Metodika analýzy rizik GDPR

pro pověřence pro ochranu osobních údajů
a zaměstnance
Gymnázia a Jazykové školy s právem státní jazykové zkoušky Zlín

Zlín 2024

schválil: Mgr. Přemysl Šil, MBA, BBA,
ředitel školy

OBSAH

1. POJMY A ZKRATKY ... 3
2. HODNOCENÍ ÚČELŮ ZPRACOVÁNÍ ... 5
2.1. ÚVOD ... 5
2.2. IDENTIFIKACE ÚČELŮ ZPRACOVÁNÍ ... 5
2.3. HODNOCENÍ ÚČELŮ ZPRACOVÁNÍ ... 5
2.4. SESKUPENÍ ÚČELŮ ZPRACOVÁNÍ ... 7
3. HODNOCENÍ RIZIK ... 8
3.1. STANOVENÍ PŮSOBENÍ HROZEB VŮČI ORGANIZACI ... 8
1.1.1 Přehled hrozeb ... 8
3.2. STANOVENÍ ÚROVNĚ HROZEB ... 11
3.2.1 Stanovení frekvence působení hrozeb na účely zpracování ... 11
3.2.2 Stanovení dopadů hrozeb na účel zpracování ... 12
3.2.3 Stanovení zranitelností účelů zpracování ... 13
3.2.4 zaznamenání hodnot identifikovaných hrozeb ... 14
3.3. ANALÝZA RIZIK ... 16
3.3.1 Výpočet rizika ... 16
3.3.2 Parciální rizika ... 16
3.3.3 Souhrnné riziko ... 19
4. ZVLÁDÁNÍ RIZIK ... 21
4.1. VÝPOČET ÚČINNOSTI OPATŘENÍ ... 21
4.2. STANOVENÍ PRIORIT REALIZACE OPATŘENÍ ... 23
4.3. STANOVENÍ ÚROVNĚ AKCEPTOVATELNÉHO RIZIKA ... 23
4.4. ZVLÁDÁNÍ RIZIK ... 23
5. PŘÍLOHY ... 24
5.1. STUPNICE HODNOCENÍ DŮVĚRNOSTI, INTEGRITY, DOSTUPNOSTI A ODOLNOSTI A KRITIČNOSTI ... 24
5.1.1 Stupnice pro hodnocení důvěrnosti ... 24
5.1.2 Stupnice pro hodnocení integrity ... 24
5.1.3 Stupnice pro hodnocení dostupnosti ... 25
5.1.4 Stupnice pro hodnocení kritičnosti ... 25
5.2. POPIS OPATŘENÍ ... 26
NÁZEV OPATŘENÍ ... 26

1. POJMY A ZKRATKY

Analytický nástroj	Analytický nástroj, založený na programu MS Excel, který jednoduchými tabulkovými výpočty připravuje podklady pro analýzu rizik
Bezpečnostní incident	Bezpečnostní událost, která může s významnou pravděpodobností způsobit kompromitaci nebo ohrožení bezpečnosti zpracovávaných osobních údajů.
Bezpečnostní událost	Jakákoli událost, která může negativně ovlivnit bezpečnost osobních údajů.
Dopad hrozby	Velikost škody, kterou může způsobit působení hrozby.
Dostupnost a odolnost	Zajištění, že osobní údaje jsou pro oprávněné uživatele přístupné v okamžiku jejich potřeby. Jedná se o zničení dat, úmyslné blokování či zahlcení technických prostředků, prostřednictvím kterých mají být tyto osobní údaje přístupné v požadovaném čase.
Důvěrnost	Zajištění, že informace (osobní údaje) jsou přístupné nebo sděleny pouze osobám k tomu oprávněným.
Hrozba	Je potenciální příčina bezpečnostní události nebo bezpečnostního incidentu, jejímž výsledkem může být způsobení škody při zpracování osobních údajů.
Integrita	Vyjadřuje, jak je důležité, aby informace nebyla neoprávněně změněna.
Kritičnost	Vyjadřuje množství osobních údajů zpracovávaných v rámci dané agendy, tedy celkový počet subjektů údajů, jejichž osobní údaje se v dané agendě můžou vyskytovat.
Opatření	Jakýkoliv proces, politika, zařízení, metoda nebo činnost, která má za cíl snížit riziko.
Organizace	V obecném chápání pojem označující zpravidla organizovanou formální skupinu lidí, kteří mají společné cíle a jsou vymezeni vůči okolnímu prostředí. V rámci této analýzy je pojmem organizace myšlena organizace příspěvková.

OÚ	Osobní údaj
Parciální riziko	Vzniká při působení konkrétní hrozby na konkrétní účel zpracování.
Relativní váha	Hodnota dané veličiny (rizika, nebo opatření) vztažená k maximální hodnotě dané veličiny. Pohybuje se v intervalu od 0 do 100, kde 100 je maximální hodnota veličiny. (Např.: Relativní váha jednoho konkrétního rizika vyjadřuje, kolik procent maximálního rizika toto konkrétní riziko představuje.)
Riziko	Představuje hrozbu, potenciální problém, nebezpečí vzniku škody, možnost selhání a neúspěchu, poškození, ztráty či zničení. Riziko je možnost, že určitá hrozba využije zranitelnosti, tedy slabého místa, a způsobí škodu na zpracování osobních údajů.
Sociální inženýrství	Způsob manipulace lidí za účelem provedení určité akce, nebo získání určité informace případně finančního obohacení. Termín je běžně používán ve významu podvodu nebo podvodného jednání za účelem získání utajených informací organizace, nebo přístupu do informačního systému.
Souhrnné riziko	Součet všech parciálních rizik generovaných jednou hrozbou vůči všem účelům zpracování.
Subjekt údajů	Fyzická osoba, jejíž osobní údaje jsou zpracovávány.
Účel zpracování	Pro tento dokument jím rozumíme účel zpracování osobních údajů.
Zranitelnost	Slabé místo aktiva nebo opatření, které může být využito jednou, nebo více hrozbami.

2. HODNOCENÍ ÚČELŮ ZPRACOVÁNÍ

2.1. ÚVOD

Metodika primárně vychází z analýzy požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), účinného dnem 1. 1. 2015 a jeho prováděcích předpisů. Zejména pak Vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), účinné také dnem 1. 1. 2015. Tato metodika byla současně přizpůsobena požadavkům 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).

Základním vstupem pro provedení analýzy rizik je identifikace jednotlivých účelů zpracování osobních údajů. Ty jsou též použity jako primární vstup do procesu analýzy rizik.

