a odvtedy patrí k veľmi rozšíreným a obľúbeným nástrojom pri implementácií front-end[46] webových aplikácií (tj. bez interakcie s externou serverovou časťou) používajúcich webový prehliadač ako aplikačnú platformu, prípadne tiež pri tvorbe mobilných aplikácií. React uľahčuje prácu najmä začiatočníkom tým spôsobom, že umožňuje vo svojich komponentoch prehľadne definovať dielčie časti štruktúry vytváranej webovej stránky (s využitím jazyka HTML rozšíreného o syntax JSX), ktoré sú pri výslednej interakcii s užívateľom prepojené do jedného vizuálne-funkčného celku schopného reaktívne reagovať na požiadavky užívateľa webovej stránky, resp. aplikácie.

[46] Pojmom „front-end“ sa označuje taká aplikácia, ktorá pre svoju činnosť nevyužíva komunikáciu s externou serverovou časťou, tj. všetky činnosti aplikácie prebehajú bez interakcie s externou serverovou časťou. Všetky procesy teda prebiehajú len na strane klienta (užívateľa).

5.2 Zostavenie zoznamu kritérií pre posudzovanie závažnosti rizika spracúvania údajov

Vytvorená aplikácia dostupná v rámci webového informačného portálu užívateľovi poskytuje možnosť podrobiť ním vykonávané činnosti spracúvania procesu posúdenia rizík za účelom stanovenia prvotnej hodnoty závažnosti tohto spracúvania. Jedná sa teda o posúdenie rizík v podobe všeobecnej povinnosti prevádzkovateľa, ktorú vykonáva s prihliadnutím na plnenie povinností definovaných v čl. 24 Nariadenia (viď kap. 2.3.1). Všeobecný proces posúdenia rizík je prevádzkovateľ povinný vykonať vždy pri realizácií akejkoľvek činnosti spracúvania údajov a jeho výsledok môže následne využiť pre rozhodnutie v otázke nutnosti vykonania plného *DPIA* (viď kap. 2.3.2).

Základný postup procesu posúdenia rizík bol priblížený pri návrhu metodiky posudzovania rizík v kontexte ochrany osobných údajov, podrobne popísanej v kap. 3. Táto predstavená metodika je základným východiskom pre vytvorenie podkladových materiálov pre webovú aplikáciu posudzovania rizík a na základe princípov uvedených v danej metodike bude realizované rozhodovanie o úrovni závažnosti rizika posudzovaných činností. Pre získanie povedomia o tom, aké činnosti sú posudzované, resp. aké úkony s osobnými údajmi sú pri vykonávaní daných činností realizované, bolo potrebné vytvoriť určitý prvok, pomocou ktorého dokáže užívateľ bližšie špecifikovať, aké činnosti chce s využitím aplikácie ohodnotiť. Pre naplnenie popísaného účelu je vytvorený formulárový dotazník obsahujúci 15 (resp. 16) kritérií[47], ktoré je potrebné zohľadniť pri posudzovaní rizík (kompletný zoznam kritérií je súčasťou prílohy B). Pre jednotlivé kritériá je definovaných niekoľko možností (pričom vždy najmenej dve) reprezentujúcich možné „vlastnosti“[48] posudzovaného spracúvania. Užívateľ[49] postupne pre každé kritérium vyberá možnosť (príp. viaceré možnosti[50]) charakterizujúcu spracovateľskú činnosť, ktorú chce podrobiť posúdeniu rizík. Takýmto spôsobom je vytvorený jedinečný súbor charakteristík konkrétnej posudzovanej činnosti, ktorý v ďalšej fáze vstupuje do procesu vyhodnotenia webovou aplikáciou.

---

[47] Kritérium týkajúce sa otázky predávania osobných údajov tretím stratám je rozpracované na dielčie podčasti, kedy sa v prípade realizovaného predávania osobných údajov posudzuje ešte dodatočne účel predávania osobných údajov tretej strane a tiež pôsobnosť tejto tretej strany z hľadiska príslušnosti medzi krajiny s adekvátnou úrovňou ochrany údajov.

[48] Jednotlivé možnosti je teda možno chápať ako konkrétne aspekty, ktorými sa vyznačujú spracovateľské činnosti.

[49] Dotazníkový formulár obsahuje v istých miestach aj doplňujúce informácie vo forme „nápovedy“ pre užívateľa poskytujúce vysvetlenie alebo aspoň upresnenie niektorých odborných pojmov, ktorých význam by užívateľovi nemusel byť na prvý pohľad zrejmý.

[50] Výnimkou sú kritériá č. 1, č. 2 a č. 10B, pri ktorých smie užívateľ označiť viac než len jednu alternatívu.

Cieľom aplikácie je poskytnúť užívateľovi výsledok obsahujúci informáciu o tom, aké závažné riziko voči právam a slobodám subjektov údajov môže byť v dôsledku realizácie konkrétnych spracovateľských činností spôsobené. Okrem základnej klasifikácie rizika, na základe hodnoty jeho závažnosti, poskytne výsledok aplikácie užívateľovi aj informáciu o nutnosti vykonania posúdenia *DPIA*. Za týmto účelom boli pri vytváraní zoznamu kritérií vzaté do úvahy také aspekty, aby mohlo byť na spracúvanie nahliadnuté primárne za účelom diskutovania problematiky vzniku pravdepodobne veľkého rizika pre práva a slobody fyzických osôb. Zoznam kritérií bol z toho dôvodu zostavený s prihliadnutím k stanovisku pracovnej skupiny WP29 k problematike nutnosti vykonania *DPIA* [12]. V rámci výkladových pokynov WP29 je uvedených deväť všeobecných kritérií pre stanovenie vysokej rizikovosti spracúvania osobných údajov:

I. vykonáva sa hodnotenie alebo sa vytvára bodové ohodnocovanie fyzických osôb, vrátane profilovania a predpovede,
II. vykonáva sa automatické rozhodovanie s právnym alebo obdobným významným účinkom,
III. vykonáva sa systematické monitorovanie, vrátane monitorovania verejne prístupných priestorov,
IV. vykonáva sa spracúvanie citlivých osobných údajov,
V. vykonáva sa spracúvanie veľkého rozsahu,
VI. vykonáva sa kombinácia alebo prepájanie údajov rôznych spracúvaní,
VII. vykonáva sa spracúvanie údajov týkajúcich sa zraniteľných subjektov údajov,
VIII. dochádza k inovatívnemu využívaniu alebo aplikácii technologických alebo organizačných riešení,
IX. vykonáva sa spracúvanie s obtiažne uplatniteľnými právami subjektov údajov.

Uvedené kritériá sú určitým spôsobom zakomponované do vytvoreného zoznamu kritérií, nad ktorým prebieha v rámci aplikácie vyhodnocovanie celkovej závažnosti rizika.

Okrem uvedených kritérií WP29 bol zoznam kritérií pre webovú aplikáciu inšpirovaný rovnako aj návodnými materiálmi zverejnenými ÚOOÚ popisujúcimi jednak operácie spracúvania, ktoré podliehajú, resp. nepodliehajú požiadavku na vykonanie *DPIA* [26], a taktiež problematiku vyhodnotenia rizikovosti operácií spracúvania osobných údajov za účelom stanovenia nutnosti vykonať *DPIA* [27]. Oba uvedené dokumenty síce vychádzajú opäť z vyššie popísaného stanoviska WP29, avšak uvádzajú už konkrétne príklady pre rozhodné kritériá, ktoré je potrebné za daným účelom posúdiť.

Použitá metodika, tak ako bola navrhnutá (viď kap. 3), aplikuje proces posúdenia rizík nad dvoma základnými rovinami – problematika posúdenia jedinečných charakteristík činností vykonávaných s osobnými údajmi v rámci ich spracúvania a management informačnej bezpečnosti – a v konečnom dôsledku ich pri vyhodnotení celkového rizika vzájomne prepája. Metodika, s ktorou pracuje webová aplikácia pri vyhodnocovaní celkovej závažnosti rizika, vychádza z totožných princípov akurát s tým rozdielom, že v rámci vytvorenej aplikácie nedochádza k prepojeniu dvoch rovín tak, ako boli popísané pri návrhu metodiky. Aplikácia bola vytvorená spôsobom zameraným výhradne na stanovenie hodnoty závažnosti rizika ako funkcie miery identifikovateľnosti subjektu údajov a miery zásahu do práv a slobôd (viď kap. 3.3.2), a to z dôvodu náročnosti implementácie funkčného prepojenia tohto procesu ešte navyše s komplexným posúdením úrovne informačnej bezpečnosti.

