Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Zajištění souladu s GDPR na ČZU

Bc. Vlachynský Petr

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Petr Vlachynský

Ekonomika a management
Provoz a ekonomika

Název práce

Zajištění souladu s GDPR na ČZU

Název anglicky

GDPR complience on CZU

Cíle práce

Tato diplomová práce se zabývá procesem zajištění souladu s GDPR na České zemědělské univerzitě v Praze. Hlavním cílem je posouzení vlivu ochrany osobních údajů (DPIA) u vybraných zpracování, která mají za následek vysoké riziko pro práva a svobody subjektů údajů. Součástí bude posouzení kritičnosti zpracování, identifikace a hodnocení hrozeb a návrh opatření pro zajištění ochrany osobních údajů.

Metodika

Práci tvoří dvě hlavní části teoretická a praktická. Praktická část práce bude zpracována na základě dosažených výsledků z kvantitativního/kvalitativního výzkumu. Práce bude vypracována v níže uvedených postupových krocích za využití vědeckých metod.

1. Formulace cíle a metodiky práce.
2. Syntéza výchozí znalostní báze.
3. Charakteristika zvoleného subjektu.
4. Realizace kvantitativního/kvalitativního výzkumu.
5. Agregace získaných poznatků a tvorba vlastních návrhů.
6. Formální dokončení práce.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

GDPR, ochrana osobních údajů, ISO 27001, analýza rizik, kritičnost zpracování, identifikace a hodnocení hrozeb

---

Doporučené zdroje informací

KOLEKTIV AUTORŮ. ÚZ č. 1319 – Zpracování osobních údajů, GDPR. Ostrava: SAGIT, 2019. ISBN 978-80-7488-353-8

NONNEMANN, F – LIDINSKÝ, V. – MAŠÍN, D. Praktická příručka GDPR. Praha: KLIKA, 2018. ISBN 978-80-88298-10-6

ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Petr Hanzlík, Ph.D.

Garantující pracoviště

Katedra informačního inženýrství

Konzultant

Ing. Jan Borák, Ph.D.

Elektronicky schváleno dne 19. 2. 2020

Ing. Martin Pelikán, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 2. 2020

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 01. 04. 2020

Čestné prohlášení

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

V Praze dne 1.4.2020 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Petru Hanzlíkovi, Ph.D. za cenné rady při zpracování této diplomové práce. Dále bych rád poděkoval Ing. Janu Borákovi Ph.D. za konzultační rady během psaní práce. Velké poděkování zaslouží moje přítelkyně Ing. Michaela Pospěchová za užitečné rady použité při psaní mé práce.

Zajištění souladu s GDPR na ČZU

Abstrakt

Diplomová práce se zabývá problematikou ochrany osobních údajů v rámci Obecného nařízení o ochraně osobních údajů známým pod zkratkou GDPR. Práce se skládá z teoretické a praktické části. Teoretická část popisuje právní základ, základní pojmy a opomíjeny nezůstávají ani hlavní zásady tohoto nařízení. Důkladně je popsána i analýza rizik opírající se o zákony a normy související s GDPR. Teoreticky je představen i hlavní cíl práce, a to posouzení vlivu na ochranu osobních údajů.

Praktická část diplomové práce je zaměřena na zajištění souladu České zemědělské univerzity v Praze s GDPR. Popsán je registr zpracování a jeho charakteristika, posouzena a vypočítána kritičnost zpracování. Jsou identifikovány hrozby a zranitelnosti, na jejichž základě je vypočítána suma zranitelnosti a míra rizika. Uvedeny a podrobně popsány jsou možnosti variant pro ošetření nalezených rizik a navrženy jak technická, tak organizační opatření pro zajištění ochrany osobních údajů. Na nejrizikovějším zpracování je pak ukázán konkrétní postup udržující soulad s GDPR na základě posouzení vlivu na ochranu osobních údajů.

Klíčová slova: GDPR, ochrana osobních údajů, ISO 27000, analýza rizik, kritičnost zpracování, identifikace a hodnocení hrozeb

GDPR compliance on CZU

Abstract

This diploma thesis deals with the issue of personal data protection of the General Data Protection Regulation known as GDPR. The work consists of theoretical and practical part. The theoretical part describes the legal basis, the basic concepts and the main principles of this regulation. Risk analysis based on GDPR related laws and standards is also thoroughly described. In theory, the main objective of the thesis, Data Protection Impact Assessment is described.

The practical part of the thesis is focused on ensuring GDPR compliance on the Czech University of Life Sciences in Prague. The processing register and its characteristics are described, the criticality of the processing with these values is evaluated and calculated. Threats and vulnerabilities are identified to calculate the sum of vulnerabilities and the level of risk. Possibilities of variants for dealing with found risks are presented and described in detail and both technical and organizational measures to ensure the protection of personal data are proposed. The most risky processing then shows a specific procedure for maintaining GDPR compliance based on a Data Protection Impact Assessment.

Keywords: GDPR, personal data protection, ISO 27000, risk analysis, criticality of processes, threat identification and assessment

Obsah

1 Úvod

Obecné nařízení o ochraně osobních údajů (dále také jen „GDPR“ - General Data Protection Regulation) je nařízení Evropské unie, které vstoupilo v platnost 25. května 2018.

GDPR stanovuje jasná pravidla pro zpracování a ochranu osobních údajů napříč zeměmi EU, neboť v den nabytí platnosti nahradilo zákony na ochranu osobních údajů jednotlivých členských zemí. To s sebou přineslo nejen výrazně vyšší ochranu osobních údajů občanů těchto zemí, ale i razantní zpřísnění pravidel pro organizace, které tyto údaje zpracovávají. V případě jejich porušení, hrozí společnostem vysoké pokuty.

Aby byla možná kontrola dodržování těchto pravidel, musí organizace, zpracovávající osobní údaje, dokládat tzv. soulad s GDPR, a to hned v několika kategoriích. Od poskytnutí informací o způsobu zpracovávání osobních údajů a právech jednotlivých subjektů, až po doložení komplexního registru zpracování a záznamech o posouzení vlivu na ochranu osobních údajů (dále také jen „DPIA“ – Data Protection Impact Assessment) u rizikových zpracování.

V této práci je na základě informací z dostupných zdrojů, zákonů a směrnic, odkazujících se na ochranu osobních údajů, a také praktických a cenných rad od Odboru bezpečnosti České zemědělské univerzity v Praze, vypracován dokument mapující současnou situaci na univerzitě a její soulad s GDPR.

2 Cíl práce a metodika

2.1 Cíl práce

Tato diplomová práce se zabývá procesem zajištění souladu s GDPR na České zemědělské univerzitě v Praze. Hlavním cílem je posouzení vlivu ochrany osobních údajů (DPIA) u vybraných zpracování, která mají za následek vysoké riziko pro práva a svobody subjektů údajů. Součástí bude posouzení kritičnosti zpracování, identifikace a hodnocení hrozeb a návrh opatření pro zajištění ochrany osobních údajů.

2.2 Metodika

Práci tvoří dvě hlavní části teoretická a praktická. Praktická část práce bude zpracována na základě dosažených výsledků z kvantitativního/kvalitativního výzkumu. Práce bude vypracována v níže uvedených postupových krocích za využití vědeckých metod.

1. Formulace cíle a metodiky práce.
2. Syntéza výchozí znalostní báze.
3. Charakteristika zvoleného subjektu.
4. Realizace kvantitativního/kvalitativního výzkumu.
5. Agregace získaných poznatků a tvorba vlastních návrhů.
6. Formální dokončení práce.

3 Teoretická východiska

Tato část práce se zabývá teoretickou rešerší a problematikou Obecného nařízení o ochraně osobních údajů (GDPR) a souvisejícího zákona č. 110/2019 Sb., o zpracování osobních údajů. Vysvětlena a detailněji popsána je rovněž problematika analýzy rizik spolu se Zákonem o kybernetické bezpečnosti a norem ČSN ISO/IEC 27000. Za účelem splnění požadavku GDPR na České zemědělské univerzitě v Praze je nutné provést posouzení vlivu na ochranu osobních údajů.

3.1 Právní základ

Právní rámec pro ochranu osobních údajů a jeho zpracování se vyvíjí a upravuje od konce 20. století. V současnosti je právo na ochranu osobních údajů zakotveno jak v české Listině základních práv a svobod, tak Listině základních práv Evropské unie. Podrobnější pravidla jsou dále zpracována v Úmluvě Rady Evropy č. 108 z roku 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat, a také v dodatkovém protokolu Rady Evropy z roku 2001 č. 181 k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat přes hranice (Nonnemann, 2018).

Konkrétní právní úprava s dopadem na všechny, kdo s osobními údaji pracují, byla vydána roku 1995 ve směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů na vnitrostátní úrovni pak zákonem č. 101/2000 Sb., o ochraně osobních údajů.

Evropská unie připravila před několika lety nový právní rámec pro zpracování osobních údajů. Výsledkem bylo nové obecné nařízení, známé jako General Data Protection Regulation (GDPR) (Nonnemann, 2018), které bylo roku 2019 doplněno o dnes již platný adaptační zákon č. 110/2019 Sb., o zpracování osobních údajů.

3.2 GDPR

Dne 25.5. 2018 vstoupilo v platnost a účinnost Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o zrušené směrnici 95/46/ES, zkráceně známé jako obecné nařízení o ochraně osobních údajů (GDPR). Tvoří tak nový právní rámec ochrany osobních údajů v evropském prostoru.

GDPR je závazné pro všechny státy Evropské unie spolu s Norskem, Islandem a Lichtenštejnskem, a je tak nadřazeno zákonům o ochraně osobních údajů v jednotlivých státech (UOOU, 2018).

Důvodem vzniku byla zejména snaha o harmonizaci a sjednocení pravidel napříč celým evropským prostorem. S rozvojem sociálních sítí a internetu a stále větší globalizací byla potřebná přísnější ochrana osobních údajů. Právní předpis ve formě nařízení EU má zajistit a sjednotit tuto ochranu pro všechny státy a zároveň bojovat proti jejímu narušení (Žůrek, 2017).

GDPR tak zavádí celou řadu nových povinností, definuje základní pravidla a pojmy a posilňuje práva dotčených osob, o nichž jsou údaje zpracovávány. GDPR také výrazně zvyšuje sankce za porušení nařízení a za nesprávné zpracovávání údajů. Nejvyšší sazba může činit až 20 milionů euro nebo 4 % z celosvětového ročního obratu organizace. Protiprávní zpracování a zneužití dat může být posouzeno také jako trestný čin. Nicméně pokud i tak dojde k protiprávnímu zneužití dat, právě řádně nastavený systém pravidelného testování a posuzování účinnosti jednotlivých opatření pro zajištění bezpečnosti údajů může organizaci ochránit.

3.2.1 Zásadní témata GDPR

Hlavní a zásadní cíl Obecného nařízení o ochraně osobních údajů je ochrana soukromí a dat všech obyvatel evropského prostoru. Ty nejzásadnější oblasti ochrany stále odpovídají původní směrnici z roku 1995, avšak díky rychlému rozvoji technologií je potřeba tuto směrnici aktualizovat. Mezi klíčové prvky můžeme zahrnout:

- Osobní údaje – jsou definovány jako veškeré informace, které umožňují přímo či nepřímo identifikovat konkrétní fyzickou osobu. Není však podmínkou, že identifikaci musí provést správce (držitel) údajů. Pokud kdokoliv jiný dokáže určit spojitost mezi daty, jsou pak rovněž považována za osobní. (Směrnice ES 95/46 ES, 1995). GDPR se však nevztahuje na osobní údaje právnických osob.
- Zpracování osobních údajů – chápeme jako jakoukoliv operaci s osobními údaji. Může se jednat o uložení, nahlížení, použití, šíření, výmaz a další.
- Subjekt údajů – subjekt, o kterém jsou údaje zpracovávány, má právo být informován o způsobu a důvodu zpracování.
- Zodpovědnost – za správnost a korektnost ručí vždy správce osobních údajů
- Osobní údaje mohou být zpracovány pouze v případě, že subjekt dal souhlas se zpracováním údajů, že zpracování je nezbytné za účelem plnění smluv, anebo kdy osobní údaj vyžadují zákony.

Výše uvedený seznam z roku 1995 postačil jako základ nového nařízení. V době vzniku však nebyl internet užíván v takové míře jako nyní, proto byla nutná novelizace. GDPR tak tyto definice zpřesňuje a doplňuje o podrobnější a přísnější požadavky reagující na nové technologie (Nonnemann, 2018).

3.2.2 Místní působnost

Předpis GDPR je vydaný Evropskou unií, dopadá však i na subjekty sídlící mimo EU. Je tomu tak v případě, kdy správce nebo zpracovatel osobních údajů sídlí mimo EU, ale má zřízenou pobočku v EU a ta se zpracováním souvisí.

Druhý příklad může být, kdy správce nebo zpracovatel sídlící mimo EU poskytuje služby nebo produkty obyvatelům EU a monitoruje tak jejich chování nebo činnost. Příkladem mohou být internetové služby, kdy zřizovatel má několik mutací stránek do jazyka států EU, kde služby poskytuje. Je tak nucen respektovat i pravidla zpracování osobních údajů daná GDPR.

3.2.3 Základní pojmy

Následující kapitoly definují základní a nejdůležitější pojmy v GDPR. S jejich znalostmi bude daná problematika snáze pochopitelná.

3.2.3.1 Osobní údaje (dále také jen „OÚ“)

Osobní údaje jsou specifické v tom, že dokáží snížit nebo dokonce znemožnit záměnu fyzické osoby s jinou. U některých osobních údajů nemusí být patrné, že označují konkrétní fyzickou osobu, ale ve spojení s dalšími údaji mohou vést k určení této osoby. Definice podle článku 4 odst. 1 Obecného nařízení říká, že se jedná o veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (GDPR, 2016).

Za pojem osobní údaj tak můžeme označit identifikační údaje (jméno, příjmení, datum narození, adresa, …), údaje kontaktní (email, telefon, korespondenční adresa), identifikátory, bankovní údaje, informace o dosavadním průběhu pracovněprávního vztahu, o kvalifikaci, o dosaženém vzdělání, o jeho platu, o pracovní morálce nebo jeho psychickém stavu. Jedná se i o biometrické údaje či údaje z kamerových záznamů. I když

organizace není schopna sama fyzickou osobu rozpoznat, po předání policii to již možné je, proto se jedná o osobní údaj. Osobní údaj je tak vše, co si dokáži spojit a přiřadit k jednotlivé fyzické osobě.

3.2.3.2 Subjekt osobních údajů

Subjekt údajů je fyzická osoba, které se dané osobní údaje týkají. Subjektem údajů nemůže být právnická osoba. Údaje o právnických osobách a údaje týkající se pouze právnických osob nejsou osobními údaji (UOOU, 2018).

3.2.3.3 Zvláštní kategorie osobních údajů

Zvláštní kategorie osobních údajů zahrnuje informace, které fyzické osobě zasahuje více do soukromí. Mohou to být údaje o zdravotním stavu, údaje o náboženství, politické příslušnosti, sexuální orientace a další. Zvláštními údaji jsou také údaje biometrické, např. otisk prstů nebo obraz oční rohovky (Zákon č. 110/2019 Sb., o zpracování osobních údajů).

3.2.3.4 Správce osobních údajů

Správce osobních údajů je dle Obecného nařízení o ochraně osobních údajů subjekt, jak fyzická nebo právnická osoba, tak orgán veřejné moci, který stanovuje účely a prostředky zpracování osobních údajů a za tyto údaje odpovídá (UOOU, 2018).

Správcem údajů je ale i organizace, které je zpracování údajů uloženo zvláštním zákonem. Každý zaměstnavatel je i správcem osobních údajů svých zaměstnanců stanovenými pracovněprávními předpisy nebo třeba nemocniční zařízení jsou správcem údajů ve zdravotnické dokumentaci a podobně.

3.2.3.5 Zpracovatel osobních údajů

Zpracovatel je subjekt, který nějakým způsobem zpracovává osobní údaje pro správce. Správce zpracovatele pověřuje a ten může vykonávat pouze takové úkony, ke kterým je pověřen. Zpracovatel je vždy externí subjekt, např. školící tutor nebo externí právník. Zaměstnanci správce tudíž nejsou zpracovateli (UOOU, 2018).

3.2.3.6 Zpracování osobních údajů

Zpracováním osobních údajů je každá činnost, operace nebo soustava operací, kterou provádí správce systematicky, s jasně daným účelem. GDPR uvádí typické operace, které spadají pod pojem zpracování. Jedná se o shromáždění, zaznamenávání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledávání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jiné zpřístupnění, seřazení, omezení, výmaz nebo zničení. Za zpracování lze považovat jak celý obvyklý cyklus práce s daty, tak i každou dílčí operaci nebo omezený sled operací.

O zpracování dle GDPR se jedná vždy, pokud je zpracování prováděno automatizovanými prostředky (nástroje informační a komunikační technologie). Pokud se jedná o ryze manuální práci s osobními údaji, tak se správce nebo zpracovatel musí řídit pravidly GDPR pouze tehdy, pokud bude výsledkem této činnosti evidence údajů, strukturalizovaný soubor údajů, ve kterém lze dotyčná subjekt dohledat podle nějaké informace (osobního údaje). Pod GDPR tak nespadá nahodilé shromažďování osobních údajů bez dalšího zpracování ani zařazení do manuálně vedené evidence. Příkladem je například zaslaný dokument obsahující osobní údaje nebo složka s vizitkami (Nonnemann, 2018).

3.2.3.7 Účel zpracování

Účel zpracování je smysl nebo cíl dané činnosti. Je nedílnou součástí jakéhokoliv zpracování. Účelem může být uzavírání a plnění smluv, profilování klientů, zasílání marketingových zpráv, příprava nových postupů, ochrana majetku či práv správce. Od účelu je pak omezena další řada činností a povinností, jako je stanovení rozsahu

zpracovávaných dat, doba uchování nebo skartační doba. Uvádí také, zda je možné data využit pro jiné účely. Správnou formulací účelu lze usnadnit další zpracování údajů i plnění povinností podle GDPR. Účel nemůže být vyjádřen příliš obecně, naopak nemusí být ani zcela detailní pro každou operaci zpracování (Nonnemann, 2018).

