Smlouva o provedení auditu připravenosti na GDPR

I.

Smluvní strany

Město Břeclav

se sídlem:	nám. T. G. Masaryka 42/3, 690 81 Břeclav
jednající:	Ing. Pavel Dominik, starosta města
IČ:	00283061
DIČ:	CZ00283061

dále jen „objednatel"

BDO CA s.r.o.

se sídlem:	Marie Steyskalové 315/14, Žabovřesky, 616 00 Brno
jednající:	Ing. Miroslav Hořický, jednatel
IČ:	255 35 269
DIČ:	CZ25535269
bankovní spojení:	Československá obchodní banka a.s.
číslo účtu:	[redacted]
	zapsána v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 31321

dále jen „auditor"

II.

Základní ustanovení

1. Smluvní strany se v souladu s ustanovením § 2652 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník"), dohodly, že se rozsah a obsah vzájemných práv a povinností z této smlouvy vyplývajících bude řídit příslušnými ustanoveními citovaného zákona a tento závazkový vztah vznikne na základě § 2652 a násl. tohoto zákona.
2. Smluvní strany prohlašují, že údaje uvedené v čl. I. této smlouvy a následně uvedené ve smlouvě jsou v souladu s právní skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny údajů podle čl. I. a dalších identifikačních a kontaktních údajů uvedených ve smlouvě oznámí neprodleně písemně druhé smluvní straně. V případě změny účtu auditora je auditor povinen rovněž doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu. Při změně identifikačních údajů smluvních stran včetně změny účtu není nutné uzavírat ke smlouvě dodatek. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto úkonu oprávněny.
3. Účelem uzavření smlouvy je provedení auditu připravenosti na požadavky vyplývající z obecného nařízení o ochraně osobních údajů (GDPR).
4. Auditor prohlašuje, že je oprávněn k poskytování služeb, které jsou předmětem této smlouvy, že je schválen Komorou auditorů České republiky a je zapsán v seznamu auditorů nebo seznamu auditorských společností vedeném Komorou auditorů České republiky. Auditor prohlašuje, že je odborně způsobilý k zajištění předmětu plnění

[redacted]

podle této smlouvy. Realizační tým je sestaven tak, aby obsáhl svými zkušenostmi a svou odborností danou problematiku.

5. Tato smlouva se uzavírá na základě veřejné zakázky s názvem „GDPR analýza" a v souladu s výzvou k podání nabídek objednatele zveřejněnou na profilu objednatele dne 27. 12. 2017 a s nabídkou auditora doručenou objednateli dne 10. 1. 2018 a obsahuje podrobné obchodní podmínky pro realizaci předmětu smlouvy.

III.

Předmět smlouvy

1. Auditor se touto smlouvou zavazuje provést audit připravenosti na GDPR subjektů, které jsou uvedeny v příloze č. 1 této smlouvy.
2. Předmět auditu je specifikován v příloze č. 2 této smlouvy. Předmět auditu bude realizován v rozsahu popisu návrhu na zpracování analýzy, který byl auditorem předložen v nabídce a tvoří přílohu č. 3 této smlouvy.
3. Ověření bude provedeno na procesech zpracování osobních údajů a skutečnostech významných pro zpracování osobních údajů. Auditor použije přiměřené relevantní auditorské předpisy tak, aby byla pokryta nejvýznamnější rizika.
4. Auditorská zpráva bude obsahovat
   a) popis nedostatků a identifikovaných rizik,
   b) klasifikaci identifikovaných nedostatků a rizik,
   c) návrhy opatření (doporučení).
5. Souhrnná zpráva o výsledku auditu bude vypracována v 1 vyhotovení.

IV.

Cena

1. Cena za provedení auditu je stanovena dohodou smluvních stran a činí: 522 000 Kč bez DPH.
2. Cena zahrnuje veškeré náklady související s provedením auditu.
3. Cena bude uhrazena objednatelem na základě vystavené faktury.
4. Auditor odpovídá za to, že sazba daně z přidané hodnoty je stanovena v souladu s platnými právními předpisy. Smluvní strany se dohodly, že v případě změny ceny v důsledku změny sazby DPH není nutno ke smlouvě uzavírat dodatek.

V.

Lhůta plnění

1. Auditor se zavazuje zaslat návrh zprávy z auditu k připomínkám a následnému projednání do 30.4. 2018.
2. Auditor není v prodlení, pokud obdržel podklady k provedení vstupní analýzy později, než 15 dnů před termínem plnění podle článku V. odst. 1. písm. g). Za prodlení auditora s poskytováním služeb se nepovažuje případ, kdy k prodlení dojde v důsledku prodlení objednatele.