Management informačnej bezpečnosti ako proces posúdenia rizík súvisiacich so zabezpečením technických prvkov určitým spôsobom zapojených do vykonávania spracovateľských operácií (viď napr. tab. 3.8) je sám o sebe rozsiahly a pomerne náročný proces, čo sa týka jeho dôslednej a podrobnej realizácie. Z tohto dôvodu nebol samostatne implementovaný do aplikácie v takom rozsahu, v akom je vyžadovaný napr. pri vykonaní plného *DPIA*, tj. identifikácia aktív, zraniteľností a hrozieb, ich následná analýza, identifikácia potenciálnych rizík a stanovenie ich hodnoty. Avšak ani pri realizácií všeobecného posúdenia rizík nie je možné vynechať úplne všetky kroky popísaného procesu. Aplikácia síce primárne cieli na stanovenie závažnosti rizík, ale v rámci posúdenia sú analyzované aj aspekty spracúvania v súvislosti s riadením informačnej bezpečnosti týkajúce sa najmä úrovne zabezpečenia triády CIA[51]. Vytvorený zoznam posudzovaných kritérií, ktorý aplikácia vyhodnocuje, obsahuje preto niekoľko kritérií[52] úzko spätých s ochranou osobných údajov ako napr. použitie mechanizmov šifrovania, spôsoby riadenia administratívneho a fyzického prístupu ku spracúvaným údajom, zabezpečenie úložísk údajov apod. Hlavným účelom týchto bezpečnostných kritérií je analyzovať úroveň zabezpečenia v súvislosti so zaistením ochrany osobných údajov pred neoprávneným prístupom a pred náhodným a/alebo úmyselným zničením, stratou či pozmenením týchto údajov.

Na základe vyššie uvedeného boli do vytvoreného zoznamu dotazníkového formulára zahrnuté nasledovné kritériá:

- kritérium 1 – kategórie zhromažďovaných údajov,
- kritérium 2 – miera identifikovateľnosti subjektu údajov,

[51] Jedná sa o zabezpečenie spracúvaných osobných údajov takým spôsobom, aby bola dostatočne zaistená ich dôvernosť (C – *confidentiality*), integrita (I – *integrity*) a dostupnosť (A – *availability*), viď kap. 3.1.2.
[52] Konkrétne sa jedná o kritériá 12 – 15; všetky kritériá budú vysvetlené v nasledujúcom texte.

- kritérium 3 – miera zraniteľnosti subjektu údajov,
- kritérium 4 – rozsah spracúvania osobných údajov,
- kritérium 5 – sústavnosť zhromažďovania osobných údajov,
- kritérium 6 – monitorovanie verejných priestorov,
- kritérium 7 – zverejňovanie zaznamenaných osobných údajov,
- kritérium 8 – inovatívnosť riešení spracúvania,
- kritérium 9 – kombinovanie a prepájanie osobných údajov,
- kritérium 10 – predávanie osobných údajov tretím stranám,
- kritérium 10A – charakteristika oblasti pôsobnosti tretej strany,
- kritérium 10B – účel predávania údajov tretej strane,
- kritérium 11 – uplatnenie práv subjektov údajov,
- kritérium 12 – zabezpečenie prístupu k osobným údajom,
- kritérium 13 – úroveň informovanosti osôb s oprávneným prístupom k údajom,
- kritérium 14 – aplikácia dodatočných prostriedkov zabezpečenia,
- kritérium 15 – dostupnosť osobných údajov.

Pre každé posudzované kritérium sú uvažované vždy najmenej dve možnosti, ktoré môžu v otázke skúmaného kritéria charakterizovať posudzované spracúvanie. Každej z uvedených možností je následne priradená určitá hodnota závažnosti rizika konkrétneho kritéria z pohľadu možného spôsobeného zásahu do práv a slobôd v dôsledku zahrnutie zvoleného aspektu medzi vlastnosti charakterizujúce posudzované spracúvanie. Každá dielčia hodnota je stanovená ako funkcia možnosti identifikovateľnosti subjektu údajov a miery nepriaznivého zásahu do práv a slobôd subjektu údajov (viď tab. 3.11).

Pre názornosť možno uviesť príklad pre aspekt spracúvania týkajúci sa spracúvania údajov umožňujúcich jednoznačnú identifikáciu subjektu údajov (kritérium 1). Nakoľko sa jedná o jednoznačné identifikátory, miera identifikácie subjektu je najvyššia možná, tj. je klasifikovaná ako „vysoká“ s kvantitatívnym ohodnotením hodnotou 4 (viď tab. 3.9). Intenzitu dopadu na práva a slobody možno zaradiť do úrovne „stredného“ dopadu, čomu prislúcha hodnota 3 (viď tab. 3.10). Na základe znalosti týchto dvoch hodnôt, spolu s využitím súčtovej matice pre stanovenie hodnoty závažnosti rizika uvedenej v tab. 3.11 možno priradiť pre závažnosť aspektu spracúvania jednoznačných identifikátorov týkajúcich sa subjektu údajov hodnotu 6, čo značí vysokú závažnosť rizika pre práva a slobody subjektov spracúvaných údajov.

5.3 Vyhodnotenie kritérií a stanovenie závažnosti rizika

Základným prvkom aplikácie je formulár obsahujúci zoznam kritérií, ktorých usporiadanie a význam už boli popísané v predošlej podkapitole. Prvotným predpokladom pre stanovenie počiatočnej závažnosti hodnoty rizika posudzovaného spracúvania je preskúmanie a následné ohodnotenie súboru jedinečných charakteristík posudzovaného spracúvania, ktoré vyplnením daného zoznamu kritérií v podobe dotazníkového formulára špecifikoval samotný užívateľ. Súbor jedinečných charakteristík následne prechádza do fázy vyhodnotenia pre stanovenie celkovej závažnosti rizika posudzovanej činnosti.

Aby bolo možné stanoviť celkovú hodnotu závažnosti a na základe toho ďalej vo výsledku klasifikovať identifikované riziko do jednej zo štyroch základných úrovní, bolo potrebné stanoviť pravidlá, pomocou ktorých bude aplikácia nahliadať na jedinečný súbor charakteristík vytvorený užívateľom pre konkrétnu posudzovanú jednotku, a pomocou ktorých následne celý proces posudzovania rizík vyhodnotí.

Pri vyhodnocovaní závažnosti rizika postupuje aplikácia v niekoľkých krokoch. Jadrom procesu vyhodnotenia je stanovenie kumulatívneho súčtu závažností všetkých posúdených kritérií na základe užívateľom navolených vlastností spracúvania[53]. Maximálna bodová hodnota kumulatívneho súčtu, ktorú môže riziko posudzované z hľadiska závažnosti dosiahnuť, je 100, čo značí vysoko rizikové spracúvanie osobných údajov. Táto hodnota by bola dosiahnutá v situácií najrizikovejšieho spracúvania, tj. pre všetky z posudzovaných kritérií by boli charakteristické tie aspekty, ktorým prislúcha najvyššia hodnota závažnosti rizika spomedzi ponúkaných možností. Od tejto maximálnej hranice sa následne odvíja kategorizácia posudzovaných činností do úrovní s nižšou mierou závažnosti. V súvislosti so stanovením metódy spôsobu výpočtu kumulatívneho súčtu závažností je problematika aspektov, ktoré odkazujú na výkladové pokyny WP29 a sú zamerané na stanovenie vysoko rizikového spracúvania, ošetrená tým spôsobom, že konkrétne „špeciálne“ možnosti, odkazujúce na týchto deväť vysokorizikových aspektov spracúvania[54], sú bodovo ohodnotené úrovňou závažnosti 7 (čo je podľa tab. 3.11 najvyššia možná dosiahnuteľná hodnota závažnosti rizika).

Hodnota získaného kumulatívneho súčtu závažností jednotlivých aspektov zaradených do súboru charakteristík posudzovaného spracúvania je ovplyvnená aplikáciou tzv.

---

[53] V prípade kritérií č. 1, č. 2 a č. 10B, pre ktoré môže užívateľ zvoliť viac než len jednu možnosť, sa pre stanovenie kumulatívneho súčtu aplikuje len „najhodnotnejšia“ zo zvolených možností, tj. možnosť s najvyššou hodnotou závažnosti pre dané kritérium.

[54] Pre jednoznačné odlíšenie týchto konkrétnych aspektov spracúvania sú v priloženom zozname kritérií (viď príloha B) uvedené pod označením „X“, no v rámci činnosti algoritmu webovej aplikácie je ich závažnosti priradená hodnota 7.

priorizujúcich pravidiel. Tie boli zvolené na základe určitých objektívnych skutočností (právne normy, stanovisko WP29, súvislosť s úrovňou managementu informačnej bezpečnosti apod.).

Pravidlo 1 – vysokorizikové kritériá

Nakoľko bol zoznam kritérií pre posúdenie závažnosti rizika vytvorený aj na základe stanoviska WP29 k nutnosti vykonania posúdenia vplyvu, a zahŕňa tak aj deväť základných kritérií pre definíciu vysoko rizikového spracúvania, ako prvé sa pri vyhodnocovaní uplatňuje pravidlo, ktoré kontroluje výber minimálne dvoch z týchto kritérií. Ak spracúvanie napĺňa aspoň dva znaky z uvedených, vyžaduje takéto spracúvanie vykonanie posúdenia vplyvu na ochranu údajov z dôvodu, že môže pravdepodobne spôsobiť vysoké riziko pre práva a slobody fyzických osôb.