3.2.3.8 Pověřenec pro ochranu osobních údajů

Pro dodržení souladu s GDPR podle článku 37 je nutnost pro organizaci jmenovat tzv. pověřence pro ochranu osobních údajů neboli „DPO“ (Data Protection Officer) v případech kdy:

- Zpracování provádí orgán veřejné moci či veřejný subjekt (neplatí pro soudy)
- Hlavní činnost zpracovatele vyžaduje rozsáhlé pravidelné a systematické monitorování občanů
- Hlavní činnost zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se rozsudků v trestních věcech nebo trestných činech.

Hlavním úkolem pověřence je monitorování souladu zpracování osobních údajů s povinnostmi vyplývajících z Obecného nařízení o ochraně osobních údajů.

Podle GDPR může být jediný pověřenec jmenován i pro více státních institucí, orgánů či firem, které mají podobnou strukturu. Pověřenci nenesou osobní odpovědnost za špatné dodržování GDPR. Veškerá odpovědnost je vždy na správci. Pověřenec monitoruje soulad s GDPR za organizaci, poskytuje informace a poradenství správcům, zpracovatelům a zaměstnancům, kteří provádějí nějaký typ zpracování, podílí se na posouzení vlivu na ochranu osobních údajů a také spolupracuje s dozorovým úřadem. (GDPR, 2016)

3.2.4 Základní zásady zpracování osobních údajů

GDPR kromě definic základních pojmů upravuje i zásady, které musí zpracovatel či správce u svého zpracování respektovat. DPO neboli Pověřenec pro ochranu osobních údajů se v těchto pravidlech musí orientovat, aby mohl dostatečně radit a posuzovat soulad zpracování s GDPR.

Hlavními zásadami jsou:

- Zákonnost zpracování
- Transparentnost zpracování
- Účelové omezení
- Minimalizace údajů
- Přesnost údajů
- Omezení doby zpracování
- Bezpečnost a integrita dat
- Doložitelná odpovědnost v souladu s GDPR (Nonnemann, 2018).

3.2.4.1 Zákonnost zpracování

Každé zpracování musí disponovat dostatečným právním titulem, aby mohlo být zpracováváno. Tyto právní důvody jsou obsaženy v čl. 6 GDPR, pro citlivé osobní údaje je výčet právních důvodů uveden v čl. 9 a 10 GDPR. Správci stačí disponovat jedním právním důvodem, aby byla dodržená zákonnost zpracování. Pokud se správci nepodaří doložit ani jeden z právních důvodů, je toto zpracování nezákonné, a osobní údaje musí zlikvidovat. Úřad pro ochranu osobních údajů navíc může uložit sankci a dotčená osoba může požadovat odškodnění za nezákonné zpracování údajů.

Mezi tyto zákonné zpracování patří dle zákona č. 110/2019 Sb., o zpracování osobních údajů:

- Souhlas subjektu údajů. Tento souhlas musí být svobodný a subjekt musí být obeznámen, za jakým účelem poskytuje své osobní údaje. Souhlas musí být udělen aktivně, tudíž ho musí sám subjekt údajů poskytnout, podepsat formulář nebo vyplnit políčko v online světě. Předem vyplněné pole nebo mlčení není uznatelné jako souhlas. Aby byl souhlas udělen, musí být také vědomý. Subjekt údajů má právo svůj souhlas kdykoliv odvolat a správce je tak povinen zpracování osobních údajů zastavit, pokud k tomu nemá další právní důvod.

- Zpracování je nezbytné pro uzavření nebo plnění smlouvy. Pokud správce a subjekt údajů o smlouvě jednají nebo již smluvně zavázáni jsou, nemusí správce pro související zpracování osobních údajů ještě navíc získávat souhlas od dotčené osoby.

- Zpracování je nezbytné pro splnění právní povinnosti správce. Pokud správci zákon předem ukládá povinnost toto zpracování provádět, není potřeba souhlas subjektu údajů nebo jiné fyzické osoby. Typické je zpracování uložené zákoníkem práce, obecním zřízením, zdravotními složkami na základě zákona o zdravotních službách či dalšími veřejnoprávními předpisy.

- Zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů. Toto zpracování není v praxi často aplikované. Jedná se o krajní případ, kdy zájem na ochranu života nebo zdraví je důležitější než hodnota soukromí.

- Zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci. Jedná se hlavně o činnosti orgánů veřejné moci při výkonu jejich pravomocí, např. obce či kraje (Žůrek, 2017).

- Zpracování na základě oprávněného zájmu správce nebo dalšího subjektu. Pokud správce hodlá zpracovávat údaje, aby zajistil svůj zájem, například ochranu majetku nebo při vedení nějaké evidence, může to udělat bez souhlasu dotčených osob v případě, kdy zájmy a práva organizace právo osoby převažují. Správce je povinen zpracovat test přiměřenosti neboli balanční test a zvážit, jak silný je jeho zájem a jak silně by zasahovalo toto zpracování do práv subjektu údajů. Na příkladu kamerového systému je ochrana majetku správce dostatečně legitimní důvod pro zpracování, nicméně musí být přiměřený.

Správce musí být za každých okolností schopen doložit právní základ pro jednotlivé zpracování. Je proto vhodné, aby měl jednotnou evidenci/registr všech zpracování, jejich účelu a souvisejících právních důvodů.

Pokud správce zpracovává jak „běžné“ tak zvláštní osobní údaje, musí k tomu mít legitimní právní důvod. Zpracování pro citlivé údaje se podrobuje vyššímu riziku pro práva dotčených osob, což musí správce zohlednit při plnění dalších povinností a následném důkladnějším zabezpečení těchto údajů před případným únikem.

3.2.4.2 Zásada transparentnosti

Zpracování osobních údajů musí být transparentní a otevřené. Subjekt osobních údajů má právo vědět kdy jsou jeho osobní údaje zpracovávány, za jakým účelem a za jakých podmínek.

V případě shromažďování údajů přímo od subjektu je povinen správce poskytnout tyto informace:

- Identifikační údaje a kontakt na správce, pokud byl jmenován pověřenec pro ochranu osobních údajů, pak kontakt na něj
- Účel a právní důvod zpracování

- Pokud je uveden právní důvod „oprávněný zájem“, je nutné vymezit tento zájem
- Pokud se správce chystá poskytnout data pro třetí stranu, je nutné ji uvést a sdělit
- Pokud se správce chystá předat údaje mimo Evropskou unii, například své mateřské společnosti, musí poskytnout informace o tomto záměru

Pokud se jedná o zpracování zvláštních údajů, musí správce informovat také o:

- Době, po kterou budou osobní údaje zpracovávány nebo uchovávány. Může se jednat o konkrétní dobu (pět, deset a více let) nebo informaci, jak dobu určit (po dobu trvání smlouvy a jiné).
- Uvedení práv subjektu údajů, tzn. že subjekt má právo svůj souhlas odvolat, právo požadovat přístup ke svým údajům, jejich opravu, výmaz, omezení jejich zpracování, práva na přenositelnost dat nebo právo na námitku nebo podání stížnosti k Úřadu pro ochranu osobních údajů.
- Skutečnosti, zda je toto zpracování nezbytné pro plnění právní povinnosti správce nebo pro uzavření smlouvy mezi správcem a subjektem údajů

Případné další informace je nutno vždy posoudit podle konkrétního zpracování. Cílem GDPR je, aby měl subjekt údajů jasný a kompletní přehled o tom, jaká data jsou o něm uchovávány. Z tohoto důvodu je nutné rozsah poskytovaných informací vždy posoudit s přihlédnutím k dalším náležitostem, jako je jeho účel, zásah do soukromí subjektu, rizikovost a podobně.

3.2.4.3 Účelové omezení

Zásada účelového omezení vyjadřuje, že správce je povinen shromažďovat osobní údaje za jedním, předem daným účelem a nesmí je tak dále zpracovávat pro jiné účely, které jsou s původním záměrem neslučitelné. Je tedy vhodné výslovně popsat a definovat všechny účely zpracování v dané organizaci.

3.2.4.4 Minimalizace údajů

Správce je povinen a schopen odůvodnit, proč a pro jaký účel zpracování potřebuje právě shromažďované osobní údaje. Pokud to věrohodně nedoloží, pak nesplňuje soulad s GDPR.

3.2.4.5 Přesnost údajů

Povinnost správce je vhodně zajistit, aby byly zpracovávány pouze přesné a aktuální osobní údaje. Pokud se jakýmkoliv způsobem dozví, že údaje byly pozměněny nebo nejsou aktuální, je povinen je opravit nebo vymazat. Není však důvod k tomu, aby byl správce povinen aktivně kontrolovat a hodnotit údaje například tím, že by je porovnával z veřejnými rejstříky osob. Tento způsob není považován za dostatečně přiměřený.

3.2.4.6 Omezení doby uložení údajů

Pravidlo říká, že osobní údaje je vhodné uchovávat jen po omezenou a nezbytnou dobu. Po uplynutí této doby je správce povinen údaje vymazat nebo nevratně anonymizovat, a to ve všech systémech a úložištích, na kterých byly údaje uloženy. Jak v papírové, tak v elektronické podobě. Nezbytná doba pro uchování je pak odvíjena od zvláštních předpisů nebo ji správce musí stanovit a odůvodnit sám. Ten je povinen nastavit proces stanovení doby uchování a následné likvidace tak, aby byl schopen jednoduše

kontrolovat, zda systém funguje. Druhotná kontrola by měla proběhnout od Pověřence pro ochranu osobních údajů danou organizací.

3.2.4.7 Bezpečnost údajů

Bezpečnost údajů je stěžejní pro oblast GDPR, nicméně nařízení nedefinuje konkrétní pravidla a postupy, jak mají správci zabezpečit a chránit údaje subjektů. Každá organizace pak musí sama a zajistit bezpečnosti zpracovávaných údajů a zvážit míru rizika včetně vyhodnocení, co by případný incident znamenal pro subjekt údajů.

GDPR však obsahuje výčet bezpečnostních opatření, které správce či zpracovatel může s ohledem na přiměřené úsilí aplikovat. Jedná se například o:

- Pseudonymizaci a šifrování dat
- Schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systému a služeb souvisejících se zpracováním
- Schopnost obnovit dostupnost osobních údajů a přístup k nim v případě incidentů
- Systém pravidelného testování a posuzování účinnosti jednotlivých opatření pro zajištění bezpečnosti údajů (GDPR, 2016).

3.2.4.8 Odpovědnost správce

Nové pravidlo, které přichází s nařízením GDPR je tzv. odpovědnost správce. Nejenom, že jsou správci povinni jednat v souladu s GDPR a dalšími předpisy, ale také svůj postup průběžně a důkladně dokumentovat, zaznamenávat a hodnotit. Nestačí však pouze schopnost doložit, že jeho zpracování je v souladu s GDPR nyní, ale musí být schopen prokázat, že se tak dělo již od počátku a bylo postupováno v souladu se zákonem. Procesy by měly být monitorovány a kontrolní mechanismy zpracovávány spolu s údaji.

3.2.5 Práva subjektu údajů

GDPR upravuje a určuje řadu práv osob, jejichž osobní údaje jsou správcem zpracovávány. To má posílit kontrolu dotyčné osoby nad zpracováním jako takovým a zvýšit tak jeho transparentnost. Jedná se o tyto práva podle čl. 14 - 22:

- Právo na informace (čl.14 GDPR)
- Právo subjektu na přístup k osobním údajům (čl.15 GDPR)
- Právo na opravu (čl.16 GDPR)
- Právo na výmaz („právo být zapomenut“) (čl.17 GDPR)
- Právo na omezení zpracování (čl.18 GDPR)
- Právo na přenositelnost údajů (čl.20 GDPR)
- Právo vznést námitku (čl.21 GDPR)
- Právo na přezkum automatizovaného rozhodnutí (čl.22 GDPR)

Správce by na prvním místě měl výkon práv subjektu údajů usnadňovat. Neměl by klást nesmyslné administrativní či technické překážky, klást bezdůvodné podmínky nebo omezovat výkon pouze na některé osoby. Správce je povinen zajistit podmínky, aby mohlo být žádosti vyhověno i elektronickou formou. Naopak však musí zajistit a přijmout dostatečná opatření k tomu, aby jednoznačně identifikoval subjekt údajů, a aby nedošlo k chybné úpravě či výmazu jiného subjektu údajů.

Správce je také povinen subjekt údajů informovat o tom, jak je s údaji nakládáno a podnět vyřídit, a to obvykle ve lhůtě 30 kalendářních dnů. Tyto úkony se provádějí zásadně bezplatně a správce nesmí požadovat ani úhradu vynaložených nákladů (čas, materiální práci s údaji atd.). Výjimkou je situace, kdy je žádost zjevně nedůvodná, nepřiměřená, šikanózní nebo se bezdůvodně opakuje. V takových případech může správce vymáhat na dotyčném náhradu skutečných nákladů spojených s vyřízením podnětu.

3.2.5.1 Právo na informace

Pokud se jednoznačně identifikovaný subjekt údajů obrátí na správce s dotazem, zda jakýmkoliv způsobem zpracovává jeho osobní údaje, je správce povinen mu oznámit, zda ano či nikoliv. Pokud ano, je také povinen doplnit další informace se zpracováním spojené, a to následující:

- Účel zpracování osobních údajů
- Kategorii údajů (identifikační, kontaktní a jiné údaje)
- Kdo jsou dalšími příjemci údajů, zda jsou předávány nebo zveřejňovány
- Doba, po kterou jsou údaje zpracovávány
- Informace o zdroji osobních údajů
- Skutečnost, jestli jsou údaje zpracovávány automatizovaně, bez zásahu lidského zaměstnance či nikoliv
- Zda jsou osobní údaje předávány do třetí země

3.2.5.2 Právo na přístup k osobním údajům

Jestliže si subjekt údajů zažádá, má právo na zpřístupnění svých údajů či jejich kopie, které o něm správce údajů zpracovává. Správce je povinen uvést všechny dostupné osobní údaje, které má o žadateli k dispozici.

Ani právo na přístup však není neomezené. GDPR uvádí, že výkonem tohoto práva nesmí být dotčena práva a svobody jiných osob. (čl. 15 odst. 4 GDPR). Poskytovaná informace také musí být dostatečná k tomu, aby subjekt pochopil, jaké jeho údaje a proč jsou zpracovávány, nicméně správce není povinen poskytnout informace týkající se jeho výrobního nebo obchodního tajemství.

3.2.5.3 Právo na opravu

Právo na opravu vychází a koresponduje se zásadou přesnosti informací. Nevyplývá z něj povinnost pro správce procházet zpracovávané údaje a hledat chyby, je však povinen, po upozornění subjektem údajů na nesprávnost či neaktuálnost některého z údajů, danou informaci opravit. Nicméně ani toto právo nezakládá stoprocentní povinnost správce tento údaj dodatečně měnit. Například ve zprávě od lékaře, by pak správce nemohl zpětně poskytnout pravdivé informace o stavu pacienta.

3.2.5.4 Právo na výmaz („právo být zapomenut“)

V tomto případě se o zcela nové pravidlo nejedná. V GDPR jsou pouze na jednom místě upraveny situace, ve kterých byl správce povinen vymazat osobní údaje i podle směrnice 95/46, resp. podle zákona o ochraně osobních údajů.

Správce je povinen údaje o subjektu vymazat, pokud:

- Osobní údaje již nejsou potřeba k účelu, pro které byly shromažďovány
- Subjekt údajů odvolal svůj souhlas o poskytnutí osobních údajů a správce nemá žádný jiný právní důvod pro další zpracování
- Subjekt může vznést námitku proti zpracování na základě oprávněného zájmu. Správce je povinen přezkoumat tuto žádost a pokud dospěje k tomu, že práva dotčeného subjektu převažují nad oprávněným zájmem správce, je povinen tyto údaje vymazat
- Pokud jsou údaje zpracovávány pouze pro účely cíleného marketingu a subjekt vznese námitku
- Pokud byly údaje zpracovávány protiprávně nebo pokud mu povinnost vymazat údaje ukládá přímo zvláštní zákon

3.2.5.5 Právo na omezení zpracování

Subjekt údajů má právo, aby omezil rozsah zpracování svých osobních údajů správcem dle článku 18 GDPR. Toto právo je na rozdíl od likvidace jen dočasné (Žůrek, 2017).

3.2.5.6 Právo na přenositelnost údajů

Právo zcela nové, které GDPR přináší. Subjekt údajů může u správce požadovat poskytnutí svých automatizovaně zpracovaných údajů a také jejich následné předání dalšímu správci na vyžádání. (čl. 20 GDPR).

Rozdílem mezi právem na přístup a právem na přenositelnost je stanovení formátu, ve kterém musí být osobní údaje poskytnuty, a možnost předání údajů jinému správci (Žůrek, 2017).

3.2.5.7 Právo vznést námitku

Pokud správce zpracovává údaje na základě právního důvodu oprávněného zájmu nebo na základě veřejného zájmu, může subjekt údajů vznést námitku proti takovému zpracování spočívající v jeho konkrétní situaci. Subjekt tak nezpochybňuje existenci právního důvodu, ale v jeho situaci by zpracování nemělo být prováděno. Správce je povinen námitku posoudit a zpracovat tzv. Balanční test, kterým je poměřena váha oprávněného zájmu, práv dotčených osob a přiměřenost zásahu do jejich práv.

3.2.5.8 Právo na přezkum automatizovaného rozhodnutí

Pokud se provádí zpracování automatizovanými prostředky, která má pro subjekt údajů právní nebo obdobně významné důsledky, může subjekt správce požádat o přezkum

tohoto rozhodnutí. Smyslem tohoto práva je umožnit, aby člověk vyjádřil názor tehdy, pokud o právech rozhoduje automatizovaný počítač a aby se lidský zaměstnanec tímto podnětem zabýval. Může se jednat například o uzavření smlouvy o úvěru nebo pojistné smlouvy.

3.3 Analýza rizik

GDPR v článku 32 o Zabezpečení zpracování oznamuje, že s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelu zpracování má správce provést vhodná technická nebo organizační opatření. Neříká ale, jak správně přistupovat k závažnosti rizika, jak zajistit úroveň zabezpečení, jak určit kritičnost zpracování nebo jaké konkrétní technické nebo organizační opatření zajistit. Proto se často v GDPR vychází z normy ČSN ISO/IEC 27000 a ze zákona o kybernetické bezpečnosti 181/2014 Sb., kde jsou tyto součástí analýzy rizik rozebrány podrobněji.