VI.

[redacted]

Místo plnění

1. Audity budou prováděny v místě sídla objednatele.
2. Místem pro předání zpracovaných zpráv je adresa sídla objednatele.

VII.

Povinnosti auditora

1. Auditor se zavazuje na základě provedeného auditu zpracovat a předat objednateli ve lhůtě uvedené v čl. V. této smlouvy auditorskou zprávu.
2. Auditor se zavazuje k řádnému provedení auditu při dodržení povinnosti náležité odborné péče tak, aby audit byl proveden řádně a včas.
3. Auditor se zavazuje písemně informovat objednatele o skutečnostech majících vliv na plnění smlouvy, a to neprodleně, nejpozději následující pracovní den poté, kdy příslušná skutečnost nastane nebo auditor zjistí, že by nastat mohla.
4. Auditor se zavazuje během plnění smlouvy i po ukončení smlouvy (předání předmětu plnění objednateli), zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví v souvislosti s plněním smlouvy.

VIII.

Povinnosti objednatele

1. Objednatel je povinen zajistit auditorovi přístup k podkladům, lidem a prostorám nezbytným pro provedení auditu.

IX.

Jakost a vady služeb

1. Auditor je povinen provést audit včetně vypracování auditorské zprávy v dohodnutém rozsahu a kvalitě. Auditor prohlašuje, že je ve smyslu § 22 zákona č. 93/2009 Sb., o auditorech a o změně některých zákonů (zákon o auditorech), ve znění pozdějších předpisů, pojištěn pro případ odpovědnosti za škodu, která by objednateli mohla vzniknout v souvislosti s výkonem auditorské činnosti, a bude takto pojištěn po celou dobu platnosti této smlouvy.

X.

Platební podmínky

1. Úhrada ceny za provedení auditu bude uskutečněna po předání závěrečné zprávy z auditu.
2. Lhůta splatnosti faktury bude činit 10 kalendářních dnů ode dne jejího doručení objednateli.

[redacted]

3. Podkladem pro úhradu smluvní ceny bude faktura, která bude mít náležitosti účetního dokladu dle § 11 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a daňového dokladu dle § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti stanovené § 435 občanského zákoníku (dále jen „faktura").
4. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude chybně vyúčtována cena nebo DPH nebo budou vyúčtovány práce, které auditor neprovedl, je objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně bez zaplacení k provedení opravy s vyznačením důvodu vrácení. Auditor provede opravu vystavením nové faktury. Vrátí-li objednatel vadnou fakturu auditorovi, přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží opět ode dne doručení do sídla objednatele nově vyhotovené náležitě doplněné či opravené faktury objednateli.

XI.

Závěrečná ujednání

1. Tato smlouva nabývá platnosti dnem podpisu smlouvy oběma smluvními stranami a účinnosti dnem zveřejnění smlouvy vč. jejich příloh v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smluvní strany se dohodly, že uveřejnění smlouvy dle zákona o registru smluv zajistí zasláním správci registru smluv objednatel. Smluvní strany vysloveně souhlasí se zveřejněním této smlouvy v jejím plném rozsahu, včetně příloh a dodatků v registru smluv vedeném Ministerstvem vnitra ve smyslu zákona o registru smluv.
2. Změnit nebo doplnit smlouvu mohou smluvní strany jen formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této smlouvy a podepsány oprávněnými zástupci smluvních stran, s výjimkou případů uvedených ve smlouvě.
3. Smluvní strany mohou ukončit smluvní vztah kdykoliv písemnou dohodou.
4. Obě smluvní strany jsou povinny zachovat mlčenlivost o všech skutečnostech, o kterých se dozvěděly při výkonu činnosti dle této smlouvy, a nesmí jich zneužít ke svému prospěchu nebo k prospěchu někoho jiného. Zprostit auditora této povinnosti může pouze statutární orgán objednatele.
5. Pro případ nedodržení sjednaného rozsahu prací, porušení právních předpisů nebo smlouvy ze strany auditora, se strany dohodly na omezení odpovědnosti auditora související se službou, a to do výše 150% jeho odměny podle čl. IV. odst. 1 této smlouvy.
6. Pro případ prodlení auditora s předáním zprávy auditora objednateli v dohodnutém rozsahu a kvalitě a termínu se sjednává smluvní pokuta ve výši 5.000,- Kč za každý započatý den s prodlením auditora s předáním zprávy auditora. Pro případ prodlení auditora s předáním zprávy auditora objednateli delší než 30 dnů, je objednatel oprávněn od této smlouvy odstoupit.
7. Auditor se zavazuje provádět audit podle této smlouvy minimálně v rozsahu projektového týmu uvedeného v nabídce auditora. Jednotlivý člen projektového týmu může být nahrazen osobou, které splňuje minimálně stejné požadavky jako nahrazený člen týmu. V případě porušení této povinnosti auditora, se auditor zavazuje uhradit objednateli smluvní pokutu ve výši 30.000,- Kč za každého chybějícího člena z projektového týmu předloženého v nabídce auditora, pokud nebude řádně nahrazen osobou splňující minimálně stejné požadavky, jako nahrazený člen týmu.