Jednou z výnimiek pre uplatnenie popísaného pravidla sú vysokorizikové aspekty príslušné pre kritériá 5 a 6, tj. aspekt systematického monitorovania a aspekt monitorovania verejných priestorov. V prípade, kedy užívateľ vyberie obe z uvedených položiek a zároveň to budú jediné dve položky spomedzi vybraných, ktoré budú ohodnotené závažnosťou $= 7$ (označenie X), neaplikuje sa pravidlo automatického vyhodnotenia posudzovaného spracúvania ako vysokorizikového, nakoľko oba tieto aspekty spoločne odkazujú len na jeden z bodov výkladových pokynov WP29, konkrétne na bod č. 3. Aby aplikácia v prípade zahrnutia týchto dvoch aspektov automaticky zaradila spracúvanie do úrovne vysokého rizika, musí byť v množine aspektov charakterizujúcich posudzované spracúvanie prítomná ešte aspoň jedna položka s hodnotou závažnosti $= 7$. Obdobne tak situácia, kedy bude zaznamenané údaje možné využiť pre profilovanie užívateľov (kritérium 1) a zároveň budú tieto osobné údaje ešte poskytované tretím stranám taktiež za účelom vytvárania bodového ohodnotenia subjektov (kritérium 10B), nebude automaticky vyhodnotená ako vysokorizikovú, nakoľko oba aspekty odkazujú spoločne na prvý bod výkladových pokynov WP29.

Pravidlo 2 – šifrovanie a pseudonymizácia

Šifrovanie a pseudonymizácia predstavujú technické prostriedky, ktoré umožňujú nadštandardne zabezpečiť zaznamenané údaje, čo môže mať za následok zníženie možného rizika pre príslušné dotknuté osoby[55]. Samotné Nariadenie uvádza v čl. 32 niekoľko

[55] Tento predpoklad uvádza aj samotné Nariadenie, viď napr. bod 28 odôvodnenia, tiež bod 78 odôvodnenia, čl. 4 bod 5 alebo čl. 1 odst. 1 Nariadenia.

doporučení k zaisteniu bezpečnosti spracúvania, v ktorom, okrem iného, navádza aj na použitie mechanizmov šifrovania a pseudonymizácie osobných údajov, pričom ale nikde explicitne nevyjadruje povinnosť ich implementácie. Jedná sa preto o mechanizmy, ktorých implementácia síce nie je povinná, ale pre účely zníženia vzniku rizika je zjavne doporučená, nakoľko môže pozitívne ovplyvniť úroveň zabezpečenia osobných údajov.

Na základe uvedených predpokladov vyplývajúcich z Nariadenia bolo do rozhodovacieho mechanizmu webovej aplikácie zahrnuté aj pravidlo prihliadajúce na skutočnosť, či množina charakteristických aspektov obsahuje pre kritérium č. 14 položku odkazujúcu na aplikáciu dodatočných mechanizmov zabezpečenia údajov. V prípade, že sú v rámci posudzovaného spracúvania údaje podrobené procesu šifrovania a/alebo pseudonymizácie, dochádza k zníženiu závažnosti rizika iných aspektov, ktoré môže zavedený mechanizmus šifrovania a/alebo pseudonymizácie ovplyvniť. Ovplyvnenie miery závažnosti rizika sa samozrejme neuplatňuje na všetky aspekty všetkých ostatných kritérií. Uplatňuje sa najmä pri tých kritériách, ktoré istým spôsobom určujú mieru identifikovateľnosti subjektu údajov, alebo pri tých, ktoré prihliadajú na prístup k osobným údajom či ich prenosnosť iným osobám. Zavedenie mechanizmov šifrovania a/alebo pseudonymizácie bude znižovať hodnoty aspektov nasledujúcich kritérií:

- kritérium 1 – kategórie zhromažďovaných údajov,
- kritérium 2 – miera identifikovateľnosti subjektu údajov,
- kritérium 3 – miera zraniteľnosti subjektu údajov,
- kritérium 4 – rozsah spracúvania osobných údajov,
- kritérium 7 – zverejňovanie zaznamenaných osobných údajov,
- kritérium 10A – charakteristika oblasti pôsobnosti tretej strany,
- kritérium 10B – účel predávania údajov tretej strane,
- kritérium 12 – zabezpečenie prístupu k osobným údajom,
- kritérium 13 – úroveň informovanosti osôb s oprávneným prístupom k údajom,

pričom bude ovplyvňovať všetky tie aspekty, ktorých hodnota závažnosti je ≥ 2, ale pritom za žiadnych okolností neznížia závažnosť vysokorizikových aspektov s prislúchajúcim označením X (hodnota závažnosti $= 7$).

Hodnoty vyššie uvedenej množiny ovplyvňovaných aspektov sú vynásobené koeficientom k, ktorý bude mať za následok zníženie hodnoty ich závažnosti, čo sa v určitej miere prejaví pri stanovení celkovej závažnosti rizika posudzovaného spracúvania. Hodnota koeficientu k znižujúceho hodnotu dielčích závažností ďalších posudzovaných

aspektov bola zvolená s prihliadnutím na nasledovnú úvahu – implementácia mechanizmov šifrovania a/alebo pseudonymizácie bude mať za následok zníženie hodnôt dielčích závažností „o úroveň nižšie“, tzn. že (i) hodnoty závažnosti, ktoré pôvodne spadali do úrovne vysokej závažnosti, bude možné po znížení zaradiť do úrovne strednej závažnosti rizika, (ii) hodnoty závažnosti, ktoré pôvodne spadali do úrovne strednej závažnosti, bude možné po znížení zaradiť do úrovne nízkej závažnosti rizika, (iii) hodnoty závažnosti, ktoré pôvodne spadali do úrovne nízkej závažnosti, bude možné po znížení zaradiť do úrovne zanedbateľnej závažnosti rizika a (iv) hodnoty závažnosti, ktoré pôvodne spadali do úrovne zanedbateľnej závažnosti, a ktorých hodnota je zároveň ≥ 2, budú patrične znížené, no stále budú zaradené do úrovne zanedbateľnej závažnosti rizika. Aby mohol byť popísaný posun v rámci kategorizácie dielčích závažností dosiahnutý pre všetky štyri úrovne závažnosti, bola pre koeficient šifrovania a/alebo pseudonymizácie zvolená hodnota[56] $k = 0.67$. Navrhované zníženie dielčích hodnôt závažností tých kritérií, ktoré sú ovplyvnené implementáciou mechanizmov šifrovania a/alebo pseudonymizácie, stanovené podľa vyššie popísaného princípu, je zachytené v tab. 5.1.

Tab. 5.1: Zníženie dielčích hodnôt závažnosti po aplikácii mechanizmov šifrovania a/alebo pseudonymizácie.

Závažnosť rizika	**Pôvodná hodnota závažnosti**	**Hodnota závažnosti znížená vplyvom koeficientu $k = 0.67$**
Zanedbateľná (max. hodnota = 3)	1	– nie je ovplyvnená –
	2	1.34 ⇨ zanedbateľná
	3	2.01 ⇨ zanedbateľná
Nízka (max. hodnota = 4)	4	2.68 ⇨ zanedbateľná
Stredná (max. hodnota = 5)	5	3.35 ⇨ nízka
Vysoká (max. hodnota = 7)	6	4.02 ⇨ stredná
	7	– nie je ovplyvnená –

[56] Konkrétna uvedená hodnota koeficientu bola zvolená na základe porovnávania výsledkov opakovaného testovania činnosti aplikácie. Zvolená hodnota sa javí ako ideálna pre nastavenie primeranej citlivosti aplikácie pri stanovovaní výslednej hodnoty závažnosti rizika a jeho následnej klasifikácii.

Dôležité je poznamenať, že uplatnenie koeficientu znižujúceho dielčie závažnosti iných aspektov práve v uvedenej hodnote $k = 0.67$, je možné uvažovať v idealizovanej situácii, kedy predpokladáme použitie bezpečných a schválených šifrovacích algoritmov[57], u ktorých je pravdepodobnosť prelomenia takmer nulová (resp. tieto algoritmy neboli doposiaľ prelomené s využitím dostupných výpočtových prostriedkov), rovnako tak predpokladáme použitie dostatočne dlhých a silných šifrovacích kľúčov. V prípade pseudonymizácie predpokladáme použitie takých mechanizmov, ktorých výstupom bude údaj svojim charakterom takmer odpovedajúci anonymizovanému[58] osobnému údaju, tj. budú použité čo najkvalitnejšie techniky pre pseudonymizáciu zaznamenaných údajov. V takýchto ideálnych situáciách možno predpokladať, že implementáciou mechanizmov pre šifrovanie a/alebo pseudonymizáciu je skutočne možné dosiahnuť znateľné zníženie celkovej závažnosti rizika pre práva a slobody subjektov údajov posudzovaných činností konkrétneho procesu spracúvania osobných údajov.