2.2. IDENTIFIKACE ÚČELŮ ZPRACOVÁNÍ

Identifikace účelů zpracování spočívá v provedení obecného rozboru činností organizace, ve kterých v rámci svých jednotlivých agend dochází ke zpracování osobních údajů, a to jak v listinné, tak i elektronické formě. Garantem (vlastníkem) účelů zpracování (procesu) je pověřený odpovědný pracovník stanovující jednotlivé procesy účelu zpracování.

2.3. HODNOCENÍ ÚČELŮ ZPRACOVÁNÍ

Účely zpracování se hodnotí podle požadavků na „**důvěrnost**“, „**integritu**“, „**dostupnost a odolnost**“ a „**kritičnost**“ daného účelu zpracování.

DŮVĚRNOST

- Zajištění, že informace (data) jsou přístupné nebo sděleny pouze osobám k tomu oprávněným,
- porušení důvěrnosti znamená nežádoucí zpřístupnění informace (dat) neoprávněné osobě; může mít negativní vliv na subjekty údajů,
- informace obsažené v jednotlivých procesech obsahují různě citlivé osobní údaje a jejich kompromitace by mohla způsobit jiné dopady na subjekty údajů a následně na organizaci, která je správcem kompromitovaných osobních údajů.

INTEGRITA

- Zajištění správnosti a úplnosti informací (dat),
- pokud dojde k nežádoucí změně dat, a to ať už úmyslně, náhodou, nebo technickým selháním, nemusí být tato nežádoucí změna vůbec odhalena a může uplynout dlouhá doba, než bude zaregistrována. Čím později se na tento bezpečnostní incident přijde, tím závažnější může být jeho dopad na subjekty údajů.

DOSTUPNOST A ODOLNOST

- Zajištění, že osobní údaje jsou pro oprávněné uživatele přístupné v okamžiku jejich potřeby. Jedná se o důsledek zničení dat, úmyslné blokování či zahlcení technických prostředků, prostřednictvím kterých mají být tyto osobní údaje přístupné v požadovaném čase.

KRITIČNOST

- Vyjadřuje množství osobních údajů zpracovávaných v rámci daného procesu,
- vyjadřuje míru důležitosti účelu zpracování pro organizaci.

Jednotlivé stupnice pro hodnocení požadavků jsou uvedeny v přílohách.

Vzor přehledu účelů zpracování osobních údajů včetně hodnocení je uveden v Tabulce č. 1

TABULKA 1: PŘEHLED ÚČELŮ ZPRACOVÁNÍ

Název organizace	Způsob zpracování	Důvěrnost	Integrita	Dostupnost a odolnost	Kritičnost	Hodnota účelu zpracování
Účely zpracování						
Zápis	Listinná podoba	4	3	1	1	**25**
Zajištění předškolního vzdělávání	Listinná podoba (Word)	3	2	1	1	**19**
Poskytování poradenských služeb SPC	Listinná + PPP4	6	4	1	4	**41**
Zajištění pobytu v dětském domově	Listinná + Evix	6	4	2	1	**36**
Personalistika	Listinná + Perm3	4	3	1	2	**27**

Pro stanovení **Hodnoty účelu zpracování** se využívá vzorec:

Pro stanovení **Hodnoty účelu zpracování** se využívá vzorec:

$$\boldsymbol{Huz = 4 * D + 2 * I + DO + 2 * K}$$

Kde:

Huz = Hodnota účelu zpracování
D = Důvěrnost
I = Integrita
DO = Dostupnost a odolnost
K = Kritičnost

2.4. SESKUPENÍ ÚČELŮ ZPRACOVÁNÍ

Pro účely analýzy rizik je nutné seskupit veliké množství identifikovaných účelů zpracování v rámci jednotlivých odborů a oddělení. Seskupení jednotlivých identifikovaných účelů zpracování je provedeno **na základě stejných hodnot důvěrnosti** v rámci jednotlivých účelů zpracování. Pokud některé účely zpracování mají stejnou hodnotu důvěrnosti, tak se seskupí do jediného účelu zpracování a dále jsou hodnoty integrity, kritičnosti, dostupnosti a odolnosti těchto účelů zprůměrovány. Výsledné hodnoty jsou zaokrouhleny na celá čísla.

3. HODNOCENÍ RIZIK

3.1. STANOVENÍ PŮSOBENÍ HROZEB VŮČI ORGANIZACI

Na organizaci jako celek působí mnoho druhů hrozeb. Hrozby mohou způsobit nežádoucí incident, který může mít za následek narušení procesů účelů zpracování a tím i poškodit organizaci. K tomuto poškození může dojít např. v důsledku kybernetického útoku na informace organizace. Výsledkem takového útoku může být např. nedovolené prozrazení, modifikace, nedostupnost nebo ztráta osobních údajů. Hrozby mohou vzniknout z náhodných, neúmyslných nebo úmyslných příčin či událostí.

Aby došlo k narušení účelů zpracování osobních údajů, využívá hrozba jedné nebo i více zranitelností systémů, aplikací nebo služeb využívaných organizací. Hrozby mohou působit z vnějšku nebo vnitřního prostředí organizace. Hrozba a zranitelnosti musí na aktivum působit současně, aby způsobily incident, který by mohl narušit průběh účelu zpracování osobních údajů.

Přehled hrozeb a předpokládané scénáře jejich dopadů jsou uvedeny v následující kapitole v tabulce č. 2 „Přehled hrozeb“.

[redacted]PŘEHLED HROZEB

TABULKA 2: PŘEHLED HROZEB

Oblast hrozeb	Hrozba	Popis hrozby
Fyzická bezpečnost	Škoda způsobená průnikem neoprávněné osoby	Hrozba spočívající v průniku neoprávněné osoby do objektu, případně do blízkosti hodnoceného účelu zpracování s cílem poškodit, zničit, případně odcizit tato data. Kanceláře, vstupy do budov, serverovny a jiná místa, kde jsou uchovávány osobní informace.
Technická hrozba	Užívání software v rozporu s licenčními podmínkami	Používání nelegálního softwaru nebo softwaru s neověřenými zdroji, které může vést k zavlečení škodlivého kódu do informačního systému. Především nastavení uživatelských práv v rámci OS a případné povolení/zakázání instalace programů.
Technická hrozba	Kybernetický útok z vnější nebo vnitřní komunikační sítě	Kybernetické útoky vedené z vnější komunikační sítě např. proti dostupnosti systému (DoS/DDoS), nebo pokus o průnik do informačního systému z vnějšího prostředí. Kybernetický útok vedený z vnitřní sítě, např. logická bomba, zadní vrátka, trojský kůň apod., útoky z vnitřní sítě jsou vedeny většinou samotnými zaměstnanci organizace. Míru rizika ovlivňují fakta,