[redacted]

8. Smluvní strany shodně prohlašují, že si smlouvu před jejím podepsáním přečetly, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, že jejímu obsahu porozuměly a svůj projev vůle učinily vážně, určitě, srozumitelně, dobrovolně a nikoliv v tísni za nápadně nevýhodných podmínek a že se dohodly na celém jejím obsahu, což stvrzují svými podpisy.
9. Smlouva je vyhotovena ve 2 stejnopisech s platností originálu, podepsaných oprávněnými zástupci smluvních stran, přičemž každá smluvní strana obdrží 1 stejnopis.
10. Nedílnou součástí této smlouvy je:

    Příloha č. 1 - Seznam subjektů pro analýzu

    Příloha č. 2 - Předmět auditu

    Příloha č. 3 - Popis návrhu na zpracování analýzy

V Brně, dne 31. 1. 2018

[redacted]

MĚSTO BŘECLAV

V Brně, dne 24. 1. 2018

[redacted]

natel

[redacted]

PŘÍLOHA Č. 1 - OVĚŘOVANÉ SUBJEKTY

a) Subjekty analýzy:

Městský úřad Břeclav – 9 odborů + útvar interního auditu
Městská policie Břeclav

Neškolské příspěvkové organizace:

Městské muzeum a galerie Břeclav, příspěvková organizace

Městská knihovna Břeclav, příspěvková organizace
Tereza Břeclav, příspěvková organizace
Domov seniorů Břeclav, příspěvková organizace

Školské příspěvkové organizace:

Základní škola Břeclav, Komenského 2, příspěvková organizace
Mateřská škola Břeclav, U Splavu 2765, příspěvková organizace
Mateřská škola Břeclav, Osvobození 1, příspěvková organizace
Základní škola a Mateřská škola Břeclav, Kpt. Nálepky 7, příspěvková organizace
Základní škola a Mateřská škola Břeclav, Kupkova 1, příspěvková organizace
Základní škola Břeclav, Na Valtické 31 A, příspěvková organizace
Mateřská škola Břeclav, Okružní 7, příspěvková organizace
Mateřská škola Břeclav, Hřbitovní 8, příspěvková organizace
Mateřská škola Břeclav, Na Valtické 727, příspěvková organizace
Základní škola Břeclav, Slovácká 40, příspěvková organizace
Základní škola Jana Noháče Břeclav, Školní 16, příspěvková organizace
Mateřská škola Břeclav, Břetislavova 6, příspěvková organizace
Základní umělecká škola Břeclav, Křižkovského 4, příspěvková organizace

PŘÍLOHA Č. 2 - SPECIFIKACE PROVÁDĚNÍ AUDITU

b) Zaměření analýzy:

Identifikace a popis konkrétních dopadů nařízení do procesů Města Břeclavi (pohled organizační) zahrnující nejméně následující okruhy:

a. zjištění jednotlivých účelů zpracování osobních údajů
b. posouzení rozsahu a nezbytnosti zpracovávaných údajů pro jednotlivé účely
c. stanovení právního základu zpracování osobních údajů pro jednotlivé účely,
d. zpracování a uchování osobních údajů,
e. organizační opatření proti ztrátě, zničení, poškození a odcizení osobních údajů,
f. eskalační procedury a postupy pro hlášení incidentů,
g. organizační struktura a odpovědnosti za ochranu osobních údajů,
h. předávání osobních údajů,
i. další související interní a externí procesy.

Identifikace a pojmenování procesů, které osobní údaje zpracovávají – základní popis procesu, identifikace osobních údajů, které daný proces zpracovává a způsob zpracování těchto osobních údajů.

Cíle bude dosaženo prostřednictvím procesní analýzy současného stavu.

Definovány budou procesy, které je nutné upravit z hlediska souladu s legislativními podmínkami a z hlediska jejich efektivnosti, smysluplnosti a využitelnosti v rámci analyzovaného subjektu.