3.3.1 ČSN ISO/IEC 27000

ČSN ISO/IEC 27000 je rodina mezinárodních standardů zaměřená na řízení informační bezpečnosti v organizacích. Jednotlivé normy pomáhají k zajištění souladu s aktuálními legislativními požadavky pro ochranu osobních údajů mezi jejichž základní principy patří:

- Informace musíme chránit → důvěrnost
- Informace musíme sdílet → dostupnost
- Informace musíme mít aktuální → integrita

Porušení je z pohledu normy rovnocenné. Zajištění důvěrnosti, dostupnosti a integrity informací organizace má zásadní význam pro udržení konkurenceschopnosti, ziskovosti, právní shody a dobrého jména organizace.

Obecné nařízení o ochraně osobních údajů (GDPR) se právě o standardy ISO 27000 opírá ve zmiňovaných 3 základních principech.

3.3.2 Zákon o kybernetické bezpečnosti

Zákon ze dne 23. července 2014 číslo 181/2014 Sb., upravuje práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon zpracovává příslušné předpisy Evropské unie a upravuje zajišťování bezpečnosti sítí, elektronické komunikace a informačních systémů.

V Hlavě I a II tohoto zákona je popsán systém zajištění kybernetické bezpečnosti, zajištění bezpečnosti informací, řízení rizik, dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. Uvádí bezpečnostní opatření, a to konkrétně organizační a technické, které budou součástí následující analýzy rizik.

Tento zákon upravuje Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), která vstoupila v platnost dne 28.5.2018.

3.3.3 Metodika analýzy rizik

3.3.3.1 Účel a cíl řízení rizik

Hlavním účelem řízení rizik zpracování osobních údajů je:

- Zajistit schopnost správce osobní údajů doložit, že zpracování osobních údajů je prováděno v souladu s Obecným nařízením o ochraně osobních údajů tj., že jsou zavedena vhodná technická a organizační opatření s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob

- Identifikovat dopady na soukromí, rizika a povinnosti v oblasti ochrany soukromí
- Poskytování informací o návrhu na ochranu soukromí
- Přezkoumání rizik v oblasti ochrany soukromí u nových projektů (např. Povinnost hodnotit projekty nového nebo změněného informačního systému z pohledu ochrany osobních údajů a případně provádět analýzu rizik) a posouzení jeho dopadu a pravděpodobnosti
- Poskytnutí základních informací a postupů zaměstnancům v oblasti ochrany osobních údajů a postupech zaměřených na akce vedoucí ke zmírnění rizika na zpracování osobních údajů
- Udržování aktualizací nebo upgradů s dodatečnými funkcemi, které by mohly mít vliv na nakládání s osobními údaji
- Sdílení a snížení rizik spojených s osobními údaji se zainteresovanými stranami nebo poskytnutí důkazů týkajících se souladu.

3.3.3.2 Riziko osobního údaje

Je to riziko pro základní práva a svobody občanů dané země. Při identifikaci rizik je třeba brát zřetel na nutnost zdokumentovat působení těchto rizik.

Scénář rizika může vypadat následovně:

1. Zdroj rizika (např. zaměstnanec)
2. Zranitelnost (např. nezabezpečený počítač)
3. Hrozba (např. Zneužití emailové schránky)
4. Výskyt nežádoucích událostí (např. zasílání spamu)
5. Specifikace příjemce
6. Analýza dopadu na soukromí subjektu údajů

3.3.3.3 Stanovení kontextu a rozsahu

Cílem stanovení kontextu a rozsahu je získat přesný přehled o procesech zpracovávaných osobních údajů.

Rozsah řízení rizik osobních údajů určuje specifické podrobnosti o následujícím:

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

Analýza rizik by měla být přizpůsobena velikosti organizace (nebo její části), informačnímu systému nebo procesu, který je předmětem řízení rizik.

3.3.3.3.1 Kritéria řízení rizik

Kritéria řízení rizik zpracování osobních údajů zohledňují následující:

Tabulka 1 - Kritéria řízení rizik

Kritérium	Poznámka
Strategické hodnoty procesů organizace	Podle stupnice rizikových kategorií
Kritičnost zpracování osobního údaje	Podle stupnice rizikových kategorií
Legislativní a regulatorní požadavky, smluvní závazky	Mandatorní
Důležitost dostupnosti, důvěrnosti a integrity informací osobního údaje	Podle stupnice rizikových kategorií
Požadavky zainteresovaných stran, negativní dopady ztráty důvěryhodnosti a dobré pověsti	Podle stupnice rizikových kategorií

Zdroj: vlastní zpracování

3.3.3.4 Identifikace hrozeb a zranitelností

Pro správnou identifikaci hrozeb a zranitelností podpůrných aktiv je uveden a používán Katalog hrozeb a zranitelností (Příloha 1), který je formulován v normě ISO/IEC 29134.

3.4 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů je často označováno jako DPIA (Data Protection Impact Assessment). Obecné nařízení o ochraně osobních údajů ukládá správci povinnost zavést odpovídající opatření, aby zajistil a byl schopen doložit soulad s GDPR. Přihlíží přitom mimo jiné k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob (článek 24, odst. 1). Povinnost správců provést posouzení vlivu na ochranu osobních údajů je třeba vnímat jako jejich povinnost vhodným způsobem řídit rizika spojená se zpracováním osobních údajů (UOOU, 2020).

Je-li pravděpodobné, že určitý druh připravovaného zpracování osobních údajů povede vzhledem k jeho povaze, rozsahu, okolnostem nebo účelu k vysokému riziku neoprávněného zásahu do práv a svobod subjektů údajů, vypracuje správce/zpracovatel posouzení vlivu takového zpracování na ochranu osobních údajů, které obsahuje alespoň:

- Obecný popis připravovaného zpracování osobních údajů a jeho operací
- Posouzení rizika neoprávněného zásahu do práv a svobod subjektů údajů
- Plánovaná opatření a vhodné záruky ke zmenšení rizika podle předchozího bodu a splnění povinností (Zákon č. 110/2019 Sb., o zpracování osobních údajů)

Rizikem se rozumí scénář, v němž je uveden popis určité události a jejích důsledků společně s odhadem její závažnosti a pravděpodobnosti. „Řízení rizik“ je naproti tomu možné definovat jako soubor koordinovaných činností určených k řízení a omezení rizika v organizaci (UOOU, 2020).

Vzhledem k faktu, že existuje několik dokumentů, které upravují nebo přímo popisují postupy řízení rizik pro správce, kteří mohou zpracovávat osobní údaje s vysokými riziky pro práva a svobody subjektu údajů, je metodika posouzení vlivu připravena s ohledem na:

- Zajištění souladu s obecným nařízení o ochraně osobních údajů

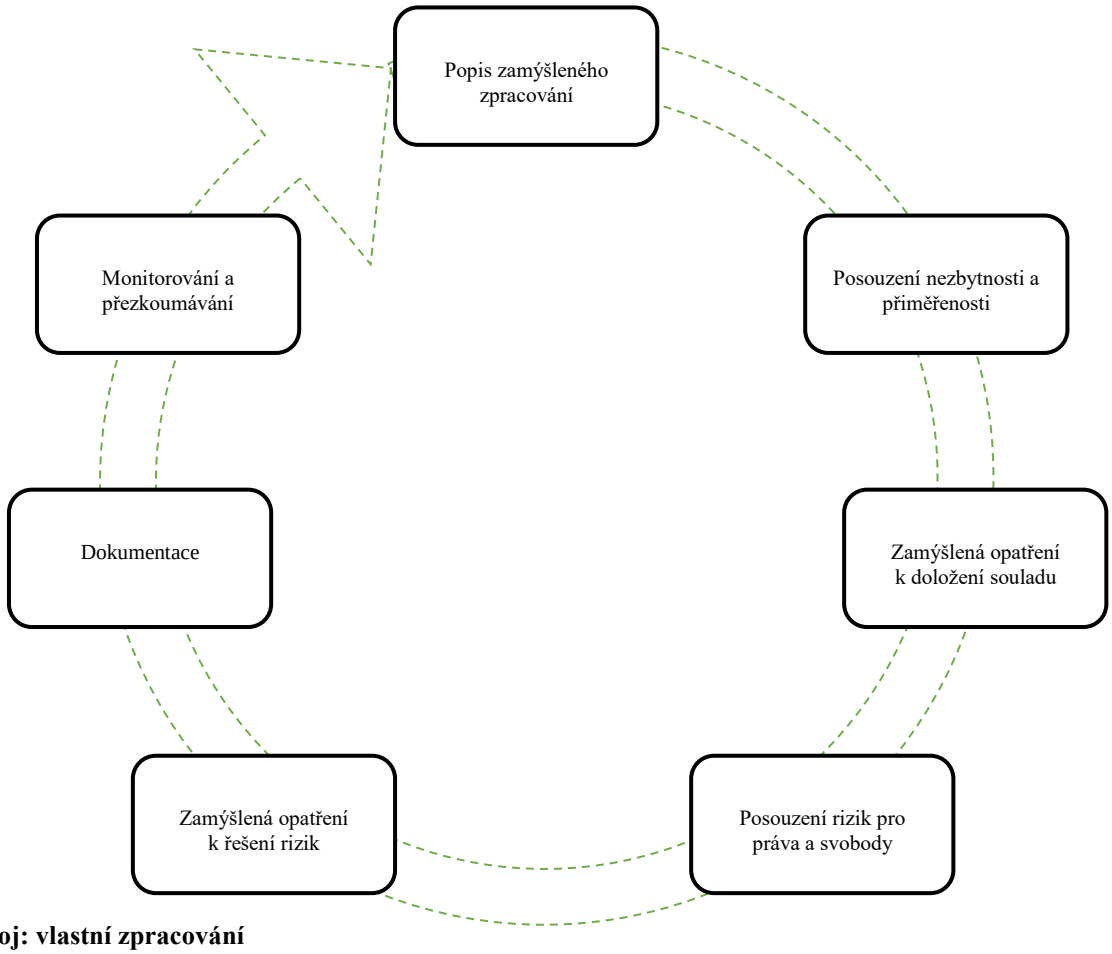
- Snížení administrativního zatížení správců, kteří mohou využít některé z metodik a postupů, které jsou povinni doložit ke splnění povinností
- Další odborné podklady, které jsou k problematice k dispozici (UOOU, 2019)

Záznam o DPIA má minimální požadavky, které musí obsahovat a to:

- Popis zamýšlených operací zpracování a účely zpracování
- Posouzení nezbytnosti a přiměřenosti operací zpracování
- Posouzení rizik pro práva a svobody subjektů údajů
- Plánovaná opatření:
    - K řešení těchto rizik
    - K doložení souladu s nařízením (GDPR, 2016).

Následující obrázek znázorňuje obecný opakující se proces provádění posouzení vlivu na ochranu osobních údajů.

Obrázek 1 - proces provádění DPIA



Zdroj: vlastní zpracování

Posouzení vlivu na ochranu osobních údajů je v našem případě taková analýza rizik, která se dotýká pouze zpracování považovaného za rizikové a na které se nevztahuje výjimka vydaná Úřadem pro ochranu osobních údajů.

3.4.1 Seznam druhů operací nepodléhající požadavku na DPIA

Úřad pro ochranu osobních údajů, po zkušenosti z dosavadní praxe a se snahou k minimalizaci administrativních požadavků, zveřejnil seznam druhů zpracování, u nichž není potřeba provádět posouzení vlivu.

Tento seznam operací navazuje na obecné nařízení o ochraně osobních údajů a Pokyny pro posouzení vlivu na ochranu údajů. Stanovuje, zda je pravděpodobné, že toto zpracování bude mít za následek vysoké riziko související s účely nařízení č. 2016/679 zpracovaných v dokumentu WP248 pracovní skupinou WP29. Tato pracovní skupina slouží jako nezávislý poradní orgán pro ochranu dat a soukromí a je složena z vedoucích zástupců dozorových úřadů členských zemí Evropské unie (Škorničková, 2020). Seznam není definitivní a jeho výčet podléhá změnám vyvolaným praktickými poznatky a rozvojem technologií.

Z tohoto důvodu byl seznam dne 10. července 2019 podroben kontrole, upraven a schválen Evropským sborem pro ochranu osobních údajů. Současná verze obsahuje:

- Zpracování osobních údajů zaměstnanců s trvalým pracovištěm na území České republiky, prováděné pouze na území České republiky, a to v rámci plnění zákonných povinností při vedení účetnictví, mzdové agendy, sociálního a zdravotního pojištění.
- Zpracování personální agendy zaměstnanců s trvalým pracovištěm na území České republiky, prováděné pouze na území České republiky, pokud neobsahuje zpracování biometrických údajů, hodnocení a bodování subjektů údajů nebo systematické monitorování subjektů údajů. Mezi zpracování personální agendy se nezahrnuje whistleblowing (na základě zákona daná země určí, jaká míra ochrany náleží oznamovateli po dobu kauzy).
- Zpracování osobních údajů zákazníků prováděné v celém rozsahu na území České republiky, týkající se obchodní činnosti (prodeje a poskytování služeb, včetně pořádání soutěží a zasílání newsletterů), prováděné pouze v českém jazyce, pokud neobsahuje zpracování zvláštních kategorií osobních údajů, hodnocení, bodování nebo systematické monitorování subjektů údajů (s výjimkou dle bodu 4 seznamu).
- Zpracování spojené s jednotlivou návštěvou zákazníka na webové stránce správce, a to včetně profilování zákazníka, založeného na jeho výběru položek či zobrazování položek z nabídky zboží, výrobků a služeb umístěných na webové

stránce správce. V rámci tohoto zpracování nedochází ke zpracování zvláštních kategorií osobních údajů, údajů vysoce osobní povahy (viz bod 4 na straně 11 Pokynu WP248) a nedochází k zaměření zpracování osobních údajů na ohrožené subjekty údajů jako samostatnou cílovou skupinu.

- Zpracování zajišťované osobou oprávněnou k poskytování zdravotních služeb, která není v zaměstnaneckém poměru. Tato osoba využívá nezbytné osobní údaje pouze k poskytování zdravotních služeb pro subjekt údajů (viz recitál 91 nařízení), přičemž nedochází k systematickému předávání do třetích zemí, pro některé operace zpracování osobních údajů o pacientech není využíván zpracovatel, nebo nedochází ke sdílení/propojení osobních údajů pacientů dvou nebo více jednotlivých lékařů.
- Zpracování zajišťované jednotlivými advokáty a notáři (advokáti a notáři, kteří nejsou v zaměstnaneckém poměru), využívající nezbytné osobní údaje pouze k zajištění právních služeb pro subjekt údajů (viz recitál 91 nařízení), přičemž nedochází k systematickému předávání do třetích zemí, pro některé operace zpracování osobních údajů o klientech není využíván zpracovatel, nebo nedochází ke sdílení/propojení osobních údajů klientů dvou nebo více jednotlivých právníků.
- Zpracování zajišťované jednotlivými podnikajícími fyzickými osobami poskytujícími sociální služby (osoby, které nejsou v zaměstnaneckém poměru) využívající nezbytné osobní údaje pouze k zajištění sociálních služeb pro subjekt údajů, přičemž nedochází k systematickému předávání do třetích zemí, pro některé operace zpracování osobních údajů o klientech není využíván zpracovatel, nebo nedochází ke sdílení/propojení osobních údajů klientů dvou nebo více jednotlivých poskytovatelů sociálních služeb. (UOOU, 2020).

3.5 Zabezpečení zpracování osobních údajů

Správce přijme taková organizační a technická opatření, aby zajistil úroveň zabezpečení osobních údajů odpovídající povaze, rozsahu, okolnostem, účelu a riziku jejich zpracování.

Jsou-li osobní údaje zpracovávány automatizovaně, spravující orgán přijme nezbytná opatření, aby:

- tyto osobní údaje zabezpečil před neoprávněným přístupem, přenosem, změnou, zničením, ztrátou, odcizením, zneužitím nebo jiným neoprávněným zpracováním,
- zajistil obnovitelnost těchto osobních údajů,
- zajistil možnost určit a ověřit osobu, která tyto osobní údaje vložila nebo které byly prostřednictvím zařízení pro přenos údajů předány nebo zpřístupněny,
- zajistil bezpečnost a spolehlivost informačního systému, který tyto osobní údaje obsahuje, včetně hlášení výskytu chyb, a
- zabránil v neoprávněném přístupu k nosiči těchto osobních údajů nebo zařízení užívanému k jejich zpracování.

Povinnosti spravujícího orgánu stanovené v 1. a 2. odstavci platí pro zpracovatele obdobně (Zákon č. 110/2019 Sb., § 40).

3.6 Provedení analýzy rizik

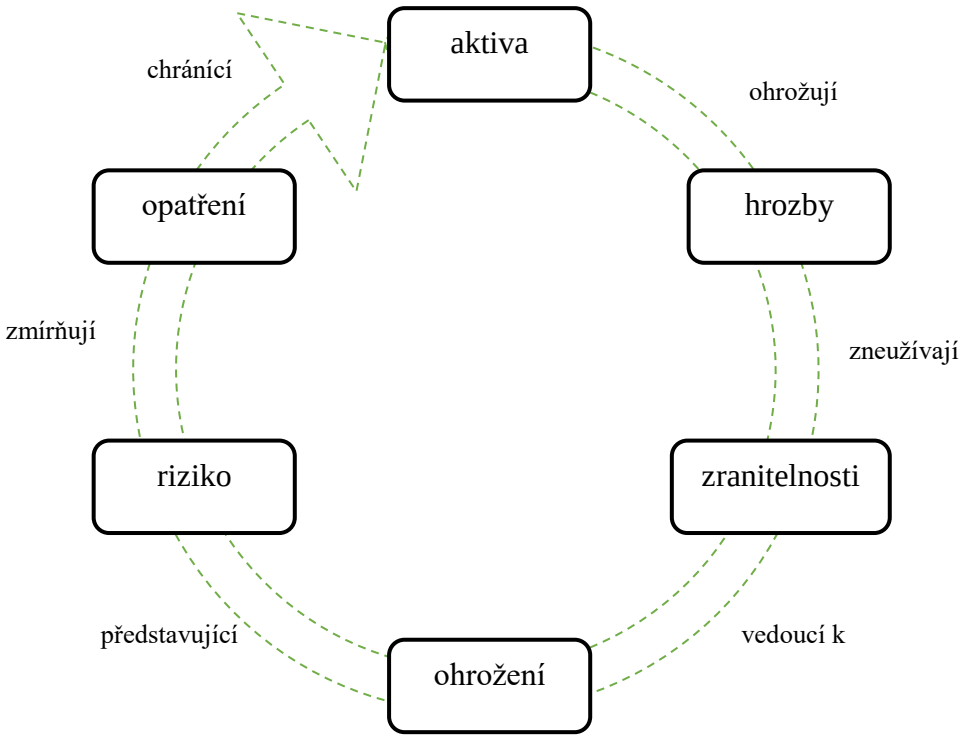
Analýza rizik přináší odpovědi na otázky, jakým hrozbám je aktivum vystaveno, jak moc je vůči nim zranitelné, jak vysoká je pravděpodobnost zneužití jeho zranitelnosti a jaký to na něj bude mít celkový dopad. Na základě zjištěných hrozeb je třeba navrhnout

vhodná opatření, která sníží jejich dopad na nejnižší možnou hranici. Jedná se o dlouhodobý a komplexní proces, který eliminuje hrozby a rizika působící na společnost a zvyšuje tak bezpečnost nejen organizace, ale i jejích zaměstnanců.