Oblast hrozeb	Hrozba	Popis hrozby
		jako jsou firewally, využití demilitarizovaných zón, segmentace sítě, nastavení proxy serverů apod.
Technická hrozba	Škodlivý kód (např. viry, spyware, trojské koně)	Zavlečení škodlivého kódu do informačního systému. Hrozba spočívá především v absenci či nesprávném nastavení antivirových programů, možnosti použití neautorizovaných přenosných zařízení apod.
Technická hrozba	Nedostatky při poskytování služeb informačního systému	Degradace služeb poskytovaných IS, prodloužená doba reakce IS, omezení funkčnosti a dostupnosti všech modulů informačního systému, výpadek energií. Hrozba může být naplněna nedostatečně nastavenými procesy kontrolujícími správnou funkci systémů včetně predikce stavu možného zatížení do budoucna (zálohy, vytížení sítě apod.) nebo jejich údržby a jejich neschopnost tyto nedostatky včas odstraňovat.
Technická hrozba	Nedostatečné monitorování činnosti administrátorů	Nedostatečně nastavené monitorování a vedení záznamů o činnosti administrátorů, které vede k nízkému prosazení odpovědnosti za vykonávanou činnost a k nedostatečným důkazům při řešení bezpečnostních incidentů.
Organizační bezpečnost	Nevhodně nastavená přístupová oprávnění	Neoprávněné přístupy k OÚ/nesprávně nastavené exporty OÚ/neoprávněné přístupy k OÚ, které se netýkají náplně práce zaměstnance či externího subjektu.
Organizační bezpečnost	Nedostatečné bezpečnostní povědomí	Nedostatečná bezpečnostní školení zaměstnanců podílejících se na zpracování OÚ/ neznalost principů sociálního inženýrství/neznalost bezpečnostních postupů při vzniku nežádoucích událostí.
Organizační bezpečnost	Nedostatečné organizační zabezpečení	Nedostatek zaměstnanců s potřebnou odbornou znalostí zajišťující některé aspekty bezpečnosti a zpracování OÚ (fyzická bezpečnost, administrátoři IS, personální zaměstnanci apod.).
Procesní hrozby	Nedostatečné postupy při identifikování a ošetřování bezpečnostních	Nedostatečně definované postupy, nebo nedostatečně informovaní zaměstnanci o postupech, kterými mají reagovat na bezpečnostní události a bezpečnostní incidenty. Špatně definované odpovědnosti, nebo postupy činností při zvládání bezpečnostních událostí a incidentů.

Oblast hrozeb	Hrozba	Popis hrozby
	událostí a incidentů	
Procesní hrozby	Nedostatečné monitorování činnosti uživatelů (kontrolní činnost)	Nedostatečně nastavené monitorování a vedení záznamů o činnosti uživatelů, které vede k nízkému prosazení odpovědnosti za vykonávanou činnost a k nedostatečným důkazům při řešení bezpečnostních incidentů. Kontrolní činnosti.
Procesní hrozby	Zpracování OÚ bez řádného právního titulu	Hrozba spočívá ve zpracování OÚ bez souhlasu subjektu údajů tím, že neexistuje právní nárok na zpracování nebo není možné doložit souhlas subjektu údajů se zpracováním OÚ v daném rozsahu nebo neupozornění na sledování prostoru průmyslovými kamerami či jinými technickými zařízeními. Hrozba se také týká využití OÚ k jiným agendám, než ke kterým byl dán souhlas včetně automatizovaného profilování.
Procesní hrozby	Krácení práv subjektů údajů	Nedodržení požadavků subjektů údajů daných články 15 až 22 GDPR. Hrozba spočívá v neexistenci nebo nedokonalosti procesů při jednání se subjekty údajů. Může se tak stát, že dané OÚ nebudou např. odstraněny nebo nebude dodržena doba nutná na odpověď subjektu údajů.
Procesní hrozby	Nejednoznačné vymezení pravomocí zaměstnanců podílející se na zpracování OÚ	Neexistence či nejednoznačnost vymezení pravomocí a odpovědností souvisejících se zpracováním OÚ. Hrozba může vést např. k dvojímu zpracování OÚ, nejednoznačnosti povinností při reakci na požadavky subjektů údajů či neznalost problematiky související se zpracováním OÚ.
Procesní hrozby	Nadbytečné zpracování OÚ v rámci existujících agend	Zpracování OÚ v rozsahu větším než je potřebné pro danou agendu. Jedná se o větší množství typů OÚ, které se v rámci dané agendy zpracovávají, avšak nejsou všechny pro danou agendu oprávněně potřebné.
Procesní hrozby	Uchování OÚ po ukončení doby uložení	Uchování OÚ i po uplynutí doby, po kterou mají být osobní údaje uloženy pro danou agendu. Doba uchování je daná zákony, skartačními řády a dobou po kterou jsou osobní údaje pro danou agendu potřeba.

Oblast hrozeb	Hrozba	Popis hrozby
Administrativní hrozba	Náhodné nebo protiprávní zničení OÚ	Hrozba spočívá ve zničení údajů, které může být způsobeno nevhodným uložením dokumentů obsahujících osobní údaje. Dále také neexistencí pravidel nakládání s těmito dokumenty mimo a v prostorách organizace. Hrozba také může být naplněna např. nedodržením nebo neznalostí postupů práce s elektronickými daty obsahujícími osobní údaje. Jakékoliv úmyslné zničení jak elektronických, tak i listinných dat obsahujících osobní údaje.
Administrativní hrozba	Ztráta OÚ	Nedodržení pravidel pro přenášení informací, obsahujících osobní údaje, mimo prostory organizace.
Administrativní hrozba	Pozměňování OÚ	Hrozba může být způsobena nedbalostí spočívající v nedostatečných znalostech zaměstnance nebo nevhodně nastaveným oprávněním k datům. Hrozba může být způsobena úmyslným prolomením nastavených oprávnění nebo čistým úmyslem změnit data a poškodit organizaci.
Administrativní hrozba	Neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů	Hrozba může být naplněna jak z nedbalosti, tak i úmyslně. Neověřením identity osoby, která přebírá informace obsahující osobní údaje. Zpřístupněním osobních údajů osobám, které k tomu nejsou oprávněny.

3.2. STANOVENÍ ÚROVNĚ HROZEB

V momentě, kdy organizace určí a ohodnotí jednotlivé účely zpracování, je nutné k jednotlivým účelům zpracování stanovit úrovně jednotlivých hrozeb.

Při stanovení úrovně hrozeb je nutné brát v potaz dva zásadní parametry, které plně ovlivňují nebezpečnost dané hrozby, a tedy výsledné riziko. Jedním parametrem je frekvence hrozeb a druhým je zranitelnost daného účelu zpracování.