Aplikácia kumulatívneho súčtu

Cieľom aplikácie je vytvoriť kvantitatívne ohodnotenie celkového rizika, na základe ktorého bude následne riziko kategorizované do jednej zo štyroch úrovní, ktoré sú bližšie špecifikované kvalifikovaným popisom celkovej závažnosti. Pre dosiahnutie tohto cieľa je potrebné stanoviť celkový súčet závažností posudzovaných kritérií. Toho je dosiahnuté spôsobom, že pre každé kritérium, konkrétne pre zvolený aspekt daného kritéria, ktorý je súčasťou jedinečného súboru charakteristík navoleného užívateľom, sa uvažuje jemu priradená hodnota závažnosti. V prípade, kedy užívateľ označí pre jedno kritérium viac než jednu možnosť, čím do súboru charakteristík pridá viacero aspektov s rozdielnou hodnotou závažnosti, vstupuje do výpočtu kumulatívneho súčtu len najvyššia hodnota závažnosti spomedzi zvolených aspektov[59]. Celkovú hodnotu závažnosti rizika posudzovanej činnosti spracúvania osobných údajov je možno, s prihliadnutím na všetky uvedené pravidlá, vyjadriť pomocou rovnice:

$$SE = \left(\sum_{i=1}^{n} (f(LI \times PE)) \cdot k \right).$$

[57] Pre zoznam aktuálne doporučených bezpečných kryptografických algoritmov a im odpovedajúce dĺžky šifrovacích kľúčov viď napr. [28].

[58] Pseudonymizovaný osobný údaj predstavuje takú formu pôvodne zaznamenaného osobného údaju, z ktorej je možné identifikovať subjekt údajov, ale len s využitím dodatočných informácií o danom subjekte. Naopak u anonymizovaných údajov už nie je možné ani s pridelením dodatočných identifikátorov jednoznačne identifikovať konkrétny subjekt.

[59] Jedná sa konkrétne o kritériá č. 1, č. 2 a č. 10B, pre ktoré môže užívateľ zvoliť viac než len jednu možnosť.

Vysvetlenie parametrov zahrnutých vo vyššie uvedenej rovnici je nasledovné:

- *SE* je označenie pre celkovú závažnosť rizika (z angl. *severity*),
- $f(LI \times PE)$ je funkcia stanovujúca úroveň závažnosti každého z kritérií v závislosti na jednoznačne zvolenej možnosti na základe miery identifikovateľnosti subjektu údajov (z angl. *level of identification*) a spôsobeného zásahu do práv a slobôd (z angl. *prejudicial effect*), viď tab. 3.11,
- n je počet posudzovaných kritérií[60],
- k je koeficient priorizujúcich pravidiel (ak sú zahrnuté).

5.3.1 Kategorizácia výsledného rizika

Najkritickejším krokom pri návrhu rozhodovacej logiky bolo stanovenie hraníc jednotlivých úrovní rizika, do ktorých môže byť posúdené spracúvanie na základe výslednej hodnoty závažnosti klasifikované – zanedbateľné, nízke, stredné alebo vysoké riziko (viď tab. 3.15). S prihliadnutím na skutočnosť, že zoznam kritérií bol vytvorený aj na základe preštudovania návodných materiálov ÚOOU k vykonaniu posúdenia vplyvu na ochranu údajov [26][27] a boli doň zahrnuté niektoré kritériá vyskytujúce sa aj v uvedených materiáloch, bol pre stanovenie hranice úrovne „vysokého rizika“ využitý princíp analógie s postupmi pre zaradenie posudzovanej spracovateľskej činnosti medzi spracovania s vysokým rizikom pre práva a slobody subjektov údajov uplatnenými práve v uvedených dvoch návodných materiáloch.

Metodiky ÚOOU pre uvažované kritériá uvádzajú vždy najmenej dve možné alternatívy, pričom tie môžu dosahovať hodnotu kritickú, významnú alebo nízku. Pre zaradenie medzi spracovania s vysokým rizikom pre práva a slobody subjektov údajov sa uvádza, že posudzované spracúvanie musí byť charakterizované napríklad takým súborom hodnôt kritérií, kedy je jedna hodnota klasifikovaná ako kritická a zároveň je najmenej päť hodnôt klasifikovaných ako významných. Príkladom vysokorizikového spracúvania môže byť také spracúvanie, kedy:

- sú spracúvané citlivé osobné údaje (*kritická* – 7)[61],
- sú subjekty údajov identifikovateľné a rozpoznateľné (*významná* – 5),
- je zraniteľnosť subjektov údajov časovo obmedzená (*významná* – 4),
- je spracúvanie osobných údajov vykonávané v strednom rozsahu (*významná* – 4),

[60] Ako už bolo uvedené v predchádzajúcom popise – v závislosti na tom, akú možnosť (áno/nie) užívateľ zvolí pre kritérium č. 10, môže byť celkový počet posudzovaných kritérií 15 alebo 16.
[61] Slovný popis odpovedá kategorizácii aspektu spracúvania podľa metodického materiálu ÚOOU [27], číselná hodnota vyjadruje hodnotu závažnosti priradenú odpovedajúcemu aspektu v rámci zoznamu kritérií vytvoreného pre činnosť webovej aplikácie.

- dochádza k monitorovaniu miest verejne obmedzene prístupných (*významná* – 4),
- sú zaznamenané osobné údaje predávané do štátov so zaistenou úrovňou ochrany mimo EÚ (*významná* – 4).

Pri využití úvahy, že všetky ostatné posudzované kritériá by vykazovali najmenšiu hodnotu závažnosti (tj. 10 kritérií s hodnotou závažnosti 1) by spracúvanie charakterizované vyššie uvedeným popisom vlastností dosiahlo v rámci posúdenia hodnotu kumulatívneho súčtu 38 (z maximálnej možnej hodnoty 100). Pre upresnenie možno uviesť ešte ďalší príklad[62] spracúvania, kedy:

- je spracúvanie osobných údajov vykonávané vo veľkom rozsahu (*kritická* – 7),
- sú subjekty údajov identifikovateľné a rozpoznateľné (*významná* – 5),
- sú spracúvané jedinečné identifikačné údaje (*významná* – 6),
- je zraniteľnosť subjektov údajov časovo obmedzená (*významná* – 4),
- má subjekt údajov obmedzené práva ovplyvniť spracúvanie (*významná* – 4),
- sú údaje verejne prístupné obmedzenému počtu iných subjektov (*významná* – 4).

Opäť pri využití úvahy, že všetky ostatné kritériá sú z hľadiska závažnosti rizika pre práva a slobody subjektov údajov zanedbateľné, dosahuje takto charakterizované spracúvanie v kumulatívnom súčte hodnotu závažnosti 39. Na základe uvedenej analógie a s prihliadnutím na ostatné faktory, ktoré mechanizmus webovej aplikácie využíva pre kategorizáciu rizika, bola stanovená dolná hranica pre klasifikáciu spracúvania do úrovne „*vysokorizikové*“ hodnota kumulatívneho súčtu 38.

Ako „*zanedbateľné*“ možno klasifikovať posudzované spracúvanie jedine v prípade, kedy nie je charakterizované aspektom iným než s hodnotou závažnosti klasifikovanou ako zanedbateľnou, tzn. všetky aspekty posudzovaných kritérií, zahrnuté do súboru charakteristík posudzovaného spracúvania budú ohodnotené stupňom závažnosti spadajúcej do intervalu zanedbateľnej závažnosti (tj. hodnota 1 – 3, viď tab. 3.12). Je teda zrejmé, že horná hranica pre klasifikáciu spracúvania do tejto kategórie pri uvažovaní najideálnejšej situácie posudzovaného spracúvania, v zmysle charakteristiky pomocou najmenej rizikových aspektov jednotlivých kritérií, bude hodnota 17.

Interval v rozmedzí hodnôt výslednej závažnosti 18 až 37 bol rozdelený rovnomerne medzi úrovne „*nízkeho*“ a „*stredného*“ rizika. Do úrovne „*nízkeho*“ rizika budú klasifikované spracovateľské činnosti, ktorých celková hodnota závažnosti rizika nepresiahne hodnotu 28. Zároveň nesmie byť dielčia závažnosť jednotlivých aspektov kategorizovaná do úrovne vysokej závažnosti, tj. dielčie závažnosti vybraných aspektov môžu dosahovať

[62] Pre druhý príklad bol ako referenčný materiál použitý dokument [26].

maximálne hodnotu 5 a pritom maximálne jeden charakteristický aspekt môže byť ohodnotený závažnosťou z intervalu strednej závažnosti rizika (hodnota závažnosti = 5)[63]. V takom prípade musia byť ostatné aspekty zvyšných $(n-1)$ kritérií ohodnotené závažnosťou s hodnotou maximálne 4.