Je třeba si uvědomit, že hrozba může být zdrojem pro jedno i více rizik. Ta sama o sobě riziko nepředstavuje, nicméně využívá jeho zranitelností, které vedou k následnému ohrožení. Aplikováním vhodných opatření organizace maximálně snižuje míru výsledného rizika.

Proces posouzení rizik nejlépe ilustruje následující obrázek:

Obrázek 2 - Proces posouzení rizik



Zdroj: vlastní zpracování

Postup posouzení rizik se skládá z několika na sebe navazujících kroků:

- Nejprve jsou identifikována aktiva neboli jednotlivá zpracování osobních údajů (registr zpracování).
- V následujícím kroku je provedeno hodnocení Kritičnost zpracování, podle kritérií ÚOOU.
- Následně jsou identifikovány a ohodnoceny hrozby a zranitelnosti z pohledu jednotlivých typů aktiv dle Katalogu hrozeb ISO/IEC 29134.
- Na základě výsledných hodnot ohodnocení aktiv, hrozeb a zranitelností je zjištěna míra rizika pro jednotlivá zpracování osobních údajů.
- Pro zmírnění rizika jsou navržena vhodná opatření dle ISO/IEC 29151, která vedou ke zmírnění rizikovosti daného zpracování
- Pro zjištěná vysoce riziková zpracování je třeba provést Posouzení vlivu na ochranu osobních údajů – DPIA jež posoudí dopady konkrétního rizikového zpracování osobních údajů na soukromí a potenciální rizika takového zpracování pro práva a svobody subjektů údajů. Toto posouzení vychází z nařízení GDPR.
- Pokud se zbytkové vysoké riziko objeví i u zpracování, které je podrobeno posouzení vlivu na ochranu osobních údajů a následně je přezkoumáno pověřencem pro ochranu osobních údajů, je nutná předběžná konzultace s dozorovým úřadem.

4 Vlastní práce

4.1 Identifikace jednotlivých zpracování osobních údajů – Registr zpracování

Kancelář DPO České zemědělské univerzity v Praze poskytla Registr zpracování, který uvádí kompletní výčet zpracování jednotlivých aktiv za celou univerzitu.

Tento seznam je složen celkem ze 125 zpracování, které k datu 31.12.2019 uvádí ČZU v Praze, a u kterých shromažďuje osobní údaje nebo s nimi jakýmkoliv způsobem nakládá. U každého zpracování je uvedeno několik informací, které detailně popisují jednotlivá aktiva z pohledu ochrany osobních údajů. Jedná se o:

- Název a účel zpracování
- Garant účelu (Vlastník aktiva / Klíčový uživatel)
- Kategorie subjektů osobních údajů
- Kategorie osobních údajů
- Zdroj osobních údajů
- Právní titul
- Způsob pořízení dat
- Četnost zpracování
- Poskytnutí třetím stranám
- Způsob uložení
- Prostředek a způsob zpracování
- Doba uchování
- Námitka
- Práva subjektu

- Informační systém
- Správce aktiva (Správce systému)

Příklad jednotlivých zpracování:

Tabulka 2 - Registr zpracování 1

Název zpracování OÚ	Účel zpracování	Vztah ke zpracování (správce/zpracovatel)	Využití externího zpracovatele pro zpracování	Operace zpracování osobních údajů	Garant účelu (Vlastník aktiv/Klíčový uživatel)	Kategorie subjektů OÚ	Kategorie a typ osobních údajů (dataset)	Zvláštní kategorie osobních údajů	Zdroj a způsob pořízení OÚ (od koho, z jakého IS, kdy, jak)
registr smluv	Zveřejňování smluv a objednávek v Registru smluv	Správce	ne	Pořízení Předávání	OIKT / EO	dodavatelé / odběratelé - kontaktní fyzické osoby; zaměstnanci	Adresní a identifikační údaje název subjektu, IČ, DIČ, spisové značky z rejstříků (VR, ŽR) **Popisné údaje** název a adresa subjektu, bankovní spojení **Identifikační IT údaje** e-mailová adresa	ne	Subjekt OÚ, EIS Magion, jiný pracovník dodavatele
ESSL - Elektronická spisová služba -	Evidence odchozí a příchozí pošty	Správce	Ne	Uchovávání Validace (kontrola) Používání Předávání Nahlížení	ČZU	Odesílatelé; Adresáti	Adresní a identifikační údaje Identifikační IT údaje Další údaje zadané uživatelem	Dle obsahu dokumentu asi ANO	Subjekt OU, provozní db, AD, TI;
Prohlášení o trestní bezúhonosti	Prokázání trestní bezúhonnosti vybraných zaměstnanců	Správce	Ne	Získávání, shromažďování, Uchovávání Validace (kontrola) Používání Nahlížení, Šíření Výmaz	Sekretariát rektora	rektor	Adresní a identifikační údaje jméno, příjmení, adresa, datum narození, **Popisné údaje** titul,	Ne	Od subjektu údajů

Zdroj: vlastní zpracování

Tabulka 3 - Registr zpracování 2

Název zpracování OÚ	Právní titul	Ze zákona?	Četnost zpracování	Rozsah zpracování (velký/malý)	Předávání třetím stranám	Způsob uložení	Prostředek a způsob zpracování	Doba uchování	Je poskytována informace subjektu údajů při získání údajů?	Námitka	Práva subjektu	Informační systém	Správce aktiva (informačního systému)
registr smluv	Plnění právní povinnosti	Ano	denně	malý	ne	Šanony (originály); db	manuálně / automaticky	1 rok pak předáno do archivu na SIC	ne			EIS Magion, DMS, Registr smluv	OIKT, MVCR
ESSL - Elektronická spisová služba -	Oprávněný zájem organizace	Ne	denně	malý	Ne	interní db	manuálně / automaticky	dle skartačního řádu	ne			essl.czu.cz; isds; ti, provozní db, AD	OASS
Prohlášení o trestní bezúhonosti	Oprávněný zájem organizace	Ne	dle potřeby	malý	ano (poskytovatelé grantů a dotací)	fyzická složka na oddělení pro strategii	písemný dokument, manuálně	5 měsíců (neustále se obnovuje)	ne				

Zdroj: vlastní zpracování

4.2 Kritičnost zpracování

Pro výše identifikovaná zpracování OÚ byla následně hodnocena kritičnost zpracování. Seznam pro posouzení kritičnosti zpracování je složen celkem z 10 kritérií. Pro vyhodnocení rizikovosti je důležité, aby správce osobních charakterizoval, popsal a následně mu přiřadit hodnotu kritičnosti, a to dle následujících hodnot:

- Nízká
- Významná
- Kritická

Skupina zpracování s vysokým rizikem pro práva a svobody subjektu údajů podléhající povinnosti provést posouzení vlivu na ochranu osobních údajů (vyjma seznamu z kapitoly 3.4.1.) je stanovena následujícím způsobem:

- Pokud úroveň dvou a více charakteristik zasáhne mezi kritické, potom se DPIA zpracovává
- Pokud jedna úroveň zasáhne mezi kritické a zároveň nejméně pět charakteristik dosáhne významné úrovně, potom se DPIA rovněž zpracovává
- Každá charakteristika se přitom započítává jen jednou (nejvyšší dosaženou) úrovní

4.2.1 Suma kritičnosti zpracování

Suma kritičnosti zpracování je dále počítána dle metodiky pracovní skupiny WP29 podle přiřazených hodnot.

Tabulka 4 - Hodnoty kritérií

Kritéria	Hodnota
Nízká	0
Významná	1
Kritická	3

Zdroj: vlastní zpracování

4.2.2 Kritéria pro posouzení rizikovosti

- Zpracování zahrnující monitorování subjektů údajů

  (podle dokumentu WP248 vypracované skupinou WP 29 se provádí systematické monitorování včetně monitorování veřejně přístupných prostor)

Tabulka 5 - Zpracování zahrnující monitorování subjektů údajů

Hodnota	Popis
Nízká	Subjekty, které jsou identifikovatelné/identifikované prostřednictvím identifikačních údajů. Mohou být docházkové systémy, zvukové záznamy nebo záznamy činností subjektů na síti.
Významná	Zpracování obrazových záznamů identifikovatelných / identifikovaných subjektů údajů za účelem ochrany majetku a zvýšení bezpečnosti osob
Kritická	Zpracování monitorující fyzický pohyb nebo pobyt identifikovatelných / identifikovaných subjektů údajů, a to zejména pomocí jejich souřadnic.

Zdroj: vlastní zpracování

- Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní povahy subjektů údajů

  (podle dokumentu WP 248 se provádí zpracování citlivých údajů nebo údajů vysoce osobní povahy)

Tabulka 6 - Zpracování kritických údajů

Hodnota	Popis
Nízká	Běžné údaje (zahrnující např. váha, výška, pohlaví, věk, účast na kurzech, údaje o členství apod.
Významná	Významné údaje (zahrnující např. identifikační údaje jako jméno, rodné číslo, číslo platební karty, číslo zákaznické karty, heslo/pin, pseudonym apod.
Kritická	Kritické údaje (zahrnující např. údaje z logů, údaje z elektronické pošty, údaje o rasovém nebo etnickém původu, o politických názorech, údaje týkajících se rozsudků ve věcech trestných apod.

Zdroj: vlastní zpracování

- Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí

  (podle dokumentu WP 248 se provádí zpracování údajů týkajících se zranitelných subjektu údajů)

Tabulka 7 - Zpracování vystavující subjekt ohrožení z okolního prostředí

Hodnota	Popis
Nízká	Subjekt údajů je bez zvláštní zranitelnosti
Významná	Časově omezená zranitelnost (nemocní, migranti apod.) nebo situačně daná zranitelnost po omezenou dobu (žadatelé vůči veřejné správě, příjemce vůči zdravotní či sociální podpoře, odběratelé léčiv apod.)
Kritická	Subjekty jsou zařaditelné jako členové vymezené skupiny podle národnosti, náboženství, sexuální orientace, odsouzení pro trestný čin apod.

Zdroj: vlastní zpracování

- Zpracování osobních údajů velkého rozsahu

  (podle dokumentu WP 248 se provádí zpracování v rozsáhlém měřítku)

Tabulka 8 - Zpracování osobních údajů velkého rozsahu

Hodnota	Popis
Nízká	Zpracování osobních údajů malého rozsahu (minimálně 1 kritérium) - do 5 000 subjektů nebo do 0,5‰ populace dotčeného státu - do 2 přistupujících osob/zaměstnanců správce - s 1 - 4 místy zpracování/pobočkami
Významná	Zpracování osobních údajů středního rozsahu (minimálně 1 kritérium) - 5 001 – 10 001 subjektů nebo mezi 0,5 - 1‰ populace dotčeného státu - 2 – 20 přistupujících osob/zaměstnanců správce - 5 – 20 místy zpracování/pobočkami
Kritická	Zpracování osobních údajů velkého rozsahu (minimálně 1 kritérium) - 10 001 subjektů nebo více než 1‰ populace dotčeného státu - nad 20 přistupujících osob/zaměstnanců správce - s více než 20 místy zpracování/pobočkami

Zdroj: vlastní zpracování

- Zpracování zahrnující snímání veřejně přístupných prostor

  (podle dokumentu WP 248 se provádí systematické monitorování, včetně monitorování veřejně přístupných prostor)

Tabulka 9 - Zpracování zahrnující snímání veřejně přístupných prostor

Hodnota	Popis
Nízká	Jde o pozemky majitele, interiéry objektů (bytové domy, průmyslové objekty, prodejny) nebo také velmi omezeně (1-1,5m) veřejná prostranství
Významná	-
Kritická	Jde o veřejná prostranství, pasáže, letiště apod., kamerové systémy monitorující veřejná prostranství ve velkém rozsahu

Zdroj: vlastní zpracování

- Zpracování osobních údajů s omezeným ovlivněním subjekty údajů

  (podle dokumentu WP 248 se provádí zpracování s obtížně uplatnitelnými právy subjektů údajů – pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy a **1** Provádí se hodnocení nebo bodování (fyzických osob), včetně profilování a předpovídání)

Tabulka 10 - Zpracování osobních údajů s omezeným ovlivněním subjekty údajů

Hodnota	Popis
Nízká	Subjekt údajů bez problémů prosazuje svá práva
Významná	Subjektem údajů může jen omezeně ovlivnit některá svá práva (omezeně časově nebo za vymezených podmínek)
Kritická	Subjektem údajů může ovlivnit svá práva jen velmi omezeně nebo vůbec. Provedení zpracování je upraveno právním předpisem nebo automatizovaným rozhodováním.

Zdroj: vlastní zpracování

- Zpracování osobních údajů, s možností jejich následného zveřejnění

  (podle dokumentu WP 248 se provádí zpracování citlivých údajů nebo údajů vysoce osobní povahy a provádí se zpracování s obtížně uplatnitelnými právy subjektů údajů – pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy)

Tabulka 11 - Zpracování osobních údajů, s možností jejich následného zveřejnění

Hodnota	Popis
Nízká	Jde o údaje v rámci zpracování přístupné pouze správci nebo zpracovateli, případně orgánům veřejné moci na základě právních předpisů.
Významná	Jde o údaje v rámci zpracování zpřístupňované správcem omezené (předem vymezené) skupině subjektů.
Kritická	Jde o údaje v rámci zpracování zpřístupňované veřejnosti správcem například na základě právních předpisů

Zdroj: vlastní zpracování

- Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách či platformách

  (podle dokumentu WP 248 se provádí přiřazování nebo slučování datových souborů (kombinace nebo propojování dat různých zpracování), provádí se zpracování v rozsáhlém měřítku a provádí se hodnocení nebo bodování (fyzických osob), včetně profilování a předpovídání)

Tabulka 12 - Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách nebo platformách

Hodnota	Popis
Nízká	Jednoduchý nebo složitý systém bez propojení na jiná zpracování prováděná stejným správcem
Významná	Systém s propojením na jiná zpracování prováděná stejným správcem nebo data získaná od jiných správců původně za různými účely
Kritická	Automatizované expertní systémy, včetně umělé inteligence sloužící k analýzám nebo profilování

Zdroj: vlastní zpracování

- Zpracování osobních údajů s vazbou na jiné správce nebo zpracovatele

  (podle dokumentu WP 248 se provádí přiřazování nebo slučování datových souborů (kombinace nebo propojování dat různých zpracování) a provádí se zpracování s obtížně uplatnitelnými právy subjektů údajů – pro procesy prováděné ve veřejné oblasti, jimž se nemohou vyhnout, nebo zpracování, které má za cíl povolit, změnit nebo odmítnout přístup subjektů údajů k službě nebo uzavření smlouvy)

Tabulka 13 - Zpracování osobních údajů s vazbou na jiné správce nebo zpracovatele

Hodnota	Popis
Nízká	Bez vazeb na jiné správce a/nebo zpracovatele
Významná	S vazbami na jednoznačně vymezené správce a/nebo zpracovatele a lze je uvést vyčerpávajícím seznamem správců a/nebo zpracovatelů
Kritická	Vazba je dána například jen kategorií správce (orgány veřejné moci, nemocnice, školy apod), a to proto, že seznam není možno vyčerpávajícím způsobem určit nebo je proměnlivý apod

Zdroj: vlastní zpracování

- Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení

  (podle dokumentu WP 248 dochází k použití nebo využití nových technologických nebo organizačních řešení)

Tabulka 14 - Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení

Hodnota	Popis
Nízká	Jedná se o řešení, se kterými má správce již zkušenosti, nebo řešení mnohokrát různě nasazená a odzkoušená („řešení na klíč“ apod)
Významná	Nové řešení již známého zpracování u správce
Kritická	Zcela nové řešení, která dosud nebyly nerealizované a se kterými nejsou žádné zkušenosti

Zdroj: vlastní zpracování

Na následující tabulce je uveden příklad pro 3 různá zpracování, dosazeny hodnoty kritérií a vypočítána kritičnost zpracování.

Tabulka 15 - Kritičnost zpracování

Název zpracování OÚ	1. Zpracování zahrnující monitorování subjektů údajů	2. Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní Povahy subjektů údajů	3. Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostředí	4. Zpracování osobních údajů velkého rozsahu	5. Zpracování zahrnující snímání veřejně přístupných prostor	6. Zpracování osobních údajů s omezeným ovlivněním subjekty údajů	7. Zpracování osobních údajů veřejně přístupný	8. Zpracování osobních údajů v technologicky složitých nebo pokročilých infrastrukturách nebo platformách	9. Zpracování osobních údajů s vazbou na jiné správce nebo zpracovate	10.Zpracování osobních údajů s využitím nových technologických nebo organizačních řešení	Rizikové zpracová	∑ kritičnosti (hodnota	Nutnost provádět DPIA
registr smluv	Nízká	Významná	Významná	Nízká	Nízká	Kritická	Kritická	Významná	Nízká	Nízká	Ano	9	Ne
ESSL - Elektronická spisová služba -	Nízká	Kritická	Nízká	Nízká	Nízká	Kritická	Nízká	Významná	Nízká	Nízká	Ano	7	Ano
Prohlášení o trestní bezúhonosti	Nízká	Významná	Významná	Nízká	Nízká	Nízká	Významná	Nízká	Nízká	Nízká	Ne	3	Ne

Zdroj: vlastní zpracování

4.3 Identifikace a hodnocení hrozeb a zranitelností

Identifikace hrozeb a zranitelností jednotlivých zpracování osobních údajů jsou podpůrným aktivem pro veškeré operace OÚ, které jsou během životního cyklu daného zpracování prováděny s ohledem na druh podpůrného média a použitého informačního systému:

- Způsob pořízení dat
- Četnost zpracování
- Předávání třetím stranám

- Způsob uložení
- Způsob zpracování a prostředek
- Doba uchování
- Informační systém.