3.2.1 STANOVENÍ FREKVENCE PŮSOBENÍ HROZEB NA ÚČELY ZPRACOVÁNÍ

Frekvence hrozeb v závislosti na zranitelnostech ovlivňuje míru rizika působícího na účel zpracování a také jeho dopady. Posouzení frekvence hrozeb musí vzít v úvahu následující:

Úmyslné hrozby. Pravděpodobnost úmyslné hrozby závisí na motivaci, znalostech, kapacitách a zdrojích, které mají k dispozici možní útočníci, a na přitažlivosti dat pro útočníky.

Náhodné hrozby. Pravděpodobnost náhodných hrozeb může být odhadnuta za pomoci statistiky a zkušeností. Pravděpodobnost těchto hrozeb může také mít vztah k tomu, jak je organizace blízko zdrojům nebezpečí, jako jsou velké silniční nebo železniční trasy, závody pracující s nebezpečnými materiály, jako jsou chemické materiály nebo ropa.

Minulé incidenty. Tj. incidenty, ke kterým již došlo a které ukazují problémy v současném ochranném uspořádání.

Nový vývoj a trendy. Zahrnuje zprávy, novinky a trendy získané z dostupných zdrojů, od specialistů nebo organizací, pomáhajících posuzovat aktuální situaci hrozeb.

Parametry pro stanovení frekvence hrozeb jsou uvedeny v následující tabulce.

TABULKA 3: STUPNICE PRO HODNOCENÍ FREKVENCE HROZEB

Stupnice pro hodnocení frekvence hrozeb		
Úroveň	**Číselné hodnocení**	**Popis hrozby**
Nízká	1	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	2	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	3	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	4	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

3.2.2 STANOVENÍ DOPADŮ HROZEB NA ÚČEL ZPRACOVÁNÍ

Pro hodnocení hrozeb je důležité stanovit předpokládaný dopad na účel zpracování při vzájemné interakci hrozby, zranitelnosti a aktiva. Současně je určena míra možného dopadu hrozby v případě její realizace na dostupnost, důvěrnost a integritu účelu zpracování.

Pro stanovení dopadů hrozby na účel zpracování jsou použity následující hodnoty dopadů uvedené v následující tabulce.

TABULKA 4: STUPNICE PRO HODNOCENÍ DOPADŮ

Dopad		
Úroveň	**Číselné hodnocení**	**Popis**
Žádný	**0**	Dopad je žádný, pokud hrozba může ohrozit již zveřejněné informace. **Důvěrnost 1**
Nízký	1	Dopad je nízký pokud hrozba může ohrozit informace **Důvěrnosti 2. Nutné zvážit hlášení ÚOOÚ**
Střední	2	Dopad je střední pokud hrozba může ohrozit informace **Důvěrnosti 3. Nutné hlášení ÚOOÚ + zvážení hlášení subjektům údajů** (zejména dle množství kompromitovaných údajů)
Vysoká	3	Dopad je vysoký pokud hrozba může ohrozit informace **Důvěrnosti 4 nebo 5. Nutné hlášení ÚOOÚ + zvážení hlášení subjektům údajů** (např. množství kompromitovaných údajů nebo vysoké riziko pro práva a svobody fyzických osob)
Kritická	4	Dopad je kritický pokud hrozba může ohrozit informace **Důvěrnosti 6. Nutné hlášení ÚOOÚ + Subjektům údajů**

3.2.3 STANOVENÍ ZRANITELNOSTÍ ÚČELŮ ZPRACOVÁNÍ

Zranitelnosti jsou bezpečnostně slabá místa spojená s jednotlivými účely zpracování organizace. Tato slabá místa mohou být využita jednou nebo více hrozbami, což zapříčiní nežádoucí incident, který může vyústit ve ztrátu, zničení nebo poškození informací daného účelů zpracování a narušení činnosti organizace. Zranitelnost sama o sobě nezpůsobuje poškození, je to pouze okolnost nebo soubor okolností, které mohou umožnit hrozbě, aby se realizovala a zapříčinila poškození informací.

Identifikace zranitelnosti musí zjistit slabá místa, která se vztahují k účelům zpracování a hodnocené hrozbě, a to zejména s ohledem na způsoby zpracování, uchování dokumentů, řízení přístupů k dokumentům nebo informačním systémům nebo znalosti zaměstnanců zpracovávající informace obsahující osobní údaje.

TABULKA 5: STUPNICE PRO HODNOCENÍ ZRANITELNOSTÍ

Stupnice pro hodnocení zranitelností		
Úroveň	**Číselné hodnocení**	**Popis**
Nízká	1	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření (procesy), která jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	2	Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	3	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	4	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

3.2.4 ZAZNAMENÁNÍ HODNOT IDENTIFIKOVANÝCH HROZEB

Frekvence výskytu hrozby, dopad hrozeb a zranitelnost účelů zpracování vůči hrozbám, představují, společně s ohodnocením účelů zpracování, vstupní informace, potřebné pro výpočty analýzy rizik.

Vstupem pro analytický nástroj, který provádí výpočty, je podkladová tabulka dat, která popisuje hodnocení frekvence, dopadu a zranitelnosti ve vztahu k účelům zpracování.

TABULKA 6: HODNOTY IDENTIFIKOVANÝCH HROZEB

Skupina aktiv **Hrozby**	Zápis			Zajištění předškolní vzděl		
Důvěrnost	4			6		
Integrita	3			4		
Dostupnost	1			1		
Kritičnost	1			1		
	FF	**DD**	**ZZ**	**FF**	**DD**	
Škoda způsobená průnikem neoprávněné osoby	11	33	22	11	44	
Užívání software v rozporu s licenčními podmínkami	11	33	22	11	44	
Kybernetický útok z vnější nebo vnitřní komunikační sítě	11	33	33	11	44	
Škodlivý kód (např. viry, spyware, trojské koně)	22	33	33	12	44	
Nedostatky při poskytování služeb informačního systému	22	33	22	22	44	

F – Frekvence

D – Dopad

Z – Zranitelnost

3.3. ANALÝZA RIZIK

3.3.1 VÝPOČET RIZIKA

Míra rizika je určena jako součin číselných parametrů hodnoty účelu zpracování, četnosti hrozby, dopadu hrozby, koeficientu účinnosti stávajících opatření. Míra rizika je kalkulována pro každou kombinaci účel zpracování / hrozba.