Poslednou možnou klasifikáciou je úroveň „*stredného*“ rizika. Do tejto úrovne budú klasifikované spracovateľské činnosti, ktorých celková hodnota závažnosti rizika nepresiahne hodnotu 38. Zároveň môže byť maximálne jedna[64] z dielčích závažností jednotlivých charakteristických aspektov kategorizovaná do úrovne vysokej závažnosti, tj. maximálne jeden aspekt môže mať hodnotu závažnosti vyššiu než 5. Ostatné aspekty zvyšných $(n-1)$ kritérií v takom prípade nesmú presahovať hodnotu závažnosti 5.

Výsledkom činnosti aplikácie je teda klasifikácia posudzovanej spracovateľskej činnosti na základe hodnoty celkovej závažnosti rizika (s prihliadnutím na všetky vyššie uvedené pravidlá) do jednej zo štyroch kategórií a taktiež kvalitatívne ohodnotenie stanoveného rizika, vychádzajúce z kvantitatívneho ohodnotenia pomocou kumulatívneho súčtu, vo forme slovného popisu spolu s odporúčaním pre prevádzkovateľa, resp. akéhokoľvek užívateľa aplikácie, aké ďalšie kroky je, vzhľadom na výslednú úroveň závažnosti rizika, potrebné či aspoň vhodné podniknúť, aby nebolo ohrozené zabezpečenie súladu posúdeného spracúvania s Nariadením. Jedná sa najmä o informáciu vzťahujúcu sa na nutnosť vykonania komplexného posúdenia *DPIA*. V prípade, kedy je riziko, ktoré môže v dôsledku realizácie spracovateľských činností vyvolať zásah do práv a slobôd subjektov údajov, klasifikované ako „*vysoké*“, je užívateľ upozornený na neodkladné vykonanie *DPIA* s prihliadnutím na pokyny stanovené čl. 35 Nariadenia. Pokiaľ je výsledné riziko klasifikované nižším stupňom celkovej závažnosti, tj. stredné, nízke alebo zanedbateľné, je vykonanie *DPIA* nanajvýš doporučené. Kategorizáciu rizík spolu s popisom, s ktorým bude po uskutočnení procesu posúdenia užívateľ oboznámený, uvádza tab. 5.2.

[63] V prípade, kedy sú implementované mechanizmy šifrovania alebo pseudonymizácie, sú pre všetky popísané pravidlá záverečnej klasifikácie uvažované dielčie hodnoty závažností už po znížení vplyvom koeficientu s hodnotou $k = 0.67$.

[64] Výnimkou sú jedine dve situácie, kedy by boli do jedinečného súboru charakteristík posudzovaných činností súčasne zahrnuté dva kritické aspekty (tj. s označením X), ktoré spoločne odkazujú na jeden a ten istý bod stanoviska WP29. Konkrétne sa jedná o dvojice vysokorizikových aspektov kritérií 5 a 6, druhú výnimku potom tvorí dvojica vysokorizikových aspektov kritérií 1 a 10B. Jedná sa teda o tú istú výnimku, ktorá bola už popísaná pri vylúčení pravidla automatického zaradenia posudzovaného spracúvania medzi „*vysokorizikové*“. Takáto situácia je pre klasifikáciu do úrovne *stredného* rizika prípustná.

Tab. 5.2: Klasifikácia rizík v závislosti na celkovej hodnote závažnosti rizika.

Úroveň rizika	**Celková závažnosť**	**Popis – informácia pre užívateľa**
Vysoké riziko	≥ 38	V dôsledku realizácie spracúvania hrozí subjektom údajov zásah do práv a slobôd spôsobom, kedy môžu pociťovať výrazné nepríjemnosti a následky bez možnosti prekonať ich. Takéto riziko je neprípustné. Je nevyhnutné podrobiť spracovateľské činnosti procesu posúdenia vplyvu na ochranu údajov (*DPIA*).
Stredné riziko	$\langle 28;\ 38)$	V dôsledku realizácie spracúvania hrozí subjektom údajov zásah do práv a slobôd spôsobom, kedy môžu pociťovať výrazné nepríjemnosti a následky. Takéto riziko je dlhodobo neprípustné. Je preto vhodné podrobiť spracovateľské činnosti procesu posúdenia vplyvu na ochranu údajov (*DPIA*).
Nízke riziko	$(17;\ 28)$	V dôsledku realizácie spracúvania hrozí subjektom údajov nepatrný zásah do práv a slobôd. Takéto riziko je považované za prijateľné. Z preventívnych dôvodov je možné podrobiť spracovateľské činnosti procesu posúdenia vplyvu na ochranu údajov (*DPIA*).
Zanedbateľné riziko	≤ 17	V dôsledku realizácie spracúvania nehrozí subjektom údajov zásah do práv a slobôd. Riziko je považované za prijateľné. Spracovateľské činnosti nie je nutné podrobiť procesu posúdenia vplyvu na ochranu údajov (*DPIA*).

ZÁVER

Bakalárska práca priniesla pohľad do problematiky posudzovania rizík pri spracúvaní osobných údajov s následným návrhom vlastnej metodiky, ktorá môže slúžiť ako návod pre prevádzkovateľov spracúvania pri realizácií posúdenia rizík nimi vedenej spracovateľskej činnosti. Konečným výstupom tejto záverečnej práce je webová aplikácia, ktorá poskytuje jej užívateľom možnosť podrobiť spracovateľské činnosti s osobnými údajmi procesu posúdenia rizík za účelom stanovenia miery závažnosti rizika, ktoré by mohlo v dôsledku vykonávania daných činností nepriaznivo zasiahnuť do práv a slobôd subjektov spracúvaných údajov.

Teoretická časť spočiatku poskytla popis problematiky riadenia rizík vo všeobecnosti. Vo svojich ďalších častiach ju následne preniesla do roviny spracúvania osobných údajov, kde tento proces popisuje s jeho príslušnými špecifikami. Predstavená bola taktiež súčasná legislatívna úprava ochrany osobných údajov, pričom je zvýšená pozornosť venovaná Nariadeniu, konkrétne článku 24, ktorý zavádza pre prevádzkovateľa spracúvania všeobecnú povinnosť v podobe nutnosti monitorovať potenciálne riziká a následne, v prípade potreby, zvyšovať mieru zabezpečenia prebiehajúceho spracúvania osobných údajov prijatím opatrení eliminujúcich vznik rizika pri danom spracúvaní, aby bolo možné uchrániť práva a slobody subjektov údajov pred nežiadúcim zásahom. Túto všeobecnú povinnosť ďalej prehlbuje článok 35 Nariadenia popisujúci podmienky nutnosti a následné postupy pre vykonanie posúdenia vplyvu na ochranu údajov v prípade, kedy spracúvanie môže predstavovať vysoké riziko pre práva a slobody subjektov údajov. Nakoľko je vykonanie plného *DPIA* viazané na výsledok prvotne realizovaného všeobecného posúdenia rizík, ktoré predstavuje prostriedok pre identifikovanie miery rizika pre práva a slobody, a vo svojej podstate je teda možné vykonané všeobecné posúdenie (v zmysle čl. 24 Nariadenia) chápať ako nevyhnutnú súčasť vykonania plného *DPIA*, nemohla byť ani táto problematika v texte opomenutá.

Ďalšia časť textu predstavila vlastný návrh metodiky pre všeobecné posudzovanie rizík spracúvania osobných údajov. Metodika sa snaží o prepojenie roviny posudzovania rizík, ktorého vykonanie súvisí s riadením rizík informačnej bezpečnosti nad prevádzkovaným informačným systémom zapojeným do realizácie činností spracúvania osobných údajov, a roviny, ktorá venuje pozornosť dôležitej otázke ochrany osobných údajov. Druhá rovina dopĺňa základný proces posúdenia rizík o niektoré špecifické kroky zamerané na vymedzenie a vyhodnotenie parametrov jedinečných pre posudzovaný proces spracúvania osobných údajov. Návrh vlastnej metodiky posudzovania rizík v kontexte ochrany osobných údajov zároveň do istej miery umožnil predstaviť i známu metodiku

PIA od francúzskeho dozorného úradu CNIL, ktorá stanovuje jedinečné kroky špecifické v rámci procesu posúdenia rizík práve v kontexte spracúvania osobných údajov, a prístup k riadeniu rizík informačnej bezpečnosti podľa normy ISO 27005, nakoľko na základe mnohých princípov a postupov z oboch uvedených metodík bolo zrealizované vytvorenie metodiky vlastnej. Výsledkom, po vykonaní procesu posúdenia rizík s využitím navrhnutej uvedenej metodiky, je pre prevádzkovateľa kompletný zoznam identifikovaných a ohodnotených rizík, čo mu umožní získať prehľad o tom, aké nežiadúce zásahy môžu v dôsledku realizácie posudzovaného procesu spracúvania údajov pre práva a slobody subjektov údajov nastať.

Pre lepšie pochopenie aplikácie navrhnutej metodiky do praxe je v závere teoretickej časti práce uvedená modelová situácia popisujúca využitie metodiky pre posúdenie konkrétneho procesu spracúvania osobných údajov. Tento dodatok vo forme názorného príkladu má slúžiť len k lepšiemu pochopeniu celého priebehu procesu posúdenia rizík, ktorý je stanovený navrhnutou metodikou, na základe aplikácie jednotlivých krokov posúdenia na konkrétne parametre súvisiace s posudzovanou spracovateľskou operáciou, nejedná sa preto o reálny príklad prevedený v kompletnom rozsahu.