Analýza bude zahrnovat navržená opatření a návrh jejich implementace, vedoucí k zefektivnění řízení analyzovaného subjektu.

Předmětem veřejné zakázky je procesní analýza současného stavu procesního řízení a s tím související řešení kybernetické bezpečnosti a ochrany osobních údajů. Cílem analýzy je nezávislé posouzení současného stavu procesního řízení v rámci celého Města, definování procesů z hlediska toků informací a nakládání s osobními údaji třetích subjektů.

Předmět veřejné zakázky zahrnuje hlavně:

a) analýzu dostupné dokumentace (strategické dokumenty, směrnice a nařízení atd.)
b) zmapování všech procesů souvisejících s bezpečností IT a ochranou osobních údajů (v minimálním rozsahu účelu zpracování, právního základu, typu osobních údajů a jejich popisu, zdrojového systému, oprávněných osob, ochrany, archivační doby, možnosti námitek a přenositelnosti
c) posouzení úrovně řešení jednotlivých organizačních a technických opatření požadovaných legislativou, tj. přehled splněných resp. nesplněných požadavků;
d) analýzu oběhu osobních údajů v organizaci v papírové i elektronické podobě
e) definování slabých míst procesů z hlediska procesního řízení a bezpečnosti IT;
f) návrh postupu pro zajištění efektivního procesního řízení a souladu s požadavky legislativy
g) plán implementace navržených opatření
h) záznamy o činnostech dle čl. 30 nařízení (ke každé skupině zpracovávaných osobních údajů)
i) návrh příslušné interní směrnice/ směrnic upravujících nakládání osobních údajů ve vztahu k nařízení

Identifikace rizik - popis možných hrozeb dopadu nařízení do procesů Města Břeclav

Součásti výstupní analýzy bude i zhodnocení rizik souvisejících s nařízením, zahrnující identifikaci, analýzu, vyhodnocení a doporučení k minimalizaci rizika. Každé riziko bude stručně, ale výstižně popsáno a bude uvedena významnost rizika (jako součin dopadu a pravděpodobnosti rizika)

Použita bude standardní stupnice:

Pravděpodobnost výskytu rizika

RIZIKO - PRAVDĚPODOBNOST VÝSKYTU			
ÚROVEŇ	OZNAČENÍ	ČÍSELNÉ VYJÁDŘENÍ	INTERVAL PRAVDĚPODOBNOSTI
5	téměř jisté	od 4,1 do 5,0	vyskytne se skoro vždy
4	pravděpodobné	od 3,1 do 4,0	pravděpodobně se vyskytne
3	možné	od 2,1 do 3,0	někdy se může vyskytnout
2	nepravděpodobné	od 1,1 do 2,0	vyskytnout se může, ale nemusí také vůbec
1	téměř vyloučené	od 0,1 do 1,0	vyskytuje se pouze ve výjimečných případech

Významnost vlivu, dopadu rizika

RIZIKO - VÝZNAMNOST VLIVU / DOPAD RIZIKA

ÚROVEŇ	OZNAČENÍ DOPADU	ČÍSELNÉ VYJÁDŘENÍ	INTERVAL PRAVDĚPODOBNOSTI
5	katastrofický	od 4,1 do 5,0	ztráta majetku/ významná ztráta, či újma
4	velmi významný	od 3,1 do 4,0	významná ztráta, soudní spor, významné poškození majetku, významná újma
3	významný	od 2,1 do 3,0	vyžaduje okamžité řešení situace
2	drobný	od 1,1 do 2,0	ovlivňuje pouze dílčí aktivity
1	téměř neznatelný	od 0,1 do 1,0	neovlivňuje znatelně fungování

V souvislosti s výše uvedeným je nutné zmapovat v rámci celého Města Břeclav nakládání s informacemi a osobními údaji u všech dotčených subjektů s cílem definovat procesní postupy dotčených subjektů pro naplnění legislativních podmínek z nařízení vyplývajících.

PŘÍLOHA Č.3 - METODIKA BDO PRO OVĚŘENÍ SHODY S POŽADAVKY GDPR

BDO ve spolupráci s dalšími evropskými pobočkami BDO vyvinulo metodiku auditu shody, který identifikuje rizika a přináší praktická doporučení k ošetření těchto rizik při zajištění maximální efektivity vynaložených nákladů.

Audit shody je rozdílová analýza, která identifikuje oblasti, které nejsou v souladu s GDPR. Společně s identifikací rizik a jejich závažnosti je součástí compliance auditu (analýzy) také návrh optimalizačních opatření.