Kalkulace probíhá dle vzorce:

$$R = (V * F * D * Z) / 10$$

kde:

R = Výsledné parciální riziko,

V = hodnota účelu zpracování

F = frekvence výskytu hrozby,

D = dopad hrozby,

Z = zranitelnost účelu zpracování vůči hodnocené hrozbě/neexistence protiopatření.

3.3.2 PARCIÁLNÍ RIZIKA

Při interakci konkrétní hrozby a konkrétního účelu zpracování vzniká tzv. „parciální riziko“. Tento princip je znázorněn v následující tabulce, kde je znázorněn příklad působení hrozeb vůči účelům zpracování.

Každý sloupeček na tomto obrázku vyjadřuje jednotlivé parciální riziko, které jedna hrozba způsobuje svým působením na jeden účel zpracování.

TABULKA 7: ZNÁZORNĚNÍ PARCIÁLNÍCH RIZIK

P.č.	Hrozba / Zranitelnost	Zápis	Zajištění předškolní vzdělávání	Poskytování poradenských služeb SPC	Zajištění pobytu v DD	Personalistika	Jídelna	Účetní - bez OÚ
1	**Škoda způsobená průnikem neoprávněné osoby**	15	8	32,8	28,8	16,2	15,6	8,8
2	**Užívání software v rozporu s licenčními podmínkami**	15	8	32,8	43,2	16,2	15,6	8,8
3	**Kybernetický útok z vnější nebo vnitřní komunikační sítě**	22,5	2	32,8	43,2	24,3	23,4	13,2
4	**Škodlivý kód (např. viry, spyware, trojské koně)**	45	4	65,6	86,4	48,6	46,8	26,4
5	**Nedostatky při poskytování služeb informačního systému**	30	6	65,6	57,6	32,4	31,2	17,6
6	**Nedostatečné monitorování činnosti administrátorů**	15	8	32,8	28,8	16,2	15,6	8,8

7	**Nevhodně nastavená přístupová oprávnění**	3 0	6	1 31,2	8 6,4	4 8,6	4 6,8	2 6,4
8	**Nedostatečné bezpečnostní povědomí**	1 5	8	9 8,4	2 8,8	1 6,2	1 5,6	1 3,2
9	**Nedostatečné organizační zabezpečení**	4 5	4	6 5,6	8 6,4	4 8,6	4 6,8	2 6,4
10	**Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů**	4 5	4	6 5,6	8 6,4	4 8,6	4 6,8	2 6,4

3.3.3 SOUHRNNÉ RIZIKO

Vzhledem k faktu, že jedna hrozba může působit na více účelů zpracování, dává obraz o nebezpečnosti hrozby teprve součet všech parciálních rizik generovaných touto hrozbou tzv. „souhrnné riziko“.

Souhrnná rizika poskytují informaci o míře nebezpečnosti hrozeb. Protože riziko je bezrozměrná veličina, nejvíce informací poskytne umístění postavení jednotlivých rizik v porovnání s ostatními riziky. Proto se používá tzv. relativní váha souhrnného rizika. Relativní váha souhrnného rizika představuje míru nebezpečnosti hrozby na stupnici od 1 do 100, kde hodnota 100 představuje hodnotu největšího identifikovaného parciálního rizika.

Hrozba, která je v seznamu nejvýše postavená, je tak nejvíce nebezpečná pro organizaci a níže postavené tak mají i nižší potencionální dopad, který je vyjádřen jejich relativní vahou vůči největší hrozbě.

TABULKA 8: PŘÍKLAD ZOBRAZENÍ SOUHRNNÉHO RIZIKA

P.č.	Hrozba / Zranitelnost	Souhrnná rizika	Relativní váha souhrnných rizik
2	Užívání software v rozporu s licenčními podmínkami	187	100
7	Nevhodně nastavená přístupová oprávnění	187	100
8	Nedostatečné bezpečnostní povědomí	187	100
10	Nedostatečné postupy při identifikování a ošetřování bezpečnostních událostí a incidentů	187	100
20	Neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů	187	100
6	Nedostatečné monitorování činnosti administrátorů	125	67
9	Nedostatečné organizační zabezpečení	125	67
11	Nedostatečné monitorování činnosti uživatelů (kontrolní činnost)	125	67
17	ztráta OÚ	125	67
19	Náhodné nebo protiprávní zničení OÚ	125	67
13	Krácení práv subjektů údajů	94	50
1	Škoda způsobená průnikem neoprávněné osoby	89	47
3	Kybernetický útok z vnější nebo vnitřní komunikační sítě	62	33
4	Škodlivý kód (např. viry, spyware, trojské koně)	62	33
5	Nedostatky při poskytování služeb informačního systému	62	33
12	Zpracování OÚ bez řádného právního titulu	62	33
14	Nejednoznačné vymezení pravomocí zaměstnanců podílející se na zpracování OÚ	62	33
15	Nadbytečné zpracování OÚ v rámci existujících agend	62	33
16	Uchování OÚ po ukončení doby uložení	62	33
18	Pozměňování OÚ	62	33

Hrozby jsou následně setříděny dle jejich celkové úrovně rizika od nejvyšší hodnoty po nejnižší.

Hrozba, která je v následující tabulce nejvýše postavená, je tak nejvíce nebezpečná pro organizaci a níže postavené tak mají zároveň nižší potencionální dopad, který je vyjádřen jejich relativní vahou vůči největší hrozbě.

Hrozbám s nejvyšší úrovní rizika je nutné se věnovat přednostně. V tomto vzorovém případě by se jednalo o minimálně první tři hrozby s ID 7, 5 a 12. Zbylé hrozby jsou ošetřovány následně alespoň do přibližné úrovně 50 % celkového rizika. I k těmto hrozbám se vypracují konkrétní postupy do Plánu zvládání rizik.

4. ZVLÁDÁNÍ RIZIK

4.1. VÝPOČET ÚČINNOSTI OPATŘENÍ

Po stanovení úrovně akceptovatelného rizika analytický nástroj provede výpočet vah opatření ke snížení rizika (analytický nástroj pracuje s opatřeními uvedenými v Příloze tohoto dokumentu „Popis opatření“). Váhy opatření pro snížení rizika jsou vypočítány na základě výběru vhodných opatření ke snížení jednotlivých parciálních rizik a vypočítá se dílčí váha každého opatření vůči danému parciálnímu riziku (viz tabulka č. 9 sloupec „Váhy opatření“). Jednotlivá opatření jsou poté seřazena sestupně podle váhy. Pro zlepšení přehledu o účinnosti, jsou tyto váhy uvedeny i v relativních hodnotách v intervalu od 1 do 100 obdobně jako u relativních souhrnných rizik. V tabulce č. 6 je uveden příklad výsledku výpočtu vah opatření.