Konečným výstupom bakalárskej práce je aplikácia pre posudzovanie rizík, ktorá svojim užívateľom slúži ako pomocný nástroj pri vykonávaní všeobecného posúdenia rizík spracúvania osobných údajov za účelom stanovenia závažnosti rizika pre práva a slobody subjektov údajov. Vytvorená aplikácia je dostupná prostredníctvom webového informačného portálu, na ktorom užívateľ nájde, okrem aplikácie, taktiež množstvo užitočných informácií týkajúcich sa problematiky spracúvania osobných údajov a ich ochrany. Pre získanie dostatočného povedomia užívateľa sú v rámci informačného portálu vysvetlené základné pojmy a definície príznačné pre terminológiu v kontexte ochrany a spracúvania osobných údajov. Užívateľ taktiež prostredníctvom portálu získa značný prehľad o význame a uplatnení samotného Nariadenia, či už z pohľadu povinností prevádzkovateľov, alebo naopak z pohľadu práv subjektov údajov, ktoré si pri spracúvaní ich osobných údajov môžu uplatniť. V čase odovzdania bakalárskej práce sú všetky príslušné kódy webovej aplikácie uložené v Git[65] repozitári, vďaka čomu je možné webovú stránku s príslušnou aplikáciou navštíviť taktiež spôsobom zadania URL adresy https://xvoska00.github.io/bp-hodnotenie-rizik/ do užívateľom preferovaného webového prehliadača.

[65] Git je verzovací systém, ktorý umožňuje ukladať postupne celú históriu projektu, monitorovať jednotlivé zmeny a v prípade potreby umožňuje aj návrat k predošlým verziám počas vývoja projektu, resp. aplikácie.

Princíp činnosti webovej aplikácie je založený na vyhodnocovaní dotazníkového formulára obsahujúceho niekoľko kritérií, ktoré je potrebné pri posudzovaní závažnosti rizika spracúvania osobných údajov vyhodnotiť. Samotný užívateľ pomocou korektného vyplnenia formulára pomôže bližšie špecifikovať spracúvanie, ktoré chce podrobiť procesu posúdenia, čím vytvorí pre konkrétne posudzované spracúvanie jedinečnú charakteristiku príslušných aspektov, ktorú následne aplikácia vyhodnocuje. Výsledkom činnosti aplikácie je jednak informácia o miere závažnosti rizika posudzovaných spracovateľských činností pre práva a slobody subjektov spracúvaných údajov a klasifikácia výsledného rizika do jednej zo štyroch úrovní práve na základe celkovej hodnoty závažnosti, a taktiež informácia, resp. odporučenie pre užívateľa v súvislosti s nutnosťou vykonania plného posúdenia *DPIA*.

Popísanú aplikáciu pre posudzovanie rizík by bolo možné do budúcnosti pre širšie a plnohodnotnejšie využitie rozšíriť naviac o implementáciu procesu riadenia rizík z hľadiska managementu informačnej bezpečnosti. Tento komplexný proces nebol do činnosti aplikácie implementovaný samostatne, nakoľko by tým boli prekročené požiadavky na rozsah a náročnosť vytvorenia funkčného výstupu tejto záverečnej práce. Aplikácia preto uvažuje len tie aspekty týkajúce sa adekvátneho zabezpečenia informačných systémov a organizačných štruktúr v rámci spracúvania osobných údajov, ktoré je nevyhnutné uvažovať ako súčasť všeobecného posúdenia rizík v kontexte ochrany osobných údajov.

LITERATÚRA

[1] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 488 s. ISBN 978-80-247-4644-9.

[2] *ČSN ISO 27005: Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2013.

[3] HÁLEK, V. *Krizový management – teorie a praxe*. Bratislava: DonauMedia, 2008, 322 s. ISBN 978-80-89364-00-8.

[4] *ČSN ISO 31000: Management rizik – Principy a směrnice.* 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. 2010.

[5] MVČR. Orientace v GDPR. *Co je GDPR – Ochrana osobních údajů.* [online]. 2017, © Ministerstvo vnitra České republiky. [cit. 2021-05-26]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

[6] NULÍČEK, M., DONÁT, J., NONNEMANN, F. aj. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář*. Praha: Wolters Kluwer ČR, 2017, 544 s. ISBN 978-90-7552-765-3.

[7] CNIL. *Methodology for Privacy Risk Management, June 2012 edition* [online]. 2012, 31 s. [cit. 2020-12-11]. Dostupné z: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

[8] ICO. *Conducting privacy impact assessments code of practice. Data Protection Act*. [online] [cit. 2020-12-11]. Dostupné z: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

[9] QUELLE, Claudia. *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach*. European Journal of Risk Regulation [online]. 2018, roč. 9, s. 502 – 526. [cit. 2021-05-26].

[10] COGLIANESE, Cary. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, roč. 50, č. 3, s. 525–564. ISSN 0363-602X.

[11] MÍŠEK, Jakub. *Osobní údaje v čase a prostoru. Role performativní regulace v ochraně osobních údajů* [online] Brno. 2019, 231 s. [cit. 2020-12-11]. Dostupné z: https://is.muni.cz/th/wpa9m/dis_final_03.pdf. Disertační práce. Masarykova univerzita, Právnická fakulta, Ústav práva a technologií. Vedoucí práce Radim Polčák.

[12] WP29. *Usmernenia týkajúce sa posúdenia vplyvu na ochranu údajov a stanovenie toho, či na účely nariadenia 2016/679 spracúvanie „pravdepodobne povedie k vysokému riziku*“ [online]. 2017, 26 s. [cit. 2020-12-11]. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[13] ŠVOLÍK, Oliver. *Řízení rizik v ochraně osobních údajů* [online]. Brno, 2019 [cit. 2020-12-11]. Dostupné z: https://is.muni.cz/th/jeyno/DP-Oliver-Svolik-Rizeni_rizik_v_ochrane_osobnich_udaju.pdf. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Jakub Harašta.

[14] *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, v. 2 of 13 September 2018* [online]. Brusel: Smart Grid Task Force, 2018, 101 s. [cit. 2020-12-11]. Dostupné z: https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

[15] WP29. *Stanovisko 06/2014 k pojmu legitímne záujmy prevádzkovateľa podľa článku 7 smernice 95/46/ES* [online]. 2014, 72 s. [cit. 2020-12-11]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_sk.pdf

[16] CNIL. *Privacy Impact Assessment (PIA): Knowledge Bases, February 2018 edition* [online]. 2018, 109 s. [cit. 2020-12-11]. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

[17] BOLDYREVA, E. L., DUYSEMBINA, E. & GRISHINA, N. Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. In *18th PCSF 2018 Professional Culture of the Specialist of the Future*. Future Academy. 2018, s. 91-102. (The European Proceedings of Social & Behavioural Sciences). [cit. 2021-05-26]. Dostupné z: https://doi.org/10.15405/epsbs.2018.12.02.10

[18] WILSON, R. European Conference on Cyber Warfare and Security. *Cambridge Analytica, Facebook, and Influence Operations: A Case Study and Anticipatory Ethical Analysis*. 2019, ProQuest Central. 11 s. [cit. 2021-05-26]. Dostupné z: https://www.proquest.com/conference-papers-proceedings/cambridge-analytica-facebook-influence-operations/docview/2261006731/se-2?accountid=17115

[19] WP29. *Usmernenia o oznámení porušenia ochrany osobných údajov podľa nariadenia 2016/679* [online]. 2017, 32 s. [cit. 2020-12-11].. Dostupné z: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[20] Európska komisia. *Druhy právnych predpisov EÚ* [online]. [cit. 2020-12-11]. Dostupné z: https://ec.europa.eu/info/law/law-making-process/types-eu-law_sk

[21] *ČSN ISO 31010: Management rizik – Techniky posuzování rizik*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[22] NIST. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* Gaithersburg: Information Technology Laboratory, National Institute Of Standards And Technology [online]. 2002. 65 s. [cit. 2020-12-11]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

[23] Znalostní systém prevence rizik v BOZP. *Pracovní úrazy. Odškodňování pracovních úrazů a nemocí z povolání z pohledu zákonné pojišťovny* [online]. [cit. 2020-12-11]. Dostupné z: https://zsbozp.vubp.cz/zdravi/pracovni-urazy/593-odskodnovani-pracovnich-urazu-a-nemoci-z-povolani-z-pohledu-zakonne-pojistovny

[24] Bootstrap. *Build fast, responsive sites with Bootstrap*. [online]. [cit. 2021-05-26]. Dostupné z: https://getbootstrap.com/

[25] Start Bootstrap. *Freelancer – a Bootstrap portfolio theme*. [online]. [cit. 2021-05-26]. Dostupné z: https://startbootstrap.com/theme/freelancer