Pro identifikaci hrozeb a zranitelností je použit Katalog hrozeb dle ISO 29134 (viz Příloha č. 2 - Katalog hrozeb a zranitelností). Před provedením posouzení vlivu je nutno prověřit, zda hrozby a zranitelnosti z katalogu odpovídají specifickým podmínkám kontextu a rozsahu dle účelu jejich zpracování.

Tyto hrozby a zranitelnosti jsou následně hodnoceny s ohledem na pravděpodobnost jejich vzniku. Výsledné hodnoty jsou pak přiřazeny jednotlivým zpracováním na základě pravděpodobnosti jejich výskytu dle následující stupnice.

Tabulka 16 - Pravděpodobnost vzniku hrozby

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

Zdroj: vlastní zpracování

4.3.1.1 Výsledná suma hrozeb

Suma hrozeb je vypočítána jako součet hodnot u všech 47 kritérií s přiřazením hodnot 0, 1, 2 nebo 3. Příklad použití této metody je zobrazen v následující tabulce:

Tabulka 17 - Identifikace a hodnocení hrozeb a zranitelnosti

	Hardware												Software											Počítačové kanály					Jednotlivci								Papírové dokumenty						Kanály přenosu papíru							
Název zpracování OÚ	HW01	HW02	HW03	HW04	HW05	HW06	HW07	HW08	HW09	HW10	HW11	SW01	SW02	SW03	SW04	SW05	SW06	SW07	SW08	SW09	SW10	SW11	CH01	CH02	CH03	CH04	CH05	HU01	HU02	HU03	HU04	HU05	HU06	HU07	HU08	PD01	PD02	PD03	PD04	PD05	PD06	PP01	PP02	PP03	PP04	PP05	PP06	∑ hrozeb	Rizikovost
registr smluv	1	1	1	1	2	1	2	1	2	1	2	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	1	2	2	1	2	2	2	1	1	2	2	1	2	2	1	1	2	1	1	1	1	64	576
ESSL - Elektronická spisová služba -	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	35	245
Prohlášení o trestní bezúhonosti	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	1	1	1	1	1	1	2	2	1	2	1	2	1	2	1	1	1	1	27	81

Zdroj: vlastní zpracování

4.3.2 Výpočet míry rizika

Výsledná míra rizika je počítána jako suma kritičnosti zpracování (viz. kap. 4.2.1.) násobena výslednou sumou hrozeb (viz. kap. 4.3.1.1.):

Míra rizika = ∑ Kritičnosti zpracování x ∑ Míra hrozby

Následně je míra rizika kategorizována na základě níže uvedené tabulky.

Tabulka 18 - Index rizika

Kategorie	Skóre	Riziko a způsob návrhu opatření
1	**0-99**	**Nízké** riziko je považováno za přijatelné.
2	**100-299**	**Střední** riziko by mělo být sníženo na nejnižší možnou přijatelnou míru. Dle rozhodnutí vlastníka rizika mohou být v rámci daného rizika vyhodnoceny největší hrozby a pro ně mohou být přijata odpovídající opatření za účelem ošetření rizika, pokud je to vhodné (např. odpovídající poměr náklady na opatření vs. přínosy).
3	**300 a vyšší**	**Vysoké** riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění. Opatření je nutné stanovit vůči jednotlivým hrozbám v maximální míře podrobnosti tak, aby byl doložen důkaz, že žádná klíčová hrozba nebyla opomenuta.

Zdroj: vlastní zpracování

Hodnoty kategorií jsou záměrně stanoveny velmi nízko, protože vedení univerzity klade velký důraz na bezpečné nakládání s osobními údaji.

4.4 Výběr variant pro ošetření rizik

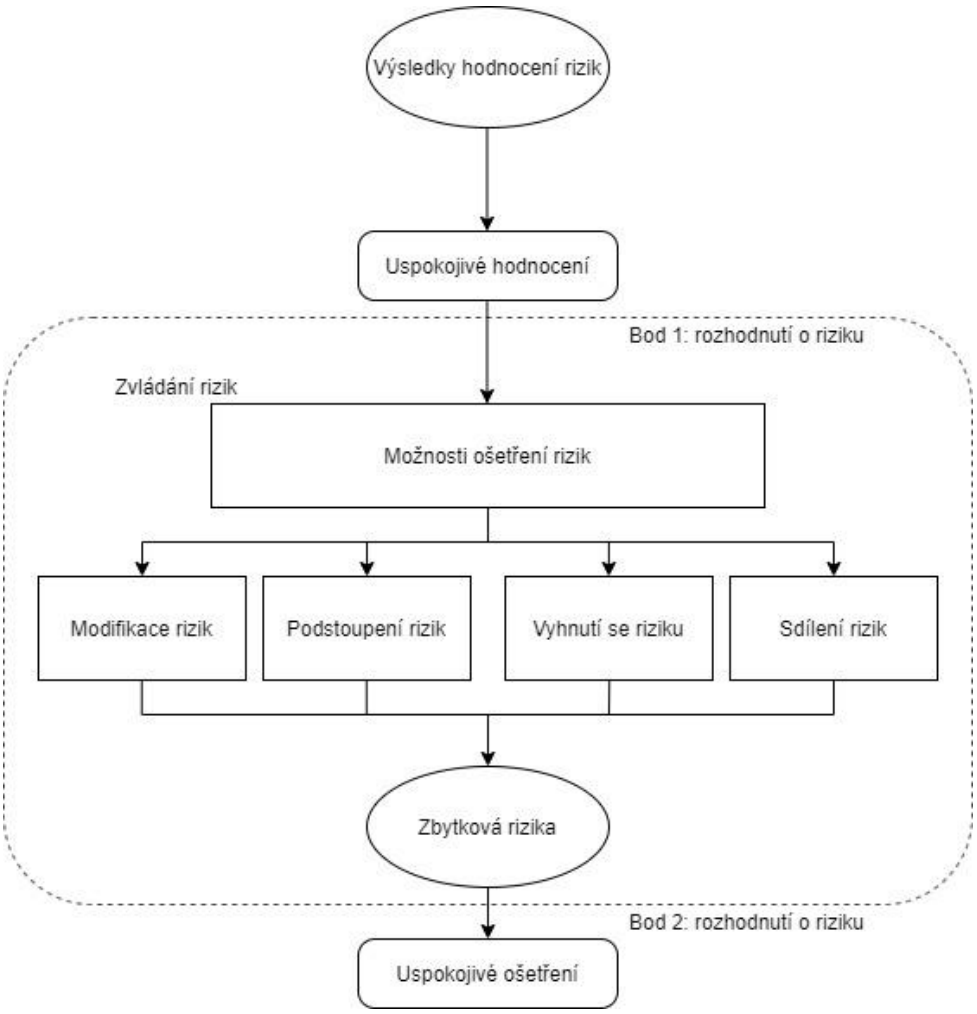
Výstupem je rozhodnutí o způsobu ošetření rizik neboli plán ošetření, který stanovuje, jak zabezpečit jednotlivá rizika nespadající do kategorie „akceptovatelná“.

Základní metody zvládání rizik v souladu s normou ČSN ISO/IEC 27005:2011 jsou:

- Modifikace rizik bezpečnosti informací

- Akceptace (podstoupení) rizik bezpečnosti informací
- Vyhnutí se riziku bezpečnosti informací
- Sdílení rizik bezpečnosti informací

Obrázek 3 - Ošetření rizik (ČSN ISO/IEC 27005:2011)



Zdroj: vlastní zpracování

4.4.1 Modifikace rizik bezpečnosti informací

Modifikace rizik spočívá v převodu konkrétního rizika do formy, která umožní snížení rizika tak, aby bylo přijatelné nebo aby jej bylo možné lépe monitorovat. Za účelem modifikace rizik by měla být vybrána vhodná a odůvodněná opatření.

4.4.2 Akceptace (podstoupení) rizik bezpečnosti informací

Jestliže úroveň rizika splňuje kritéria jeho akceptace, není zapotřebí přijímat další opatření a riziko lze podstoupit. Musí však jasně vyhovovat legislativním požadavkům, politikám a kritériím pro akceptaci rizik.

Rozhodnutí o akceptaci rizika bez další akce musí být učiněno v závislosti na hodnocení rizik. Akceptace rizika přichází v úvahu v případě rizik s méně častým výskytem nebo sice možným, ale minimálně pravděpodobným vznikem, kdy protiopatření představují vyšší náklady než bezpečnostní zisk.

Vstupem pro akceptaci rizik jsou rizika označena jejich analýzou jako akceptovatelná. Výstupem je pak odsouhlasený seznam akceptovaných rizik s jejich odůvodněním.

Akceptace rizik musí být formálně zaznamenána a schválena. V případě akceptace rizika musí být jednoznačně dohledatelná odpovědnost za dané rozhodnutí (autor návrhu akceptace rizika, projednání, formální akceptace).

4.4.3 Vyhnutí se riziku bezpečnosti informací

Pokud je to možné, je zapotřebí vyhnout se činnostem, které dávají riziku vzniknout. To je vhodné provést zejména v případech, kdy:

- Jsou identifikovaná rizika považována za příliš vysoká
- Náklady na implementaci ošetření rizika převyšují přínosy

4.4.4 Sdílení rizik bezpečnosti informací

Sdílení rizik znamená, že riziko je sdíleno s třetí stranou, která je schopná toto nebezpečí účinněji zvládat. V případě sdílení rizika s externími subjekty mohou vznikat nová rizika nebo se mohou měnit již existující, dříve identifikovaná a řízená rizika.

Sdílení rizika lze též provést formou pojištění, které bude pokrývat následky nebo uzavřením smlouvy s partnerem zajišťující dozor nad systémem a bude schopen přijmout okamžitá opatření k nápravě.

Je možné sdílet odpovědnost za zvládnutí rizika, ale nelze sdílet odpovědnost za jeho dopad. Tj. za případnou nefunkčnost systému bude vždy odběratel služby posuzovat chybu provozovatele, nikoli chybu jiné služby nebo organizace. Zákazníka nezajímá, že není funkční síť, kterou spravuje třetí subjekt, ale zajímá ho, že jím vyžadovaná služba není dostupná.

4.4.5 Komunikace a konzultace rizik

Vstupem komunikace a konzultace rizik jsou veškeré informace o rizicích získané v průběhu procesu jejich řízení. Během této komunikace je získávána dohoda o tom, jak rizika řídit mezi různými subjekty (zainteresované strany, organizační jednotky, dodavatelé atd.), kterých se dotýkají.

Výstupem je trvalé chápání procesu řízení rizik bezpečnosti informací a výsledků tohoto procesu.

4.5 Návrh opatření pro zajištění osobních údajů

Organizační a technická opatření vyplývají ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Dále je uveden výčet těchto opatření.

4.5.1 Organizační opatření

- Systém řízení bezpečnosti informací
- Řízení rizik
- Bezpečnostní politika
- Organizační bezpečnost
- Stanovení bezpečnostních požadavků pro dodavatele
- Řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému
- Řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému
- Akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů
- Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Řízení kontinuity činností
- Kontrola a audit kritické informační infrastruktury a významných informačních systémů

4.5.2 Technická opatření

- Fyzická bezpečnost
- Nástroj pro ochranu integrity komunikačních sítí

- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kódem
- Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a správců
- Nástroj pro detekci kybernetických bezpečnostních událostí
- Nástroj pro sběr a vyhodnocení kybernetických a bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti informací
- Bezpečnost průmyslových a řídících systémů

4.5.3 Opatření a návaznost na hrozby

Postup výběru opatření je takový, kdy po výpočtu rizika následuje zjištění, zda se jedná o riziko přesahující míru akceptovatelnosti. To je pak určeno k redukci pomocí opatření vybraných na základě informací, jaké hrozby na něj působí.

Pro hrozby (viz. Příloha č. 2) jsou následně vybírána vhodná opatření z Katalogu opatření uvedeného v ISO/IEC 29151. Pokud je přijato například jedno opatření, které pokryje danou hrozbu, čímž se sníží pravděpodobnost její realizace tak, že riziko klesne pod akceptovatelnou míru, pak stačí přijmout toto jedno opatření. Druhým případem je situace, kdy se jedním přijatým opatřením nepodaří riziko dostatečně snížit a pak je nutné přijmout dodatečná opatření. Znamená to totiž, že dané riziko působí ještě jiné další hrozby, které se uplatňují vůči tomuto zpracování.

V Příloze č. 3 je uvedena tabulka mapování bezpečnostních opatření vyplývajících z ISO/IEC 29151 a její návaznost na hrozby z Přílohy č. 2, ke které se daná opatření vztahují. Ta jsou rozdělena podle typu na organizační a technická.

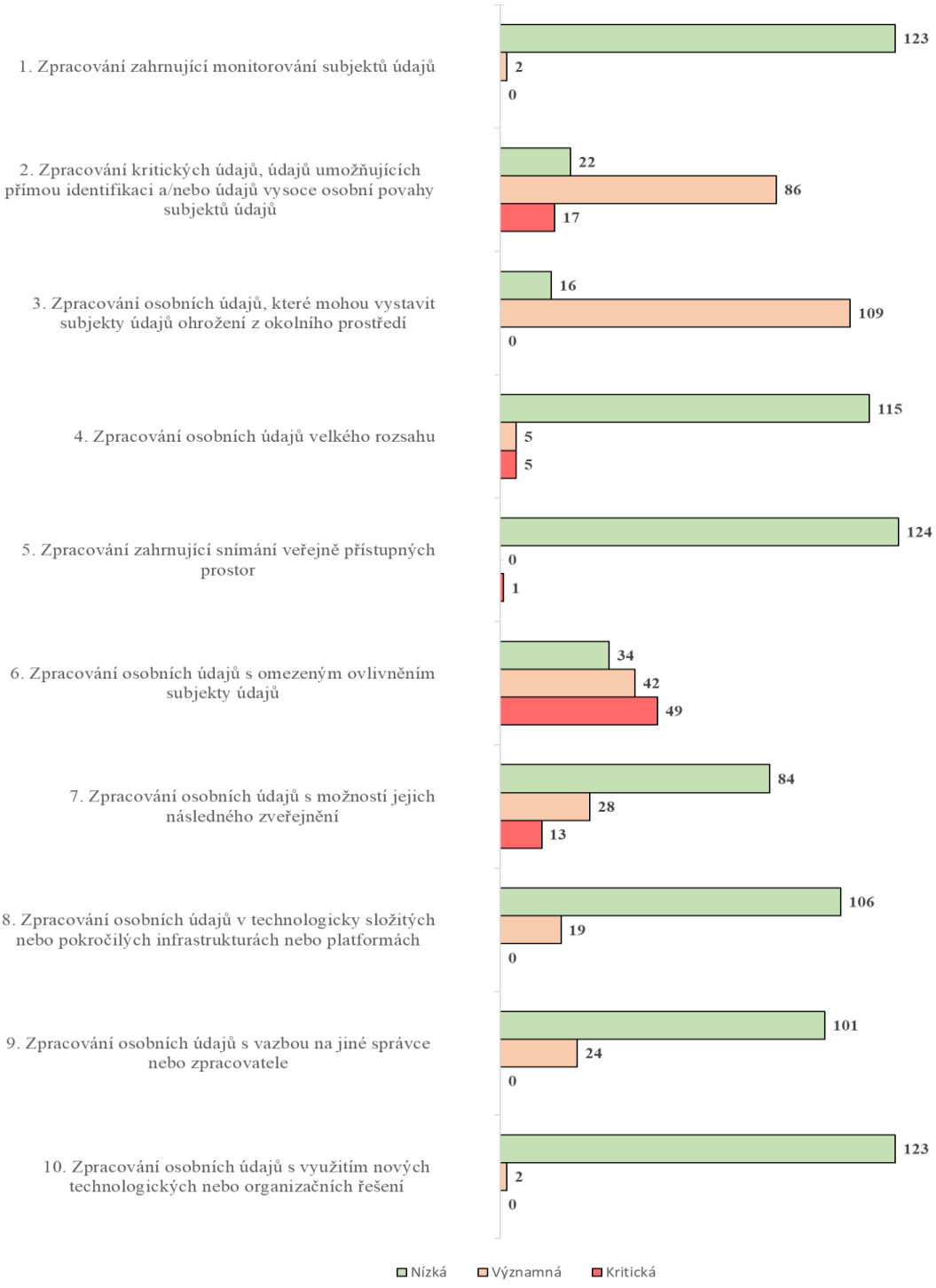
5 Výsledky a diskuse

5.1 Kritičnost zpracování

Podle informací popsaných v kap. 4.2. je kritičnost zpracování vyhodnocena na základě přiřazení hodnoty každému z deseti kritérií (viz kap. 4.2.2.) stanovených Úřadem pro ochranu osobních údajů. Tyto hodnoty jsou dosazeny do všech ze 125 zpracování uvedených v registru České zemědělské univerzity v Praze ke dni 31.12.2019.

Následující tabulka ukazuje zařazení všech zpracování podle jejich hodnoty kritičnosti na základě každého z deseti hodnotících kritérií.