TABULKA 9: VÁHY OPATŘENÍ

ID	Název opatření	Váhy opatření	Relevantní váhy opatření
16	**Řízení přístupových oprávnění**	25519	100
6	**Řízení aktiv**	22589	89
8	**Řízení provozu a komunikací**	20757	81
4	**Organizační bezpečnost - stanovení rolí a jejich odpovědností**	20513	80
21	**Aplikační bezpečnost**	19902	78
1	**Zavedení systému řízení bezpečnosti informací**	19536	77
3	**Bezpečnostní politika**	19536	77
22	**Kryptografické prostředky**	19292	76
19	**Detekce bezpečnostních událostí**	16361	64
20	**Sběr a vyhodnocení bezpečnostních událostí**	16361	64
18	**Zaznamenávání činností informačních systémů, jejich uživatelů a administrátorů**	16484	65
12	**Kontrola a audit**	12698	50
5	**Bezpečnostní požadavky pro zpracovatele**	13309	52
7	**Bezpečnost lidských zdrojů**	13065	51
9	**Řízení přístupu a bezpečné chování uživatelů**	10256	40
17	**Ochranu před škodlivým kódem**	11844	46
10	**Zvládání bezpečnostních událostí a incidentů**	10745	42
11	**Řízení kontinuity činností**	10745	42
14	**Ochrana integrity sítí**	9158	36
2	**Řízení rizik**	10379	41
15	**Ověřování identity uživatelů**	9035	35
13	**Fyzická bezpečnost**	6105	24
23	**Zajišťování úrovně dostupnosti**	4884	19

4.2. STANOVENÍ PRIORIT REALIZACE OPATŘENÍ

Po vypočtení analytickým nástrojem účinnost jednotlivých opatření se stanovení priority implementace jednotlivých opatření bezpečnosti takovým způsobem, že vypočtené celkové váhy jednotlivých opatření (v tabulce 9 – označeno jako „Váhy opatření“) setřídí od největší po nejmenší. Takto seřazená opatření budou mít za výsledek snížení rizik v pořadí, které reaguje na aktuální stav bezpečnosti organizace.

4.3. STANOVENÍ ÚROVNĚ AKCEPTOVATELNÉHO RIZIKA

Po seřazení všech rizik dle jejich rizikovosti pro organizaci od nejvyšších po nejnižší se mohou vyřadit z hodnocení ta rizika, která dosahují jen velmi nízkých hodnot, a tudíž na bezpečnost organizace mají jen zanedbatelný vliv. Toto rozdělení se provede stanovením akceptovatelné úrovně rizika, tj. úrovně, pod kterou rizika už mají jen zanedbatelný vliv na účely zpracování organizace.

4.4. ZVLÁDÁNÍ RIZIK

Výsledná opatření jsou vybírána a následně implementována na základě nejlepší praxe z oblasti řízení rizik a vždy jsou upravována dle cílového prostředí dané organizace. Opatření mohou být technického nebo organizačního charakteru a jejich bližší popis možnosti jejich zavedení jsou uvedeny v příloze „Popis opatření“, přičemž pořadí, ve kterém budou jednotlivá opatření implementována je uvedeno v tabulce „Váhy opatření“, ve sloupci „Váhy opatření“, kde se bude postupovat od váhy nejvyšší po nejnižší.

Osoba odpovědná za nastavení opatření bezpečnosti vypracovává konkrétní plán zvládání rizik, ve kterém jsou uvedeny jednotlivá rizika a plán jak tyto nežádoucí stavy zvládat, včetně priorit jejich řešení. Při sestavování plánu zvládání rizik se jednotlivá opatření již konkretizují na přesně definovaná pravidla, postupy, procesy atd.

Výsledný plán zvládání rizik je schvalován vedením organizace.

5. PŘÍLOHY

5.1. STUPNICE HODNOCENÍ DŮVĚRNOSTI, INTEGRITY, DOSTUPNOSTI A ODOLNOSTI A KRITIČNOSTI

5.1.1 STUPNICE PRO HODNOCENÍ DŮVĚRNOSTI

Důvěrnost	
Úroveň	**Popis**
1	Běžné veřejné údaje
2	Interní údaje (dostupné pro všechny zaměstnance). Např. Jméno, ID zaměstnance, služební email.
3	Běžné OÚ →Jméno, příjmení, e-mail, telefon, bydliště (odpovídá datům předávaným e-shopům)
4	Stejné jako hodnota důvěrnosti 3. Navíc pracovně právní agenda a jakékoliv další osobní informace, které nejsou citlivé z hlediska zákona. (např. výše platu, číslo účtu, rodné číslo, atd.)
5	Citlivé OÚ dle zákona → Členství v odborech, politické názory, sociální postavení, náboženství
6	Citlivé OÚ dle zákona → Zdravotní stav, biometrické (genetické) údaje, sexuální orientace, etnický původ

5.1.2 STUPNICE PRO HODNOCENÍ INTEGRITY

Integrita	
Úroveň	**Popis**
1	Narušení integrity účelu zpracování neohrožuje oprávněné zájmy správce údajů z důvodu požadavku na d**ůvěrnost je určen na hodnotu 1.**
2	Narušení integrity účelu zpracování může vést k poškození oprávněných zájmů správce údajů. Požadavek na **důvěrnost je určen na hodnoty 2 a 3**
3	Narušení integrity účelu zpracování vede k poškození oprávněných zájmů správce údajů. Požadavek na **důvěrnost je určen na hodnoty 4 a 5**
4	Narušení integrity účelu zpracování vede k poškození oprávněných zájmů správce údajů s vážnými dopady pro správce údajů. Požadavek na **důvěrnost je určen na hodnotu 6.**

5.1.3 STUPNICE PRO HODNOCENÍ DOSTUPNOSTI

Dostupnost a odolnost	
Úroveň	**Popis**
1	Narušení dostupnosti informací v rámci daného účelu zpracování by nemělo překročit dobu jednoho **měsíce.**
2	Narušení dostupnosti informací v rámci daného účelu zpracování by nemělo překročit dobu jednoho **týdne.**
3	Narušení dostupnosti informací v rámci daného účelu zpracování by nemělo překročit dobu **pracovního dne.**
4	Narušení dostupnosti informací v rámci daného účelu zpracování by nemělo překročit dobu **několika hodin.**
5	Narušení dostupnosti informací v rámci daného účelu zpracování není přípustné a **i krátkodobá nedostupnost** vede k vážnému ohrožení zájmů správce.