[26] ÚOOÚ. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů*. [online]. 2020, 16 s. © Úřad pro ochranu osobních údajů. [cit. 2021-05-26]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940

[27] ÚOOÚ. *K povinnosti správců provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. [online]. 2020, 9 s. © Úřad pro ochranu osobních údajů. [cit. 2021-05-26]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003

[28] BARKER, Elaine. *Recommendation for key management-part 1: General*. In NIST Special Publication. 2016, 161 s. [online]. [cit. 2021-05-26]. Dostupné z: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4

Právne pramene a judikatúra

[29] *Rozsudok SDEÚ vo veci Patrick Breyer proti Bundesrepublik Deutschland zo dňa 19. októbra 2016. Vec C-582/17.* In: InfoCuria [právny informačný systém]. © Európska únia. [cit. 2020-12-11]. Dostupné z: http://curia.europa.eu/juris/documents.jsf?num=C-582/14

[30] *Nariadenie Európskeho parlamentu a Rady (EU) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)*. In: EUR-Lex. [právny informačný systém]. © Úrad pre vydávanie publikácií Európskej únie. [cit. 2020-12-11]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:32016R0679&from=SK

[31] *Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů*. In: Zákony pro lidi [právny informačný systém]. AION CS, s.r.o. [cit. 2020-12-11]. Dostupné z: https://zakonyprolidi.cz/cs/2000-101

[32] *Zákon č. 262/2006 Sb., zákoník práce, v znění pozdějších předpisů*. In: Zákony pro lidi [právny informačný systém]. AION CS, s.r.o. [cit. 2020-12-11]. Dostupné z: https://zakonyprolidi.cz/cs/2006-262

[33] *Charta základných práv Európskej únie*. In: EUR-Lex [právny informačný systém]. © Úrad pre vydávanie publikácií Európskej únie. [cit. 2020-12-11]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/HTML/?uri=CELEX:12012P/TXT&from=SK

ZOZNAM POUŽITÝCH SKRATIEK

CSS	Cascading Style Sheets
DPIA	Posúdenie vplyvu na ochranu osobných údajov
EÚ	Európska únia
HTML	Hypertext Markup Language
Nariadenie	Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
Charta EÚ	Charta základných práv Európskej únie
Smernica 95/46	Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov
SDEÚ	Súdny dvor Európskej únie
PIA	Privacy Impact Assessment
ÚOOÚ	Úřad pro ochranu osobních udajů
WP29	Pracovná skupina zriadená podľa článku 29 Smernice 95/46

ZOZNAM PRÍLOH

DODATOK

Práca so súbormi obsahujúcimi zdrojové kódy k webovej aplikácii

Zobrazenie stránok webovej aplikácie, resp. webového informačného portálu, ktorého súčasťou je aj implementovaná aplikácia pre posudzovanie rizík, prebieha pomocou otvorenia súboru *docs/index.html*, ktorý je súčasťou archívu `bp-hodnotenie-rizik.zip` obsahujúceho elektronickú prílohu, v niektorom z dostupných webových prehliadačov. Niektoré funkcie, najmä presmerovania na ďalšie webové lokality, vyžadujú aktívne internetové pripojenie.

Príloha A – Obsah archívu s elektronickou prílohou

Priložený archív *bp-hodnotenie-rizik.zip* obsahuje zdrojové kódy k vytvorenej webovej aplikácií ku dňu 31. 5. 2021.

Príloha B – Zoznam posudzovaných kritérií

kritérium 1 – kategórie zhromažďovaných údajov

ZÁVAŽNOSŤ	**Kategórie zhromažďovaných údajov o subjektoch údajov**
X[66]	sú spracúvané zvláštne kategórie údajov a údaje týkajúce sa rozsudkov trestných činov spáchaných subjektom údajov *citlivé osobné údaje*
X	zaznamenané údaje je možné využiť pre profilovanie užívateľov alebo pre účely automatizovaného rozhodovania *napr. údaje z logov, história navštívených webových stránok, údaje vypovedajúce o uskutočnení telefonických hovorov, údaje vypovedajúce o využívaní komunikácie prostredníctvom elektronickej pošty + finančné údaje (o stave majetku, výške disponibilných finančných prostriedkov, údaje o pôžičkách a finančných dlhoch)*
5	údaje, ktoré umožňujú, v prípade ich zneužitia, vystupovať v mene subjektu údajov *prístupové meno, heslo/PIN, pseudonym*
6	údaje umožňujúce jednoznačnú identifikáciu subjektu údajov *do tejto skupiny osobných údajov radíme jednoznačné identifikátory ako napr. rodné číslo, číslo občianskeho preukazu, číslo vodičského preukazu, číslo cestovného dokladu (pas), číslo sociálneho poistenia, číslo zdravotného poistenia*
5	údaje umožňujúce prístup a manipuláciu k finančným prostriedkom subjektu údajov *spracovanie zahŕňa údaje ako napr. meno aj priezvisko, titul, dátum narodenia, adresa pobytu, číslo platobnej karty, heslo/PIN, telefónne číslo, e-mailová adresa, informácie o vlastníctvach subjektu údajov*
1	ostatné osobné údaje *údaje, ktoré samé o sebe neumožnia jednoznačnú identifikáciu – softbiometrické údaje (váha, výška, vek, pohlavie, farba vlasov, farba očí, typ postavy apod.), bežné obrazové záznamy, ktoré vznikli z dôvodu oprávneného monitorovania určitej oblasti napr. pre zaistenie bezpečnosti atď.*

[66] Pokiaľ sa u niektorých aspektov nachádza v mieste pre hodnotu závažnosti rizika daného aspektu označenie „X“, znamená to, že tento aspekt odkazuje na jeden z deviatich vysokorizikových bodov spracúvania definovaných v stanovisku WP29 [12]. V rámci činnosti aplikácie je pre tieto aspekty uvažovaná hodnota závažnosti 7.

kritérium 2 – miera identifikovateľnosti subjektu údajov

ZÁVAŽNOSŤ	**Identifikácia dotknutej osoby**
6	na základe zaznamenaných údajov je možné subjekt jednoznačne identifikovať a lokalizovať *jedná sa najmä o spracovanie údajov monitorujúcich pohyb identifikovateľných subjektov údajov*
5	na základe zaznamenaných údajov je možné subjekt jednoznačne identifikovať a rozpoznať *jedná sa najmä o spracovanie obrazových záznamov identifikovateľných subjektov údajov*
4	na základe zaznamenaných údajov je možné subjekt jednoznačne identifikovať
1	na základe zaznamenaných údajov nie je možné subjekt jednoznačne identifikovať

kritérium 3 – miera zraniteľnosti subjektu údajov

ZÁVAŽNOSŤ	**Subjekt údajov**
X	subjekt údajov spadá do kategórie stále zraniteľných subjektov *do tejto kategórie radíme osoby, ktoré sa v rámci celej spoločnosti dostávajú, na základe istých špecifických prvkov, do znevýhodnenej pozície – vymedzené skupiny obyvateľstva podľa národnosti, náboženstva, sexuálnej orientácie, telesného a mentálneho hendikepu, odsúdenia za spáchanie trestného činu apod.*
4	subjekt údajov z istého dôvodu v danej fáze svojho života spadá do skupiny zraniteľných subjektov *do tejto kategórie radíme osoby, ktoré nemožno považovať za osoby stále znevýhodnené, avšak počas určitého obdobia svojho života nadobúdajú isté faktory, ktoré ich stavajú do znevýhodnenej pozície voči celej spoločnosti – migranti, osoby lietacie sa zo závažného ochorenia, staršie osoby (v dôchodkovom veku), deti a mladiství*
1	subjekt údajov nedisponuje vlastnosťami, na základe ktorých ho možno zaradiť medzi zraniteľné subjekty

kritérium 4 – rozsah spracúvania osobných údajov

ZÁVAŽNOSŤ	**Rozsah spracovania osobných údajov**
X	veľký rozsah spracovania *viac než 10 tisíc subjektov údajov a/alebo viac než 20 osôb oprávnených pristupovať k spracúvaným údajom a/alebo viac než 20 miest, na ktorých je realizovanie spracúvané a zároveň úroveň štátu z hľadiska umiestnenia subjektov údajov*
4	stredný rozsah spracovania *viac než 5 tisíc subjektov údajov a/alebo viac než 2 osoby oprávnené pristupovať k spracúvaným údajom a/alebo viac než 5 miest, na ktorých je realizovanie spracúvané a zároveň úroveň regiónu/kraja z hľadiska umiestnenia subjektov údajov*
1	malý rozsah spracovania *najviac 5 tisíc subjektov údajov a/alebo najviac 2 osoby oprávnené pristupovať k spracúvaným údajom a/alebo najviac 4 miesta, na ktorých je realizovanie spracúvané a zároveň úroveň najmenej obce z hľadiska umiestnenia subjektov údajov*

kritérium 5 – sústavnosť zhromažďovania osobných údajov

ZÁVAŽNOSŤ	**Je zber spracúvaných údajov realizovaný nepretržite?**
X	áno *dlhodobé, sústavné, opakované, pravidelné a systematické monitorovanie a zber údajov*
1	nie *krátkodobé, jednorazové, dočasné, príležitostné monitorovanie a zber údajov*

kritérium 6 – monitorovanie verejných priestorov

ZÁVAŽNOSŤ	**Zahŕňa realizované spracúvanie aj snímanie verejne prístupných priestorov?**
X	je uskutočňované snímanie verejne prístupných miest *snímanie miest so zvýšenou koncentráciou obyvateľstva ako napr. verejných priestranstiev, pasáží, letísk apod. prostredníctvom kamerových systémov*