Tabulka 19 - Kritičnost zpracování



Zdroj: vlastní zpracování

5.1.1 Rizikové zpracování

Podle hodnocení kritičnosti zpracování bylo vyhodnoceno, zda se jedná o rizikové zpracování (blíže popsané v kapitole 4.2.), a tedy zda je nutné provádět posouzení vlivu na ochranu osobních údajů DPIA. Po dosazení hodnot vyšlo celkem 14 zpracování popsaných v následujících tabulkách:

Tabulka 20 - Rizikové zpracování 1

Název zpracování OÚ	1. Zpracování zahrnující monitorování subjekt údajů	2. Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní Povahy subjekt údajů	3. Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolního prostře	4. Zpracování osobních údajů velkéh rozsah	5. Zpracování zahrnující snímání veřejně přístupn prosto	6. Zpracování osobních údajů s omezeným ovlivněním subjekt údajů	7. Zpracování osobních údajů veřejn přístupn	8. Zpracování osobních údajů v technologick y složitých nebo pokročilých infrastruktur ách neb platform	9. Zpracování osobních údajů s vazbou na jiné správce nebo zpracova	10.Zpracován í osobních údajů s využitím nových technologick ých nebo organizač h řeše	Riziko zpraco	∑ kritičn (hodno	Nutnost provádět DPIA
registr smluv	Nízká	Významná	Významná	Nízká	Nízká	Kritická	Kritická	Významná	Nízká	Nízká	Ano	9	Ne
ESSL - Elektronická spisová služba -	Nízká	Kritická	Nízká	Nízká	Nízká	Kritická	Nízká	Významná	Nízká	Nízká	Ano	7	Ano
Úrazová evidence	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Nízká	Nízká	Významná	Nízká	Ano	8	Ne
Podpora studia UIS a Moodle	Nízká	Kritická	Významná	kritická	Nízká	Významná	Významná	Významná	Nízká	Nízká	Ano	10	Ano
školka, Poníček	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Významná	Nízká	Nízká	Nízká	Ano	8	Ne
Plnění pracovně-právních smluv a povinností Kostelec	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Významná	Nízká	Nízká	Nízká	Ano	8	Ne
Úrazová evidence, Kostelec	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Významná	Nízká	Nízká	Nízká	Ano	8	Ne

Zdroj: vlastní zpracování

Tabulka 21 - Rizikové zpracování 2

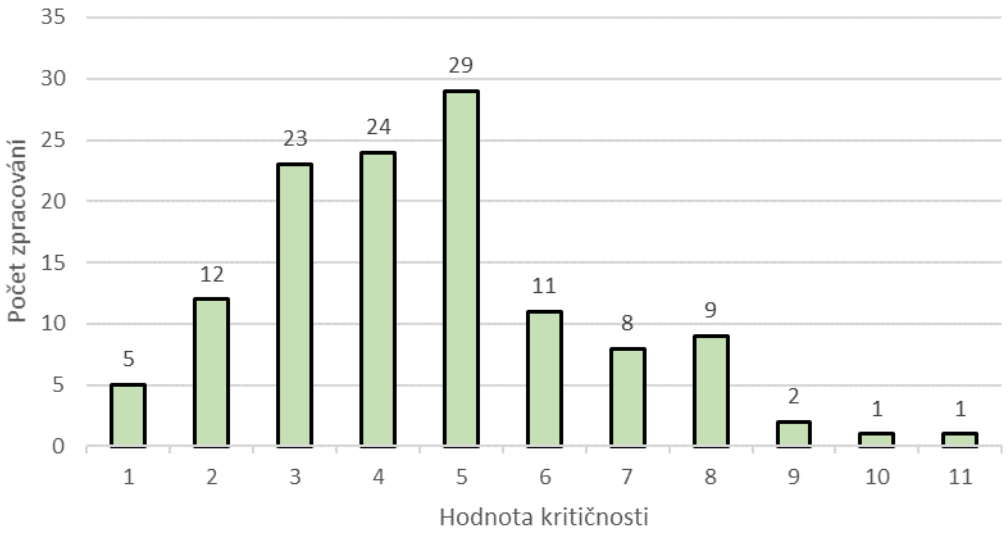
Název zpracování OÚ	1. Zpracování zahrnující monitorování subjekt údajů	2. Zpracování kritických údajů, údajů umožňujících přímou identifikaci a/nebo údajů vysoce osobní Povahy subjekt údajů	3. Zpracování osobních údajů, které mohou vystavit subjekty údajů ohrožení z okolní prostře	4. Zpracování osobních údajů velkéh rozsah	5. Zpracování zahrnující snímání veřejně přístupn prosto	6. Zpracování osobních údajů s omezeným ovlivněním subjekt údajů	7. Zpracování osobních údajů veřejn přístupn	8. Zpracování osobních údajů v technologick y složitých nebo pokročilých infrastruktur ách neb platform	9. Zpracování osobních údajů s vazbou na jiné správce nebo zpracova	10.Zpracován i osobních údajů s využitím nových technologick ých nebo organizač h řeše	Riziko zpraco	Σ kritičn (hodno	Nutnost provádět DPIA
Pojistné události, Kostelec	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Významná	Nízká	Nízká	Nízká	Ano	8	Ne
Lékařské prohlídky	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Nízká	Nízká	Významná	Nízká	Ano	8	Ne
evidenci docházky eTablo	Nízká	Významná	Významná	Nízká	Nízká	Kritická	Kritická	Významná	Významná	Významná	Ano	11	Ne
veřejně přístupné údaje e-Tablo	Nízká	Významná	Významná	Nízká	Nízká	Nízká	Kritická	Významná	Významná	Významná	Ano	8	Ano
Zveřejňování prací	Nízká	Významná	Významná	Nízká	Nízká	Kritická	Kritická	Nízká	Nízká	Nízká	Ano	8	Ne
Přijímací řízení	Nízká	Kritická	Nízká	Kritická	Nízká	Kritická	Nízká	Nízká	Nízká	Nízká	Ano	9	Ne
Výplata sociálních stipendií	Nízká	Kritická	Významná	Nízká	Nízká	Kritická	Významná	Nízká	Nízká	Nízká	Ano	8	Ne

Zdroj: vlastní zpracování

5.1.2 Suma kritičnosti zpracování

Použitím metodiky, popsané v kapitole 4.2.1. pro kvantifikování sumy kritičnosti zpracování, je vypočítána hodnota u všech 125 zpracování uvedených v registru ČZU. Následující graf ukazuje, v jakém složení a s jakými hodnotami zpracování vystupují.

Tabulka 22- Suma kritičnosti zpracování



Zdroj: vlastní zpracování

U zpracování, která jsou hodnocena jako riziková a je tak u nich požadavek pro vypracování DPIA, je výsledná suma kritičnosti následující:

Tabulka 23 - Suma kritičnosti zpracování u rizikových zpracování

Název zpracování	Počet hodnot nízká	Počet hodnot významná	Počet hodnot kritická	Suma kritičnosti zpracování
Registr smluv	5	3	2	9
ESSL – Elektronický spisová služba	7	1	2	7
Úrazová evidence	6	2	2	8
Podpora studia UIS a Moodle	4	4	2	10
Školka Poníček	6	2	2	8

Název zpracování	Počet hodnot nízká	Počet hodnot významná	Počet hodnot kritická	Suma kritičnosti zpracování
Plnění pracovně-právních smluv a povinností dle zákoníku práce a souvisejících předpisů	6	2	2	8
Úrazová evidence - Kostelec	6	2	2	8
Pojistné události	6	2	2	8
Lékařské prohlídky	6	2	2	8
Evidence docházky e-Tablo	3	5	2	11
Veřejně přístupné údaje e-Tablo	4	5	1	8
Zveřejňování prací	6	2	2	8
Přijímací řízení	7	0	3	9
Výplata sociálních stipendií	6	2	2	8

Zdroj: vlastní zpracování

Výsledná suma kritičnosti slouží pro vypočítání výsledné míry rizika. Není tak brána jako posuzovací kritérium pro zpracování, u kterých bude nutné vypracovat posouzení vlivu na ochranu osobních údajů.

Na základě pokynů Úřadu pro ochranu osobních údajů byla vyjmuta zpracování, která nepodléhají požadavku pro vypracování DPIA (viz kap. 3.4.1.). Výsledný seznam rizikových zpracování, u kterých je povinnost provádět DPIA vypadá následovně:

Tabulka 24 - Suma kritičnosti zpracování u zpracování podléhajících DPIA

Název zpracování	Počet hodnot nízká	Počet hodnot významná	Počet hodnot kritická	Suma kritičnosti zpracování
ESSL – Elektronický spisová služba	7	1	2	7
Podpora studia UIS a Moodle	4	4	2	10
Veřejně přístupné údaje e-Tablo	4	5	1	8

Zdroj: vlastní zpracování

5.2 Identifikace a hodnocení hrozeb a zranitelností

Identifikace a hodnocení hrozeb a zranitelností, dle metodiky popsané v kap. 4.3. a příloze č. 2, je ukázána na příkladech zpracování, u kterých je nutné provést posouzení vlivu na ochranu osobních údajů, a to konkrétně:

- ESSL – elektronická spisová služba
- Podpora studia UIS a Moodle
- Veřejně přístupné údaje e-Tablo

Ve všech případech se jedná o elektronické zpracování, tudíž se zde nevyskytují hrozby a zranitelnosti z kategorií papírových dokumentů ani kanálů přenosu papíru. V těchto skupinách je tedy dosazena hodnota 0.

Naopak skupiny obsahující hardware, software, počítačové kanály či samotní jednotlivci hrozby a zranitelnosti zastupují. V některých případech, kdy je hrozba málo

pravděpodobná až pravděpodobná je jí přiřazena hodnota 1. Předpokládaná realizace takové hrozby je v rozpětí od 1 roku do 5 let.

V případě že se jedná o hrozbu pravděpodobnou až velmi pravděpodobnou, s předpokládanou dobou realizace od 1 měsíce do 1 roku, bude jí přiřazena hodnota 2.

Hodnota 3 nebyla v tomto případě vůbec použita, neboť ani v jednom z případů se nejednalo o hrozbu jistou.

Na následující tabulce jsou přiřazeny hodnoty k jednotlivým hrozbám pro výše zmíněné 3 zpracování.

Tabulka 25 - Identifikace a hodnocení hrozeb

	Hardware											Software										Počítačové kanály					Jednotlivci							Papírové dokumenty						Kanály přenosu papíru						
Název zpracování OÚ	HW01	HW02	HW03	HW04	HW05	HW06	HW07	HW08	HW09	HW10	HW11	SW01	SW02	SW03	SW04	SW05	SW06	SW07	SW08	SW09	SW10	SW11	CH01	CH02	CH03	CH04	CH05	HU01	HU02	HU03	HU04	HU05	HU06	HU07	HU08	PD01	PD02	PD03	PD04	PD05	PD06	PP01	PP02	PP03	PP04	PP05	PP06	∑ hrozeb
ESSL - Elektronická spisová služba -	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	35
Podpora studia UIS a Moodle	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	38
veřejně přístupné údaje e-Tablo	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	39

Zdroj: vlastní zpracování

Součet jednotlivých hodnot následně slouží pro výpočet míry rizika daného zpracování.

Tabulka 26 - Suma hrozeb podléhajícím posouzení vlivu DPIA

Zpracování	Suma míry hrozeb
ESSL – elektronická spisová služba	35
Podpora studia UIS a Moodle	38
Veřejně přístupné údaje e-Tablo	39

Zdroj: vlastní zpracování

5.2.1 Výpočet míry rizika

Jak již bylo zmíněno v kapitole 4.3.2., výsledná míra rizika se vypočítá jako součin sumy kritičnosti zpracování a sumy míry hrozeb.

$$\textbf{Míra rizika} = \sum \textbf{Kritičnosti zpracování} \times \sum \textbf{Míra hrozby}$$

Tento výpočet byl dále použit pro zpracování dat z tabulek č. 16 a 17. Mimo výslednou míru rizika je zde pro přehlednost uvedena také kategorie Indexu rizika, do které dané zpracování, na základě míry rizika, spadá.

Tabulka 27 - Míra rizika

Zpracování	Suma kritičnosti zpracování	Suma míry hrozeb	Míra rizika	Index rizika
ESSL – elektronická spisová služba	7	35	245	Střední
Podpora studia UIS a Moodle	10	38	380	Vysoké
Veřejně přístupné údaje e-Tablo	8	39	312	Vysoké

Zdroj: vlastní zpracování

Dle indexu rizika (blíže popsaném v kap. 4.3.2.) zpracování „ESSL - elektronická spisová služba“ spadá do kategorie „Střední riziko“ a na základě opatření by mělo být sníženo na nejnižší možnou přijatelnou míru. Podle rozhodnutí vlastníka rizika však mohou být v rámci konkrétního nebezpečí vyhodnoceny pouze největší hrozby a pro ně navrhnouta odpovídající opatření, pokud je to v daném případě možné (např. odpovídající poměr mezi náklady na opatření a přínosy).

Zbylé dvě zpracování „Podpora studia UIS a Moodle“ a „Veřejně přístupné údaje e-Tablo“ spadají do kategorie „Vysoké riziko“, které je nepřípustné, a proto musí být neprodleně zahájeny kroky k jeho odstranění. Opatření je nutné stanovit vůči jednotlivým hrozbám v maximální míře podrobnosti tak, aby bylo možné doložit, že žádná klíčová hrozba nebyla opomenuta.

5.3 Seznam opatření a návaznost na hrozby

V návaznosti na míru rizika a hodnocení hrozeb a zranitelností, následuje seznam opatření sloužící jako doporučená příručka, jak postupovat při zvýšeném riziku na základě

norem ISO. Konkrétně norma ISO/IEC 29151 uvádí seznam opatření, který je součástí Přílohy č. 3 – Katalog opatření.

Následující tabulky uvádí soupisy možných opatření na základě četnosti jejich výskytu u hrozeb popsaných v předchozí kapitole. Je uvedeno vždy 8 nejčastěji se vyskytujících opatření v každém ze tří nejrizikovějších zpracování.

Popis dalších 28 možných opatření ke všem třem rizikovým zpracováním je uveden v příloze č. 4, 5 a 6.

Tabulka 28 - Seznam 8 nejčetnějších opatření pro zpracování ESSL – Elektronická spisová služba

ID Opatření	Název opatření	Návaznost na počet hrozeb
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	35
OR 2	Pokyny vedení pro bezpečnost informací	35
OR 3	Stanovení organizace ochrany osobních údajů	35
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	35
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	35
OR 13	Stanovení postupů a odpovědností ICT provozu	12
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	11
OR 21	Dodržování právních a smluvních požadavků	11

Zdroj: vlastní zpracování

Tabulka 29 - Seznam 8 nejčetnějších opatření pro zpracování Podpora studia UIS a Moodle

ID Opatření	Název opatření	Návaznost na počet hrozeb
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	38
OR 2	Pokyny vedení pro bezpečnost informací	38
OR 3	Stanovení organizace ochrany osobních údajů	38
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	38
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	38
OR 13	Stanovení postupů a odpovědností ICT provozu	14
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	14
OR 21	Dodržování právních a smluvních požadavků	12

Zdroj: vlastní zpracování

Tabulka 30 - Seznam 8 nejčetnějších opatření pro zpracování Veřejně dostupné informace e-Tablo

ID Opatření	Název opatření	Návaznost na počet hrozeb
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	39
OR 2	Pokyny vedení pro bezpečnost informací	39
OR 3	Stanovení organizace ochrany osobních údajů	39
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	39
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	39
OR 13	Stanovení postupů a odpovědností ICT provozu	14
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	12
OR 21	Dodržování právních a smluvních požadavků	12

Zdroj: vlastní zpracování

Na základě výsledků a dosažených hodnot v jednotlivých tabulkách je zřejmé, že doporučená opatření na ochranu osobních údajů během jejich zpracování, které vyšly jako nejvíce rizikové, budou zejména opatření organizační. Organizace by na tomto základě měla vyhodnotit, která z opatření již v praxi aplikuje, a to jak za účelem snížení, tak úplné eliminace této hrozby, nebo zda se bude navrženými kroky a jejich aplikací zabývat v blízké budoucnosti.

Z dostupných informací je známo, že univerzita dlouhodobě dbá na snižování rizik zaváděním organizačních opatřená a jejich aplikací v praxi. Pravidelně aktualizuje směrnice, dbá na pokyny vedení bezpečnosti informací, systém organizace ochrany osobních údajů obsahuje ve své směrnici, dodržuje své právní a smluvní požadavky a další.

Univerzita přistupuje k ochraně osobních údajů s péčí a bezpečností, a tak dlouhodobě udržuje soulad s GDPR.

5.4 Záznam o posouzení vlivu na ochranu osobních údajů

Povinnost pro správce osobních údajů, vyplývajících z nařízení kontrolního úřadu České republiky, je vypracovat zprávu dokládající zjištění rizikového zpracování, u kterého je nutno posoudit jeho vliv na ochranu osobních údajů. Tento dokument následně slouží jako záznam pro kontrolní úřad a oficiální dokument pro zjištěný stav.

Formální i obsahová stránka dokumentu, posuzujícího skutečnosti o zpracování, je vždy na samotné organizaci. V kap, 3.4. je uveden minimální seznam požadavků, které by měl dokument obsahovat. Na organizaci je pak doplnění o další informace o daném zpracování. Takto formulovaný dokument by měl organizaci postačit i jako oficiální záznam pro kontrolní úřady.

Níže je vypracován dokument pro zpracování – Veřejně přístupné údaje e-Tablo.

Tabulka 31 - Záznam o posouzení vlivu na ochranu osobních údajů

Název zpracování	**Veřejně přístupné údaje e-Tablo**
Popis zpracování	Veřejně přístupné údaje v systému e-Tablo, kdy cílem je podat informace o přítomnosti osob v budově, a to v rozsahu jednoho měsíce. Systém zaznamenává i dovolenou, účast na akcích v terénu nebo návštěvu u lékaře.
Systematický popis zpracování: Jedná se o zabudovaný tablet, na kterém lze zjistit údaje	
Zpracovávané osobní údaje	Jméno, email, tituly, pozice, kancelář, kalendář, přítomnost, dovolené, činnost v terénu, návštěva lékaře, fotografie, délka pracovní doby.