5.1.4 STUPNICE PRO HODNOCENÍ KRITIČNOSTI

Kritičnost	
Úroveň	**Popis**
1	Počet údajů zpracovaných v dané agendě je v rozmezí 0 - 100
2	Počet údajů zpracovaných v dané agendě je v rozmezí 101 - 500
3	Počet údajů zpracovaných v dané agendě je v rozmezí 501 - 1 000
4	Počet údajů zpracovaných v dané agendě je v rozmezí 1 001 - 5 000
5	Počet údajů zpracovaných v dané agendě je v rozmezí 5 001 - 25 000
6	Počet údajů zpracovaných v dané agendě je v rozmezí 25 001 - 100 000
7	Počet údajů zpracovaných v dané agendě je více než 100 001

5.2. POPIS OPATŘENÍ

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
Zavedení systému řízení bezpečnosti informací	Ustanovení systému řízení bezpečnosti informací spočívá v definování cílů, zdrojů a způsobů řízení bezpečnosti informací a osobních údajů. Organizace dále blíže specifikuje jednotlivé oblasti bezpečnosti organizace (Informační a kybernetická bezpečnost, Fyzická bezpečnost, Administrativní bezpečnost, Personální bezpečnost a Ochrana osobních údajů) a ustanoví role odpovědné za jednotlivé oblasti bezpečnosti. V rámci ustanovení budou definovány kontrolní procesy a mechanizmy, které v pravidelných intervalech budou vyhodnocovat účinnost jednotlivých bezpečnostních opatření a zároveň budou poskytovat informace o nastaveném systému.
Řízení rizik	Organizace zavede systém, podle kterého bude schopna identifikovat, hodnotit a řídit rizika, která jednotlivým účelům zpracování hrozí. Měla by být definována metodika analýzy rizik, která bude obsahovat postupy, jakým způsobem identifikovat jednotlivé účely zpracování a ty následně hodnotit. Metodika by dále měla obsahovat postupy identifikace rizik a jejich hodnocení a postupy jak jednotlivá rizika řídit.
Bezpečnostní politika	Organizace by měla na nejvyšší úrovni definovat „politiku bezpečnosti informací", která je schválena vedením a která stanovuje přístup organizace k řízení svých cílů bezpečnosti informací. Tyto politiky by měly být sdělovány zaměstnancům a relevantním externím stranám.
Organizační bezpečnost - stanovení rolí a jejich odpovědností	Organizace zavede řízení ochrany osobních údajů, v rámci kterého určí bezpečnostní role a jejich práva a povinnosti související s realizací OOÚ u organizace. Jsou jednoznačně definovány role, které mohou schvalovat přístupy k OÚ, mající odpovědnost za řešení bezpečnostních incidentů, role, které mohou jednat se subjekty údajů apod. Organizačním opatřením jsou zakázány jakékoliv neautorizované exporty, kopírování, tisk, stahování apod. osobních údajů a jiných citlivých dat obsažených v informačních systémech organizace. Vedou se záznamy o vypůjčených dokumentech (zaznamenává se, o jaké dokumenty se jedná, datum

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	zapůjčení a datum vracení - ten kdo si půjčuje stvrdí zápůjčku podpisem, při vrácení podepisuje ten, komu byly dokumenty navráceny). Jsou nastaveny procesy, podle kterých se budou poskytovat informace, na které mají subjekty nárok dle GDPR. Provádí se pravidelná kontrola rozsahu zpracovávaných OÚ v jednotlivých agendách (např. pracovněprávní agenda, poskytování různých služeb, …), zda všechny údaje v těchto agendách zpracovávané jsou nezbytně nutné pro vykonávání daných činností. Každý zpracovávaný rozsah OÚ musí být obhajitelný jako potřebný pro danou agendu. DPO a vedoucí pracovníci pravidelně ověřují, zda na veškeré shromažďované OÚ existuje právní titul. A to buď zákonný, nebo existuje souhlas subjektu se zpracováním OÚ. Provádí se pravidelná kontrola uchovávání osobních údajů (zamykání do skříní, uzamykání kanceláří, kontrola pravidla prázdného stolu, apod.). Směrnicí jsou definované způsoby nakládání s dokumenty obsahující osobní údaje mimo prostory organizace (např. nevynášet dokumenty, šifrovat přenosné disky atd.).
Bezpečnostní požadavky pro zpracovatele	Jsou stanovena pravidla pro zpracovatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své zpracovatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti IS, které zpracovávají OÚ. Rozsah zapojení zpracovatelů se dokumentuje písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací. Před uzavřením smlouvy je prováděno hodnocení rizik zpracování OÚ. Jsou nastavena správná SLA se zpracovateli a dodavateli.
Řízení aktiv	Jsou identifikována a evidována aktiva (systémy a prostředky), na kterých dochází ke zpracování osobních údajů. Jsou určeni jednotliví garanti těchto aktiv, kteří jsou za ně odpovědní, včetně odpovědnosti za OOÚ. Jsou stanovena pravidla pro manipulaci s OÚ, včetně pravidel pro bezpečné elektronické sdílení a fyzický přenos. Jsou stanoveny přípustné způsoby používání aktiv. Jsou zavedena pravidla ochrany odpovídající úrovni aktiv. Jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat.

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	Vede se evidence schváleného a legálně pořízeného softwaru.
Bezpečnost lidských zdrojů	Je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení. O školení jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly. Jsou prováděna pravidelná školení uživatelů zaměřená na předcházení nežádoucích situací spojených s používáním výpočetní techniky (e-maily, viry, internet a sociální sítě, apod) a jejich reakce na tyto hrozby. Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role. Je zajištěno dlouhodobé plánování v oblasti potřeby zaměstnanců a výchova specialistů z vlastních řad zaměstnanců. Je věnována pozornost zlepšení školícího aparátu se zaměřením na specializování činnosti zaměstnanců.
Řízení provozu a komunikací	Je zajištěn bezpečný provoz informačních systémů zpracovávajících OÚ. Za tímto účelem jsou stanoveny provozní pravidla a postupy, které obsahují: - Práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů. - Postupy řízení a schvalování provozních změn. - Postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech. Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh. Provádí se pravidelné testování, posuzování a hodnocení