4	je uskutočňované snímanie miest verejne obmedzene prístupných *snímanie s nevýraznou koncentráciou obyvateľstva ako napr. interiérov verejných budov, bytových objektov, súkromných pozemkov majiteľa apod.*
1	snímanie verejne prístupných priestorov nie je realizované

kritérium 7 – zverejňovanie zaznamenaných osobných údajov

ZÁVAŽNOSŤ	**Prístupnosť osobných údajov**
6	zaznamenané údaje sú verejne prístupné neobmedzenému počtu subjektov *údaje sú v rámci spracúvania sprístupňované verejnosti napr. na základe právnych predpisov*
4	zaznamenané údaje sú verejne prístupné obmedzenému počtu subjektov *údaje sú v rámci spracúvania sprístupňované obmedzenej skupine iných subjektov, ktorú musí prevádzkovateľ vopred presne a jednoznačne vymedziť*
1	zaznamenané údaje nie sú verejne prístupné *údaje sú v rámci spracúvania sprístupňované len prevádzkovateľovi a/alebo sprostredkovateľovi spracúvania, prípadne orgánom verejnej moci na základe právnych predpisov*

kritérium 8 – inovatívnosť riešení spracúvania

ZÁVAŽNOSŤ	**Sú pre realizáciu spracúvania využívané automatizované systémy vrátane umelej inteligencie?**
X	áno
1	nie *vykonávané činnosti využívajú jednoduché zreťazenie základných operácií na princípe ľahko realizovateľného a pochopiteľného výpočtového algoritmu*

kritérium 9 – kombinovanie a prepájanie osobných údajov

ZÁVAŽNOSŤ	**Dochádza ku kombinovaniu zaznamenaných údajov s údajmi, ktoré boli získané za iným účelom?**
X	áno
1	nie

kritérium 10 – predávanie osobných údajov

ZÁVAŽNOSŤ	**Existujú tretie strany, ktorým sú zaznamenané údaje poskytované?**
–	áno[67]
1	nie

kritérium 10A – charakteristika oblasti pôsobnosti tretej strany

ZÁVAŽNOSŤ	**Sú osobné údaje predávané v rámci územia EÚ?**
6	osobné údaje sú predávané do štátov s nezaistenou úrovňou ochrany mimo EÚ *súčinnosť s daným typom tretej strany je vykonávaná na základe článku 49 Nariadenia GDPR*
4	osobné údaje sú predávané do štátov so zaistenou úrovňou ochrany mimo EÚ *súčinnosť s daným typom tretej strany je vykonávaná na základe článku 46 Nariadenia GDPR*
1	zaznamenané údaje nie sú verejne prístupné

[67] V prípade, že je v rámci spracovateľských činností realizované aj predávanie osobných údajov tretej strany, tak je dodatočne posudzovaný ešte účel predávania osobných údajov tretej strane a tiež pôsobnosť tejto tretej strany z hľadiska príslušnosti medzi krajiny s adekvátnou úrovňou ochrany údajov. V prípade, že je teda zvolená možnosť „*áno*“, sú užívateľovi sprístupnené otázky 10A a 10B. Až po ich zodpovedaní môže pristúpiť k zodpovedaniu ďalších otázok (tj. 11 – 15). Pokiaľ je zvolená možnosť „*nie*“, ako nasledujúca je sprístupnená priamo otázka 11.

kritérium 10B – účel predávania údajov tretej strane

ZÁVAŽNOSŤ	**Za akým účelom sú osobné údaje poskytované tretím stranám?**
1	osobné údaje sú predávané sprostredkovateľovi spracúvania, ktorý vykonáva spracúvanie týchto údajov na základe poverenia nadobudnutého od prevádzkovateľa spracúvania
1	osobné údaje sú predávané medzi spoločnými prevádzkovateľmi realizujúcimi spracúvanie pre plnenie spoločného účelu
1	osobné údaje sú predávané za účelom zabezpečenia nevyhnutnej zdravotnej starostlivosti poskytnutej subjektu údajov
1	osobné údaje sú predávané za účelom plnenia zmluvy, ktorej zmluvnou stranou je subjekt údajov
X	osobné údaje sú predávané za účelom vytvárania bodového ohodnotenia subjektu údajov
4	osobné údaje sú predávané k marketingovým účelom

kritérium 11 – uplatnenie práv subjektov údajov

ZÁVAŽNOSŤ	**Môže si subjekt údajov uplatniť práva k prebiehajúcemu spracúvaniu?**
1	subjekt údajov má právo ovplyvniť spracúvanie údajov a ich prípadné poskytovanie *tie spracovania, kedy si subjekt môže bez problémov presadiť všetky práva vyplývajúce z Nariadenia GDPR*
4	subjekt údajov má obmedzené právo ovplyvniť spracúvanie údajov a ich prípadné poskytovanie *tie spracovania, kedy si subjekt môže presadiť práva vyplývajúce z Nariadenia GDPR napr. v obmedzenom časovom úseku alebo za vymedzených podmienok; jedná sa najmä o činnosti spracúvania takých údajov, ktoré sú potrebné k uplatneniu práv vyplývajúcich zo zákona, napr. pri uzatváraní licenčných zmlúv.*

X	subjekt údajov nemá právo ovplyvniť spracúvanie údajov a ich prípadné poskytovanie *tie spracovania, kedy si subjekt môže len obmedzene alebo vôbec nemôže presadiť svoje práva vyplývajúce z Nariadenia GDPR; jedná sa najmä o činnosti spracúvania založené na plnení zákonnej povinnosti prevádzkovateľa.*

kritérium 12 – zabezpečenie prístupu k osobným údajom

ZÁVAŽNOSŤ	**Sú implementované adekvátne opatrenia pre zabezpečenie fyzického a administratívneho prístupu k spracúvaným údajom?**
6	nie
1	áno *otázka fyzického zabezpečenia osobných údajov sa týka zabezpečenia prístupu do objektov, z ktorých je možné realizovať prístup k osobným údajom, či priamo k zariadeniam, ktoré slúžia ako úložisko týchto údajov; zabezpečenie administratívneho prístupu spočíva v zabezpečení prístupu do databáz či úložísk, v ktorých sú osobné údaje uchovávané, tj. používanie prístupového hesla spĺňajúceho požiadavky pre dostatočne silné heslo, znalosť prístupového hesla len pre osoby oprávnené pristupovať k údajom, rozlíšenie privilégií oprávnených osôb v rámci manipulácie s uchovávanými údajmi*

kritérium 13 – úroveň informovanosti osôb s oprávneným prístupom k údajom

ZÁVAŽNOSŤ	**Sú osoby oprávnené pristupovať k spracúvaným údajom dostatočne a pravidelne informované o zásadách vykonávania spracúvania?**
1	áno, tieto osoby sú účastné pravidelných školení
4	áno, tieto osoby boli poučené jednorazovo
5	nie

kritérium 14 – aplikácia dodatočných prostriedkov zabezpečenia

ZÁVAŽNOSŤ	**Sú spracúvané osobné údaje podrobené procesu šifrovania a/alebo pseudonymizácie?**
-	áno
-	nie

kritérium 15 – dostupnosť osobných údajov

ZÁVAŽNOSŤ	**Je zaistená neustála dostupnosť systému a služieb spracúvania?**
1	áno, pravdepodobnosť výpadku systému a služieb spracúvania je zanedbateľná
1	áno, v prípade výpadku systému a/alebo služieb spracúvania je možné obnoviť dostupnosť osobných údajov a prístup k nim včas *v prípade výpadku systému a služieb spracúvania je možné na nevyhnutný čas, potrebný pre zabezpečenie prístupu k údajom počas doby trvania výpadku, využiť aj záložné kópie uchovávaných údajov, ak sú vedené*
3	nie je možné garantovať neustálu dostupnosť systému a služieb spracúvania, ale zároveň je dočasná nedostupnosť údajov prijateľná *tie spracovania, kedy by nedostupnosť osobných údajov nespôsobila kritické obtiaže pre subjekty údajov*
6	nie je možné garantovať neustálu dostupnosť systému a služieb spracúvania a zároveň je dočasná nedostupnosť údajov neprijateľná *tie spracovania, kedy by nedostupnosť osobných údajov mohla mať za následok vznik kritickej situácie pre subjekt údajov, napr. nedostupnosť zdravotnej dokumentácie pacienta pri nasadzovaní liečby*