Příjemci osobních údajů	Kdokoliv, kdo přijde do budovy, dále jsou možné přístupy přes webové rozhraní, zejména pro vedoucí pracovníky, co zpracovávají docházku.
Doba zpracování	Po dobu platnosti smlouvy zapsaných osob s přesahem 30 dní.
Přístup k osobním údajům	Kdokoliv, kdo přijde do budovy, dále jsou možné přístupy přes webové rozhraní, zejména pro vedoucí pracovníky, co zpracovávají docházku.
Účel zpracování	Cílem je podat informace o přítomnosti osob na budově, a to v rozsahu jednoho měsíce.
Právní titul	Souhlas
Oprávněné zájmy správce	Nejsou
Prostředky zpracování	Systém e-Tablo ke shlédnutí na místě s možností dálkového přístupu. Případně možný opis nebo nafocení.
Soulad s kodexy chování	Nejsou
Nezbytnost a přiměřenost operací z hlediska účelů zpracování:	
Posouzení nezbytnosti	Údaje jsou potřebné pro zajištění výukové činnosti
Posouzení přiměřenosti	Zveřejnění nepřiměřeného množství údajů.
Posouzení rizik pro práva a svobody subjektu údajů:	
Identifikace hrozeb	Sledování a stalking, zneužití údajů o určité osobě, upravení údajů za účelem poškození
Identifikace zdrojů hrozeb	Od jiného subjektu údajů (studentů, jiných zaměstnanců, jiných fyzických osob v areálu univerzity)
Identifikace potenciální újmy	Ztráta soukromí, změna výkazu o pobytu v zaměstnání

Zhodnocení pravděpodobnosti vzniku újmy	Pravděpodobnost spíše malá, nicméně velice snadná k provedení
Zhodnocení závažnosti újmy	Vysoká závažnost při ztrátě soukromí.
Posouzení opatření k řešení rizik	Přístup pouze přes studentskou/zaměstnaneckou kartu, kdy je případná viník snáze dohledatelný.
Posouzení opatření k doložení souladu	Existuje příručka a postup pro správné zacházení a pracování se systémem
Posudek DPO	Zpracování veřejně přístupných údajů e-Tablo bylo vyhodnoceno jako neadekvátní. Správci tohoto systému a zařízení je doporučeno, aby omezil veřejně přístupné informace pouze na přijatelné minimum, a to: jméno, příjmení, tituly, pozice, kancelář, email a fotografie vyplněná samotným subjektem OU
Výsledné stanovisko	Zpracování bylo vyhodnoceno jako nepřípustné a vysoce rizikové z důvodu omezení soukromí subjektu OÚ. Hrozbu představuje zejména fakt, že kdokoliv vidí a dokáže zjistit, zda a v jaké časy je zaměstnanec v budově či nikoliv, zda je na služební cestě, zda má „homeoffice“ a tudíž je kancelář prázdná. Jako nejméně drastické opatření je navrženo omezení zveřejňování některých OÚ ve veřejném zařízení e-tablo. Jako jedno z variant je i úplné odstranění zařízení pro elektronickou kontrolu docházky.

Zdroj: vlastní zpracování

6 Závěr

Tato diplomová práce se zabývá tématem, které se za poslední dva roky dostalo do podvědomí většiny lidí. GDPR vzbudilo rozruch ještě před nabytím své účinnosti. Obavy z velkých pokut a sankcí pro organizace které osobní údaje zpracovávají nebyly ojedinělé, což mělo za následek vznik nových pracovních pozic a specializovaných společností, které tuto problematiku pomáhají řešit a připravovat na případné kontroly od dozorového úřadu.

S odstupem času ale může většina lidí připustit, že jsou zejména díky tomuto nařízení osobní údaje lépe zabezpečeny. V dnešním virtuálním světě totiž hraje bezpečnost soukromých informací důležitou roli.

Cílem práce bylo za pomoci dostupných zdrojů, včetně zákonů, doporučených norem a vlastní zkušenosti z praxe, zpracovat materiály potřebné pro doložení souladu České zemědělské univerzity v Praze s GDPR.

K vypracování těchto materiálů bylo zapotřebí splnit jednotlivé dílčí úkoly vedoucí k hlavnímu cíli. Nejprve byl použit registr zpracování, který zaznamenává veškerá zpracování osobních údajů na univerzitě. Celkem bylo hodnoceno 125 zpracování (operací, která využívají osobní údaje subjektů údajů). Na základě metodik a kritérii publikovaných Úřadem na ochranu osobních údajů byla následně ohodnocena kritičnost jednotlivých zpracování. Z celkového počtu 125 zpracování bylo 14 vyhodnoceno jako rizikových. Nicméně pouze tři vyžadovaly posouzení vlivu na ochranu osobních údajů na základě výjimek pro zpracování, u kterých není posouzení vlivu vyžadované.

U vybraných rizikových zpracování byla následně provedena identifikace a hodnocení hrozeb a zranitelností, která určila, jaká konkrétní nebezpečí mohou zpracování nejvíce ovlivnit a z jaké oblasti mohou pocházet. Zdrojem většiny hrozeb byly počítačové komponenty, software, kanály počítačové komunikace nebo chyby či nedbalost jednotlivců.

Ke každé z nalezených hrozeb byla navržena doporučená opatření, která umožňují snížit riziko na přijatelnou úroveň. U všech hodnocených zpracování se jednalo o stanovení nových pravidel formou směrnic či předpisů, dodržování pokynů vedení univerzity na bezpečnost informací nebo určení zodpovědných osob za správu a nakládání s osobními údaji Výčet zmíněných opatření je doporučením, na které by se měla univerzita primárně zaměřit.

Vypracován byl také detailní záznam o posouzení vlivu na ochranu osobních údajů podle doporučených metodik, vytvořený pro zpracování s názvem „Veřejně přístupné údaje e-Tablo“. Tento záznam může univerzitě posloužit mimo jiné jako šablona či doporučený postup analýzy dalších zpracování, u kterých bude nutné mít tento dokument vypracovaný. Aby byl dodržen soulad s GDPR, nesmí odpovědné osoby univerzity zapomínat, že posouzení vlivu na ochranu údajů je neustálý proces, nikoliv jednorázová záležitost. České zemědělské univerzitě se podařilo vytyčené cíle splnit a je tak o mnoho blíže k dosažení plného souladu.

7 Seznam použitých zdrojů

- KOLEKTIV AUTORŮ. Úplné Znění č. 1319 - *Zpracování osobních údajů, GDPR*. Ostrava: SAGIT, 2019. ISBN 978-80-7488-353-8
- NONNEMANN, F -- LIDINSKÝ, V. -- MAŠÍN, D. *Praktická příručka GDPR*. Praha: KLIKA, 2018. ISBN 978-80-88298-10-6
- ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: ANAG, 2017. ISBN 978-80-7554-097-3.
- ČESKO. Zákon č. 181 ze dne 23. července 2014 *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: Sbírka zákonů české republiky. Praha: Parlament České republiky, 2014, částka 75.
- ČESKO. Zákon č. 110 ze dne 12. března 2019 *o zpracování osobních údajů*. In: Sbírka zákonů české republiky. Praha: Parlament České republiky, 2019, částka 47.
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů* a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [online]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016R0679
- Vyhláška č. 82/2018 Sb.: *o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. In: . Česko: Národní úřad pro kybernetickou a informační bezpečnost, 2018, ročník 2018, číslo 82.
- ČSN ISO/IEC 27000 *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací* - Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. Třídící znak 36 9790.

- ČSN ISO/IEC 29134 *Informační technologie - Bezpečnostní techniky - Směrnice pro posuzování dopadu na soukromí*. Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018. Třídící znak 36 9712.
- ČSN ISO/IEC 29151 *Informační technologie - Bezpečnostní techniky - Soubor postupů na ochranu osobně identifikovatelných informací*. Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018. Třídící znak 36 9711.
- Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů* a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.*
- Řada norem ISO/IEC 27000 [online]. Praha: Risk Analysis Consultants, 2015 [cit. 2020-09-30]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000
- Úřad pro ochranu osobních údajů. *Pokyny pro posouzení vlivu na ochranu osobních údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679:* s účinností od 4. 11. 2017 [online]. 2020 [cit. 2020-03-30]. *Dostupné z:* https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=31892
- ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *GDPR (Obecné nařízení)* [online]. 2020. Dostupné z: https://www.uoou.cz/gdpr-obecne-narizeni/ds-3938/p1=3938

- ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Metodika obecného posouzení vlivu na ochranu osobních údajů* [online]. 2020 [cit. 2019-10-23]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38693
- ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)* [online]. 2020 [cit. 2018-02-07]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=29003
- ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů* [online]. 2020 [cit. 2020-01-08]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940
- ŠKORNIČKOVÁ, Eva. GDPR Obecné nařízení o ochraně osobních údajů prakticky: Pracovní skupina 29 [online]. 2020 [cit. 2020-03-27]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pracovni-skupina-29/

Seznam obrázků

Seznam tabulek

8 Přílohy

Příloha 1- Registr zpracování

1	AV záznam z přednášek a seminářů	**2**	Pořizování fotografií osob pro propagační účely	**3**	Poplatky za ubytování
4	Rekreace na zařízení Janov	**5**	Poskytování ubytování	**6**	Účetnictví
7	registr smluv	**8**	ESSL - Elektronická spisová služba	**9**	Prohlášení o trestní bezúhonnosti
10	Evidence dokumentů	**11**	Zveřejnění kontaktních údajů a osob	**12**	Zpracování smluv; veřejné zakázky
13	Vedení evidence o vypůjčených vozidlech	**14**	Rezervace vozidel	**15**	Průchody na čipovou kartu
16	Úrazová evidence	**17**	Evidence registračních značek automobilů (Cartag)	**18**	Školení BOZP a další povinná školení
19	Evidence kvalifikovaných podpisů (elektronické podpisy, certifikáty)	**20**	Přestupková evidence (zbraně, přestupky)	**21**	Kamerové systémy
22	Čipová karta	**23**	ISIC	**24**	Evidence uživatelů knihovny
25	práce s prezenčním fondem, půjčování	**26**	Poskytování knihovních služeb	**27**	Vedení pomocných evidencí

	klíčů od místností				
28	Vyřizování požadavků na přidělení ISBN	**29**	Objednávání časopisů a knih pro katedry a knihovny	**30**	Placená rešerše materiálů v knihovně
31	Virtuální polytechnická knihovna	**32**	Zajištění slev v knihovnách	**33**	Autoritní záznamy vytvořené při katalogizaci do Souborného katalogu NK ČR
34	IT identity	**35**	Podpora studia UIS a Moodle	**36**	O365 - Poskytování licencí MS Office; poštovní služby a aplikace; úložiště dat; pracovní prostředí
37	UEP - Univerzitní elektronická peněženka	**38**	vědecké publikace	**39**	Pořádání seminářů / workshopů / webinářů včetně rozesílání informací o novinkách
40	GA.czu.cz - Evidence a správa grantů	**41**	CV.czu.cz - Curriculum vitae evidence publikací	**42**	Letní škola v rámci výzkumné spolupráce ESCAPAdE
43	Pořádání vědecký konferencí	**44**	Vydávání vědeckých časopisů	**45**	Evidence strojníků a jejich průkazů
46	Evidence komisařů a	**47**	Evidence výcvikových	**48**	Evidence lektorů a

	jejich průkazů		zařízení		jejich certifikátů
49	Zajištění vydání průkazů účastníkům kurzů	**50**	Univerzita třetího věku: přihláška	**51**	Univerzita třetího věku: průběh studia
52	Univerzita třetího věku: podpora studia a studijní materiály	**53**	U3V: Přihláška	**54**	U3V: Seznam neúspěšných studentů
55	U3V: Seznam úspěšných studentů	**56**	U3V: Evidence kontaktních osob	**57**	U3V: Pořádání seminářů a promocí
58	Online kurz Tutor e-learningového vzdělávání	**59**	U3V: Poskytování vzdělávání	**60**	školka, Poníček
61	Biologická olympiáda	**62**	Letní dětský tábor (LDT)	**63**	Evidence pracovníků na LDT
64	Letní dětská univerzita	**65**	Žádosti o stipendia pro mobility	**66**	Zveřejňování fotografií na sociálních sítích a univerzitním webu
67	Databáze mediálních kontaktů	**68**	Marketing: evidence účastníků kurzů	**69**	databáze absolventů ČZU
70	Poskytování služeb mobilních zařízení	**71**	Eshop	**72**	Studentské poplatky a platby v e-shopu
73	Kostelec: Plnění pracovně-právních	**74**	Kostelec: Poskytování ubytování	**75**	Kostelec: Poskytování

	smluv a povinností				stravování
76	Kostelec: Úrazová evidence	**77**	Kostelec: Pojistné události	**78**	Kostelec: Nájmy nemovitostí
79	Kostelec: Povolení k vjezdu	**80**	Kostelec: Lovecké povolenky - povolenky k lovu	**81**	Kostelec: Rybářské povolenky
82	Kostelec: Samovýroba	**83**	Zajištění jazykového vzdělávání ve spolupráci s JCL	**84**	Poskytování služeb podnikatelského inkubátoru PointOne
85	Evidence životopisů	**86**	Další doklady v rámci přijímacího řízení	**87**	Pracovní smlouvy a pracovní poměr
88	Osobní spis	**89**	Lékařské prohlídky	**90**	Pracovní doba
91	údaje pro evidenci docházky e-Tablo	**92**	evidence docházky e-Tablo	**93**	Evidence ZTP
94	Evidence zaměstnanců/cizinců na Úřadu práce	**95**	Odvody za zaměstnance	**96**	Evidenční listy
97	Sociální dávky při pracovní neschopnosti nebo při ošetřování člena rodiny	**98**	Výplaty, Výpočet výplaty	**99**	Výplatnice
100	Mzdové listy	**101**	Nemocenské pojištění	**102**	Daně
103	Hygiena práce,	**104**	Náborový dorazník,	**105**	Poskytování vzdělání

	kategorizace		brigády		
106	Organizace voleb do akademického senátu	**107**	Zveřejňování prací	**108**	Neplatnost státní zkoušky
109	Přijímací řízení	**110**	Zápis do studia	**111**	Státní zkoušky
112	Přerušení studia	**113**	Vydání diplomu a řádné ukončení studia	**114**	Další způsoby ukončení studia
115	Průkaz studenta	**116**	Výkaz o studiu	**117**	Doklad o zkouškách
117	Potvrzení o studiu	**118**	Disciplinární řízení a vyloučení	**119**	Poplatek za studium
120	Matrika	**121**	Uznání zahraničního vzdělání	**122**	Evidence praxe studenta
123	Výplata ubytovacích stipendií	**124**	Výplata sociálních stipendií	**125**	Výplata mimořádných stipendií

Příloha 2 -Tabulka hrozeb a zranitelností

ID hrozby	Podpůrná aktiva	Akce (dopad na aktivum)	Riziko s dopadem na soukromí	Příklady hrozeb
HW01	Hardware	Abnormální / neobvyklé použití	Ztráta OÚ	Skladování/uložení osobních souborů, osobní užití atd.
HW02	Hardware	Abnormální / neobvyklé použití	Nezákonné přístupy k OÚ	Použití USB flash disků nebo disků, které nejsou vhodné pro citlivost informací, použití nebo přeprava tajného/citlivého hardware pro osobní účely atd.
HW03	Hardware	Poškození	Ztráta OÚ	Záplavy, požár, vandalismus, poškození přirozeným opotřebením, poškození paměťového zařízení atd.
HW04	Hardware	Špionáž	Nezákonné přístupy k OÚ	Sledování obrazovky člověka bez jeho vědomí, focení obrazovky, geolokace hardwaru, dálková detekce elektromagnetických signálů atd.
HW05	Hardware	Ztráta	Ztráta OÚ	Krádež laptopu nebo mobilního telefonu, zbavení se/odstranění zařízení nebo hardwaru atd.

HW06	Hardware	Ztráta	Nezákonné přístupy k OÚ	Krádež laptopu z hotelového pokoje, krádež profesionálního mobilního telefonu kapsářem, získání vyhozeného úložného zařízení nebo hardwaru, ztráta elektronického úložného zařízení atd.
HW07	Hardware	Pozměnění	Ztráta OÚ	Přidání nekompatibilního hardwaru vedoucího k poruchám, vyjmutí komponentů nezbytných pro správné fungování systému atd.
HW08	Hardware	Pozměnění	Nezákonné přístupy k OÚ	Sledování hardwarový keyloggerem, vyjmutí hardwarových komponentů, připojení zařízení (jako je USB flash disk) pro spuštění OS nebo načtení dat atd.
HW09	Hardware	Pozměnění	Nežádoucí změny v OÚ	Přidání nekompatibilního hardwaru vedoucího k poruchám, vyjmutí komponentů nezbytných pro správné fungování aplikace atd.
HW10	Hardware	Přetížení / Zahlcení	Ztráta OÚ	Skladovací jednotka je plná, výpadek proudu, provozní přetížení kapacity, přehřátí, nadměrné teploty atd.

HW11	Hardware	Ztráta pevného disku	Nezákonné přístupy k OÚ	Špatné smlouvy o likvidaci nebo údržbě mohou mít za následek neoprávněný přístup k OÚ atd.
SW01	Software	Abnormální / neobvyklé použití	Ztráta OÚ	Vymazání dat, používání padělaného nebo kopírovaného softwaru, chyba operátora, která smaže data atd.
SW02	Software	Abnormální / neobvyklé použití	Nezákonné přístupy k OÚ	Skenování obsahu, nelegitimní odkazování na data, zvyšování oprávnění, maskování stop použití, posílání spamů přes e-mail, zneužití síťových funkcí atd.
SW03	Software	Abnormální / neobvyklé použití	Nežádoucí změny v OÚ	Nechtěné pozměnění dat v databázi, vymazání souborů potřebných pro správný chod softwaru, chyby operátora, které pozmění data atd.
SW04	Software	Poškození	Ztráta OÚ	Vymazání běžících spustitelných nebo zdrojových kódů, logická bomba atd.

SW05	Software	Špionáž	Nezákonné přístupy k OÚ	Skenování síťových adres a portů, shromažďování konfiguračních dat, analýza zdrojových kódů za účelem nalezení využitelných nedostatků/vad; testování, jak databáze reagují na škodlivé dotazy atd.
SW06	Software	Špionáž	Nezákonné přístupy k OÚ	Skenování síťových adres a portů, napadení zranitelností při poslechu, analýze, podávání zpráv nebo zprostředkovatelských portů a služeb
SW07	Software	Ztráta	Ztráta OÚ	Neobnovení licence pro software používaný pro přístup k datům atd.
SW08	Software	Pozměnění	Ztráta OÚ	Chyby během updatů, konfigurace údržby, zavirování malware, nahrazení komponentů atd.
SW09	Software	Pozměnění	Nezákonné přístupy k OÚ	Sledování softwarovým keyloggerem, zavirování malware, instalace dálkového/vzdáleného administračního nástroje, substituce komponentů atd.