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování OÚ. V organizačním opatření (směrnici), je uveden přísný zákaz instalovat jakýkoliv software, který není legálně organizací pořízen. Nastavení technických opatření, která zamezují uživatelům instalovat software (rozdělení rolí v rámci operačního systému nebo Active directory na uživatele a administrátory).
Řízení přístupu a bezpečné chování uživatelů	Na základě provozních a bezpečnostních potřeb (NTK) je řízen přístup k informačnímu systému zpracovávajícímu OÚ, a každému uživateli je přiřazen jednoznačný identifikátor. Jsou přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů. Je omezeno přidělování administrátorských oprávnění. Přidělování a odebírání přístupových oprávnění je prováděno v souladu se stanovenými pravidly. Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích. Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení (notebooky smartphony apod.), případně i bezpečnostní opatření spojená s využitím technických zařízení, které nejsou ve vlastnictví organizace.
Zvládání bezpečnostních událostí a incidentů	Jsou přijata nezbytná opatření, která zajistí oznamování bezpečnostních událostí u informačního systému zpracovávajícího OÚ ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních jsou vedeny záznamy. Je připraveno prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí, je prováděno jejich vyhodnocení a jsou identifikovány kybernetické bezpečnostní incidenty. Je prováděna klasifikace bezpečnostních incidentů, přijímáno opatření pro odvrácení a zmírnění dopadu bezpečnostního incidentu a je zajištěn sběr věrohodných podkladů potřebných pro analýzu bezpečnostního incidentu. Jsou prošetřeny a určeny příčiny bezpečnostního incidentu, je vyhodnocena účinnost řešení bezpečnostního incidentu a na základě vyhodnocení jsou stanovena nutná bezpečnostní

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	opatření k zamezení opakování řešeného bezpečnostního incidentu. Jsou připraveny postupy pro hlášení případů porušení zabezpečení osobních údajů dozorovému úřadu podle čl. 33 GDPR a oznamování případů porušení zabezpečení osobních údajů subjektu údajů podle čl. 34 GDPR.
Řízení kontinuity činností	Jsou stanoveny: - práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role při řízení kontinuity činností, - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému zpracovávajícího OÚ, - doby obnovení chodu, během které bude po bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému, - plány kontinuity činností informačního systému. Tyto plány jsou aktualizovány a pravidelně testovány.
Kontrola a audit	Je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému zpracovávajícímu OÚ. Jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.
Fyzická bezpečnost	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů. Jsou přijata nezbytná opatření k zamezení neoprávněného vstupu do vymezených prostor, kde jsou zpracovávány osobní údaje a umístěna technická aktiva informačního systému. Zaměstnanci mají vlastní zamykatelné skříňky, kde uchovávají listinné dokumenty obsahující osobní údaje. Klíče od těchto skříněk má jen daný odpovědný zaměstnanec (popř. kopie je umístěna v trezoru v zapečetěné obálce). Místnosti jsou vybaveny zámkem, jehož klíče mají jen oprávnění zaměstnanci. Úklid probíhá jen pod dohledem

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	zaměstnanců. Vstupy do budov jsou řízeny pomocí evidence klíčů, čipů apod. Serverovny nebo místnosti s uloženými IT prostředky jsou vybaveny detektory pohybu a v případě umístění v přízemí nebo prvním patře s okny, jsou okna opatřena mříží.
Ochrana integrity sítí	Pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou organizace, a vnitřní komunikační sítě, která je pod správou organizace, je zavedeno(a): - Řízení bezpečného přístupu mezi vnější a vnitřní sítí. - Segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí. - Použití kryptografických prostředků pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií. - Opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě. - Zařízení, která jsou oprávněná k přístupu k síti, jsou vedena v organizační doméně. - Řízení povolených zařízení na základě MAC adresy (pro externí hosty s omezenou platností povolení). Registrace je prováděna i pracovníky organizace zadáním vlastních přístupových údajů. - Oddělení frontend a backend serverů
Ověřování identity uživatelů	Jsou používány nástroje pro ověření identity uživatelů a administrátorů informačního systému. Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje: - Minimální délku hesla osm znaků. - Minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3.

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	- Maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací. - Zamezuje opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin. - Využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení ostatních požadavků na heslo.
Řízení přístupových oprávnění	Jsou jednoznačně vymezeny procesy schvalování a přidělování přístupových oprávnění. Je používáno řízení přístupových oprávnění: - pro přístup k jednotlivým aplikacím a datům - pro čtení dat, pro zápis dat a pro změnu oprávnění Je zaznamenáváno použití přístupových oprávnění. Administrátorská i uživatelská oprávnění jsou pravidelně přezkoumávána; administrátorská oprávnění jsou přezkoumávána častěji.
Ochrana před škodlivým kódem	Pro řízení rizik spojených s působením škodlivého kódu je používán nástroj pro ochranu informačního systému před škodlivým kódem (antivir), který zajistí ověření a stálou kontrolu: - Komunikace mezi vnitřní sítí a vnější sítí. - Serverů a sdílených datových úložišť. - Pracovních stanic. - Notebooků a smartphonů. Na mailservery je instalován antispyware program. Je zavedeno sledování připojených externích paměťových zařízení a jejich antivirová kontrola před samotným čtením dat z tohoto zařízení. Je prováděna pravidelná aktualizace definic a signatur nástroje pro ochranu před škodlivým kódem. Je nastavena automatizovaná instalace aktualizací (po vytvoření bodu obnovy a záloze dat).
Zaznamenávání činností informačních systémů, jejich uživatelů a administrátorů	Provádí se sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost

NÁZEV OPATŘENÍ	Popis konkrétních kroků opatření
	činnosti. Získané informace jsou chráněny před neoprávněným čtením nebo změnou. Zaznamenávají se alespoň následující aktivity: - Přihlášení a odhlášení uživatelů a administrátorů. - Činnosti provedené administrátory. - Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů. - Zahájení a ukončení činností technických aktiv informačního systému. - Automatická varovná nebo chybová hlášení technických aktiv. - Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností. Vedou se administrátorské deníky, do kterých se zaznamenávají činnosti, které se servery administrátoři provedli (např. změna nastavení, instalace SW apod.). Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času.
Detekce bezpečnostních událostí	Zapnutý firewall na vstupním routeru, který je pravidelně aktualizován.
Sběr a vyhodnocení bezpečnostních událostí	Jsou jednoznačně definované odpovědnosti za řešení bezpečnostních incidentů. O jednotlivých incidentech se vedou záznamy, včetně uvedení kořenových příčin a způsobu nápravy. Zaměstnanci jsou školeni v oblasti identifikace bezpečnostních incidentů a jejich následného zvládání.
Aplikační bezpečnost	Tvorba návodů a postupů pro práci v aplikacích obsahující osobní údaje.
Kryptografické prostředky	Na prostředky zpracovávající OÚ, jejichž kompromitace představuje největší rizika pro zájmy subjektu údajů, jsou aplikovány kryptografické prostředky, nebo se údaje pseudonymizují a pseudonymizační údaje jsou drženy separátně od zpracovávaných osobních údajů.
Zajišťování úrovně dostupnosti	Instalace UPS zařízení Nastavení automatizovaného zálohování