SW10	Software	Pozměnění	Nežádoucí změny v OÚ	Chyby během updatů, konfigurace údržby, zavirování malware, nahrazení komponentů atd.
SW11	Software	Přetížení / Zahlcení	Ztráta OÚ	Překročení velikosti databáze, vkládání dat mimo normální rozsah hodnot atd.
CH01	Počítačové kanály	Poškození	Ztráta OÚ	Odpojená kabeláž / elektrické rozvody, špatný příjem Wi-Fi atd.
CH02	Počítačové kanály	Špionáž	Nezákonné přístupy k OÚ	Zastavení provozu / přenosu Ethernetu, získávání dat odeslaných přes Wi-Fi síť atd.
CH03	Počítačové kanály	Ztráta	Ztráta OÚ	Krádež měděných kabelů atd.
CH04	Počítačové kanály	Pozměnění	Nežádoucí změny v OÚ	"Man-in-the middle" nebo "man in the browser" útok pro pozměnění nebo přidání dat do síťové komunikace, opakovaný útok (znovu poslání zachycených dat), atd.
CH05	Počítačové kanály	Přetížení / Zahlcení	Ztráta OÚ	Zneužití rozsahu / šířky, neoprávněné stahování, ztráta internetového připojení atd.

HU01	Jednotlivci	Abnormální / neobvyklé použití	Nezákonné přístupy k OÚ	Ovlivňování (phishing, sociální inženýrství, podplácení / korupce atd.), vyvíjení nátlaku (vydírání, psychické obtěžování atd.), atd.
HU02	Jednotlivci	Abnormální / neobvyklé použití	Nežádoucí změny v OÚ	Ovlivňování (drby / fámy, dezinformace atd.), atd.
HU03	Jednotlivci	Poškození	Ztráta OÚ	Pracovní nehoda / úraz, nemoc z povolání, jiné zranění a nemoci, smrt, neurologické, psychické nebo psychiatrické onemocnění atd.
HU04	Jednotlivci	Špionáž	Nezákonné přístupy k OÚ	Neúmyslné vyzrazení informací během hovoru, použití poslechových zařízení k odposlechu na setkáních atd.
HU05	Jednotlivci	Ztráta	Ztráta OÚ	Přemístění/přiřazení, ukončení smlouvy nebo propuštění, převzetí celé nebo části organizace atd.
HU06	Jednotlivci	Ztráta	Nezákonné přístupy k OÚ	Přetahování zaměstnanců, změny přiřazení, převzetí celé nebo části organizace atd.

HU07	Jednotlivci	Přetížení / Zahlcení	Ztráta OÚ	Vysoký pracovní tok, stres nebo negativní změny pracovních podmínek, přiřazení zaměstnanců k úkolům mimo jejich schopnosti, špatné používání dovedností atd.
HU08	Jednotlivci	Přetížení / Zahlcení	Nežádoucí změny v OÚ	Vysoký pracovní tok, stres nebo negativní změny pracovních podmínek, přiřazení zaměstnanců k úkolům mimo jejich schopnosti, špatné používání dovedností atd.
PD01	Papírové dokumenty	Poškození	Ztráta OÚ	Stárnutí archivovaných dokumentů, spálení souborů během požáru atd.
PD02	Papírové dokumenty	Špionáž	Nezákonné přístupy k OÚ	Čtení, Fotokopie/kopírování, fotografování atd.
PD03	Papírové dokumenty	Ztráta	Ztráta OÚ	Krádež dokumentů, ztráta šanonů/desek během přesunu, likvidace atd.
PD04	Papírové dokumenty	Ztráta	Nezákonné přístupy k OÚ	Krádež šanonů / desek z kanceláře, krádež pošty z poštovní schránky, znovuzískání vyřazených dokumentů atd.

PD05	Papírové dokumenty	Pozměnění	Nežádoucí změny v OÚ	Změny údajů v šanonech / deskách, nahrazení originálu padělkem atd.
PD06	Papírové dokumenty	Přetížení / Zahlcení	Ztráta OÚ	Postupné vymazávání v průběhu času, dobrovolné vymazávání částí dokumentu atd.
PP01	Kanály přenosu papíru	Poškození	Ztráta OÚ	Ukončení pracovního postupu následujícího po reorganizaci, doručení pošty zastaveno stávkou / útokem atd.
PP02	Kanály přenosu papíru	Špionáž	Nezákonné přístupy k OÚ	Čtení podpisových oběžníkových podpisových archů, reprodukce dokumentů při přepravě atd.
PP03	Kanály přenosu papíru	Ztráta	Ztráta OÚ	Eliminace procesu následujícího po reorganizaci, ztráta společnosti pro doručování dokumentů atd.
PP04	Kanály přenosu papíru	Pozměnění	Ztráta OÚ	Změna v tom, jak je pošta zasílána, reorganizace kanálů pro přenos papíru, změna v pracovním jazyce atd.

PP05	Kanály přenosu papíru	Pozměnění	Nežádoucí změny v OÚ	Změny ve zprávě/interním sdělení bez vědomí autora, změna z jedné podpisové knihy na jinou, posílání několika konfliktních dokumentů atd.
PP06	Kanály přenosu papíru	Přetížení / Zahlcení	Ztráta OÚ	Přetížení poštovní a kurýrní služby, přetížení validačního procesu atd.

Příloha 3 - Návrh opatření

ID Opatření	Název opatření	Návaznost (Příloha 2)
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	HW 1 – HW 11 SW 1 – SW 11 CH 1 – CH 5 HU 1 – HU 8 PD 1 – PD 6 PPO 1 – PPO 6
OR 2	Pokyny vedení pro bezpečnost informací	HW 1 – HW 11 SW 1 – SW 11 CH 1 – CH 5 HU 1 – HU 8 PD 1 – PD 6 PPO 1 – PPO 6
OR 3	Stanovení organizace ochrany osobních údajů	HW 1 – HW 11 SW 1 – SW 11 CH 1 – CH 5 HU 1 – HU 8 PD 1 – PD 6 PPO 1 – PPO 6
OR 4	Stanovení pravidel pro ochranu osobních údajů před vznikem pracovního poměru	HU 1 – HU 4
OR 5	Stanovení pravidel pro ochranu osobních údajů v průběhu pracovního poměru	HU 1 – HU 4 HU 7 – HU 8

OR 6	Stanovení pravidel pro ochranu osobních údajů během procesu ukončení pracovního poměru	HU 1 – HU 6
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	HW 1 – HW 11 SW 1 – SW 11 CH 1 – CH 5 HU 1 – HU 8 PD 1 – PD 6 PPO 1 – PPO 6
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	HW 1 – HW 11 SW 1 – SW 11 CH 1 – CH 5 HU 1 – HU 8 PD 1 – PD 6 PPO 1 – PPO 6
OR 9	Stanovení uživatelských rolí a jejich přístupových oprávnění	SW 1 – SW 2 PD 2
OR 10	Stanovení a vynucování odpovědností uživatelů informačního systému	HW 2, HW 4, HW 5, HW 6, HW 8
OR 11	Zavedení zabezpečených oblastí a pravidel pro práci v nich	HW 1, HW 2, HW 4, PD 1 – PD 5
OR 12	Zavedení fyzické ochrany ICT vybavení	HW 1, HW 3, HW 4, HW 11, CH 3

OR 13	Stanovení postupů a odpovědností ICT provozu	HW 7, HW 9, HW 10, HW 11, SW 1, SW 3, SW 7, SW 8, SW 9, SW 10, CH 1, CH 4
OR 14	Provádění audit informačních systémů zpracovávajících osobní údaje	SW 2
OR 15	Stanovení bezpečnostních požadavků na informační systémy zpracovávajících osobní údaje	HW 1, SW 1, SW 11
OR 16	Stanovení pravidel pro vývojové a podpůrné procesy	HW 7, HW 9, SW 11
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	HW 7, HW 9, HW 11, SW 1, SW 2, SW 6, SW 8, SW 9, SW 10, CH 2, CH 4, PPO 3
OR 18	Dohled a řízení dodavatelsky zajišťovaných služeb	SW 3, SW 6, CH 5, PPO 3, PPO 6
OR 19	Zavedení procesu řízení bezpečnostních incidentů	SW 5, SW 6
OR 20	Stanovení pravidel bezpečnosti osobních údajů v procesech řízení kontinuity	HW 3, HW 10, CH 1, CH 3, CH 5, PD 1
OR 21	Dodržování právních a smluvních požadavků	HW 9, HW 11, SW 1, SW 2, SW 7, HU 3 – HU 8, PPO 1, PPO 4

OR 22	Zavedení procesu testování bezpečnosti osobních údajů	HW 4, SW 2, SW 5, SW 6, CH 2
TE 1	Přijetí opatření pro zabezpečení mobilních zařízení a vzdáleného přístupu k informačnímu systému organizace	HW 1, HW 2, HW 5, HW 6
TE 2	Stanovení pravidel pro ochranu fyzických médií	HW 1, HW 2, HW 3, HW 6, HW 10, HW 11, PD 1 – PD 6, PPO 2, PPO 5
TE 3	Zavedení opatření pro prosazování pravidel řízení přístupu	SW 2, SW 3
TE 4	Zavedení řízení přístupů k systémům a aplikacím	SW 2. SW 3, SW 6
TE 5	Využití kryptografických prostředků pro ochranu dat	HW 2, HW 6, CH 2, CH 4
TE 6	Přijetí opatření chránících před malwarem	SW 2, SW 4, SW 5, SW 8, SW 9, SW 10
TE 7	Provádění zálohování dle zálohovacího plánu	HW 1, HW 3, HW 10, SW 1, SW 3, SW 11
TE 8	Pořizování záznamů z přístupu k osobním údajům a bezpečnostní dohled	HW 8, SW 2 – SW 5, SW 8, SW 9, SW 10, CH 2, CH 5
TE 9	Zavedení pravidel správy softwarového vybavení	SW 4, SW 8, SW 9, SW 10

TE 10	Zavedení procesu řízení technických zranitelností	HW 1, SW 4
TE 11	Zavedení bezpečnostních opatření pro ochranu komunikačních sítí	SW 2, SW 5, SW 6, CH 1, CH 2, CH 4, CH 5
TE 12	Zabezpečení přenášených osobních údajů	HW 2, CH 2, CH 4
TE 13	Stanovení pravidel pro testování	HW 7, HW 9, SW 11
TE 14	Stanovení pravidel pro vysokou dostupnost ICT prostředků	HW 1, HW 3, HW 10, CH 5

Příloha 4 - Seznam opatření pro zpracování ESSL – Elektronická spisová služba

ID Opatření	Název opatření	Návaznost na počet hrozeb
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	35
OR 2	Pokyny vedení pro bezpečnost informací	35
OR 3	Stanovení organizace ochrany osobních údajů	35
OR 4	Stanovení pravidel pro ochranu osobních údajů před vznikem pracovního poměru	4
OR 5	Stanovení pravidel pro ochranu osobních údajů v průběhu pracovního poměru	6
OR 6	Stanovení pravidel pro ochranu osobních údajů během procesu ukončení pracovního poměru	6
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	35
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	35
OR 9	Stanovení uživatelských rolí a jejich přístupových oprávnění	2
OR 10	Stanovení a vynucování odpovědností uživatelů informačního systému	5

OR 11	Zavedení zabezpečených oblastí a pravidel pro práci v nich	3
OR 12	Zavedení fyzické ochrany ICT vybavení	5
OR 13	Stanovení postupů a odpovědností ICT provozu	12
OR 14	Provádění audit informačních systémů zpracovávajících osobní údaje	1
OR 15	Stanovení bezpečnostních požadavků na informační systémy zpracovávajících osobní údaje	3
OR 16	Stanovení pravidel pro vývojové a podpůrné procesy	3
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	11
OR 18	Dohled a řízení dodavatelsky zajišťovaných služeb	3
OR 19	Zavedení procesu řízení bezpečnostních incidentů	2
OR 20	Stanovení pravidel bezpečnosti osobních údajů v procesech řízení kontinuity	5
OR 21	Dodržování právních a smluvních požadavků	11
OR 22	Zavedení procesu testování bezpečnosti osobních údajů	5
TE 1	Přijetí opatření pro zabezpečení mobilních zařízení a vzdáleného přístupu k informačnímu systému organizace	4
TE 2	Stanovení pravidel pro ochranu fyzických médií	6

TE 3	Zavedení opatření pro prosazování pravidel řízení přístupu	2
TE 4	Zavedení řízení přístupů k systémům a aplikacím	3
TE 5	Využití kryptografických prostředků pro ochranu dat	4
TE 6	Přijetí opatření chránících před malwarem	6
TE 7	Provádění zálohování dle zálohovacího plánu	6
TE 8	Pořizování záznamů z přístupu k osobním údajům a bezpečnostní dohled	10
TE 9	Zavedení pravidel správy softwarového vybavení	4
TE 10	Zavedení procesu řízení technických zranitelností	2
TE 11	Zavedení bezpečnostních opatření pro ochranu komunikačních sítí	7
TE 12	Zabezpečení přenášených osobních údajů	3
TE 13	Stanovení pravidel pro testování	3
TE 14	Stanovení pravidel pro vysokou dostupnost ICT prostředků	4

Příloha 5 - Seznam opatření pro zpracování Podpora Studia UIS a Moodle

ID Opatření	Název opatření	Návaznost na počet hrozeb
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	38
OR 2	Pokyny vedení pro bezpečnost informací	38
OR 3	Stanovení organizace ochrany osobních údajů	38
OR 4	Stanovení pravidel pro ochranu osobních údajů před vznikem pracovního poměru	4
OR 5	Stanovení pravidel pro ochranu osobních údajů v průběhu pracovního poměru	6
OR 6	Stanovení pravidel pro ochranu osobních údajů během procesu ukončení pracovního poměru	6
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	38
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	38
OR 9	Stanovení uživatelských rolí a jejich přístupových oprávnění	3
OR 10	Stanovení a vynucování odpovědností uživatelů informačního systému	5

OR 11	Zavedení zabezpečených oblastí a pravidel pro práci v nich	3
OR 12	Zavedení fyzické ochrany ICT vybavení	5
OR 13	Stanovení postupů a odpovědností ICT provozu	14
OR 14	Provádění audit informačních systémů zpracovávajících osobní údaje	2
OR 15	Stanovení bezpečnostních požadavků na informační systémy zpracovávajících osobní údaje	3
OR 16	Stanovení pravidel pro vývojové a podpůrné procesy	3
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	14
OR 18	Dohled a řízení dodavatelsky zajišťovaných služeb	3
OR 19	Zavedení procesu řízení bezpečnostních incidentů	2
OR 20	Stanovení pravidel bezpečnosti osobních údajů v procesech řízení kontinuity	5
OR 21	Dodržování právních a smluvních požadavků	12
OR 22	Zavedení procesu testování bezpečnosti osobních údajů	6
TE 1	Přijetí opatření pro zabezpečení mobilních zařízení a vzdáleného přístupu k informačnímu systému organizace	4
TE 2	Stanovení pravidel pro ochranu fyzických médií	6

TE 3	Zavedení opatření pro prosazování pravidel řízení přístupu	3
TE 4	Zavedení řízení přístupů k systémům a aplikacím	4
TE 5	Využití kryptografických prostředků pro ochranu dat	4
TE 6	Přijetí opatření chránících před malwarem	9
TE 7	Provádění zálohování dle zálohovacího plánu	6
TE 8	Pořizování záznamů z přístupu k osobním údajům a bezpečnostní dohled	13
TE 9	Zavedení pravidel správy softwarového vybavení	6
TE 10	Zavedení procesu řízení technických zranitelností	2
TE 11	Zavedení bezpečnostních opatření pro ochranu komunikačních sítí	8
TE 12	Zabezpečení přenášených osobních údajů	3
TE 13	Stanovení pravidel pro testování	3
TE 14	Stanovení pravidel pro vysokou dostupnost ICT prostředků	4

Příloha 6 - Seznam opatření pro zpracování Veřejně přístupné údaje e-Tablo

ID Opatření	Název opatření	Návaznost na počet hrozeb
OR 1	Stanovení pravidel pro ochranu osobních údajů formou směrnice, nebo jiného závazného interního předpisu.	39
OR 2	Pokyny vedení pro bezpečnost informací	39
OR 3	Stanovení organizace ochrany osobních údajů	39
OR 4	Stanovení pravidel pro ochranu osobních údajů před vznikem pracovního poměru	5
OR 5	Stanovení pravidel pro ochranu osobních údajů v průběhu pracovního poměru	7
OR 6	Stanovení pravidel pro ochranu osobních údajů během procesu ukončení pracovního poměru	7
OR 7	Stanovení odpovědnosti za jednotlivá zpracování osobních údajů a s nimi spojených dat	39
OR 8	Provedení kategorizace a ohodnocení zpracování osobních údajů	39
OR 9	Stanovení uživatelských rolí a jejich přístupových oprávnění	2
OR 10	Stanovení a vynucování odpovědností uživatelů informačního systému	6

OR 11	Zavedení zabezpečených oblastí a pravidel pro práci v nich	4
OR 12	Zavedení fyzické ochrany ICT vybavení	6
OR 13	Stanovení postupů a odpovědností ICT provozu	14
OR 14	Provádění audit informačních systémů zpracovávajících osobní údaje	1
OR 15	Stanovení bezpečnostních požadavků na informační systémy zpracovávajících osobní údaje	3
OR 16	Stanovení pravidel pro vývojové a podpůrné procesy	3
OR 17	Stanovení bezpečnostních požadavků na dodavatelsky zajišťované služby	12
OR 18	Dohled a řízení dodavatelsky zajišťovaných služeb	3
OR 19	Zavedení procesu řízení bezpečnostních incidentů	2
OR 20	Stanovení pravidel bezpečnosti osobních údajů v procesech řízení kontinuity	5
OR 21	Dodržování právních a smluvních požadavků	12
OR 22	Zavedení procesu testování bezpečnosti osobních údajů	6
TE 1	Přijetí opatření pro zabezpečení mobilních zařízení a vzdáleného přístupu k informačnímu systému organizace	4
TE 2	Stanovení pravidel pro ochranu fyzických médií	6

TE 3	Zavedení opatření pro prosazování pravidel řízení přístupu	2
TE 4	Zavedení řízení přístupů k systémům a aplikacím	3
TE 5	Využití kryptografických prostředků pro ochranu dat	4
TE 6	Přijetí opatření chránících před malwarem	7
TE 7	Provádění zálohování dle zálohovacího plánu	6
TE 8	Pořizování záznamů z přístupu k osobním údajům a bezpečnostní dohled	11
TE 9	Zavedení pravidel správy softwarového vybavení	5
TE 10	Zavedení procesu řízení technických zranitelností	2
TE 11	Zavedení bezpečnostních opatření pro ochranu komunikačních sítí	7
TE 12	Zabezpečení přenášených osobních údajů	3
TE 13	Stanovení pravidel pro testování	3
TE 14	Stanovení pravidel pro vysokou dostupnost ICT prostředků	4