Auditoři vychází při auditu shody z ustanovení GDPR, zvláštních zákonů, které upravují zpracování osobních údajů (např. zákoník práce), judikatury a stanovisek orgánů dozoru a standardů řady ISO/IEC řady 27000 upravujících řízení bezpečnosti informací. Auditoři také přihlížejí k připravovaným právním předpisům, jako např. k návrhu zákona o zpracování osobních údajů.

Analýza zahrnuje:

a) **identifikaci a popis konkrétních dopadů do procesů města Břeclav (pohled organizační) zahrnující nejméně následující okruhy:**

- popis kategorií zpracovávaných osobních údajů,
- popis zjištěných účelů zpracování osobních údajů,
- posouzení rozsahu a nezbytnosti zpracovávaných osobních údajů pro jednotlivé účely,
- posouzení právního základu zpracování osobních údajů pro jednotlivé účely,
- posouzení dalších právních aspektů zpracování a uchování osobních údajů,
- prověření organizačních opatření proti ztrátě, zničení, poškození a odcizení osobních údajů,
- posouzení eskalační procedury a postupů pro hlášení incidentů,
- posouzení adekvátnosti organizační struktury a nastavení odpovědnosti za ochranu osobních údajů,
- prověření systému předávání osobních údajů,
- identifikaci rizik souvisejících s ochranou osobních údajů, včetně klasifikace jejich závažnosti.
- a prověření další souvisejících interních a externích procesů a aspektů zpracování osobních údajů,

b) **identifikaci a pojmenování procesů, které osobní údaje zpracovávají, a to provedením procesní analýzy zahrnující zejména:**

- analýzu dostupné dokumentace (strategické dokumenty, směrnice a nařízení atd.),
- zmapování všech procesů souvisejících s bezpečnostní IT a ochranou osobních údajů (účel zpracování, právní základ, typ osobních údajů a jejich popis, zdrojový systém, oprávněné osoby, ochrana, archivační doba, možnost námitek a přenositelnosti),
- posouzení úrovně řešení jednotlivých organizačních a technických opatření požadovaných legislativou, tj. přehled splněných resp. nesplněných požadavků,

- analýzu oběhu osobních údajů v organizaci v papírové i elektronické podobě,
- definování slabých míst procesů z hlediska procesního řízení a bezpečnosti IT,
- návrh postupu pro zajištění efektivního procesního řízení a bezpečnosti IT,
- plán implementace navržených opatření,
- záznamy o činnostech dle čl. 30 GDPR (ke každé skupině zpracovávaných osobních údajů),
- návrh příslušné interní směrnice/směrnic upravujících nákladní s osobními údaji ve vztahu k GDPR,

c) identifikace rizik - popis možných hrozeb dopadu GDPR do procesů města Břeclav, zahrnující identifikaci, analýzu a vyhodnocení a doporučení k minimalizaci rizik.

1. ZAMĚŘENÍ ANALÝZY

1.1 Dimenze analýzy

Auditoři prověří plnění následujících požadavků požadovaných při zpracování osobních údajů:

- dodržování pravidel právních předpisů pro zpracování osobních údajů, včetně základních zásad zpracování osobních údajů,
- vedení dokumentace systému řízení osobních údajů,
- nastavení a fungování organizačních opatření,
- řízení lidských zdrojů z pohledu bezpečnosti osobních údajů a
- nastavení a fungování technických opatření.

Níže uvádíme komentář k jednotlivým dimenzím analýzy.

1.2 Dodržování pravidel pro zpracování osobních údajů

GDPR stanoví základní zásady (základní povinnosti), které musí být dodržovány v průběhu zpracování osobních údajů.

1.2.1 *Transparentnost zpracování osobních údajů*

Všechny informace a všechna sdělení týkající se zpracování osobních údajů musí být snadno přístupné, srozumitelné a podávané za použití jasných a jednoduchých jazykových prostředků.

1.2.2 *Povinnost zpracovávat osobní údaje pouze pro konkrétní a legitimní účely*

Osobní údaje musí být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

1.2.3 *Minimalizace osobních údajů*

Osobní údaje musí být přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány.

1.2.4 *Omezení uložení osobních údajů*

Osobní údaje musí být uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány. Osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů.

1.2.5 *Zákonnost zpracování osobních údajů*

Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným způsobem. Zpracovávat osobní údaje je možné pouze tehdy, pokud existuje alespoň jeden z dále uvedených právních titulů (důvodů) pro zpracování osobních údajů:

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů,
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů,
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje,
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby,
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, nebo
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

1.3 Vedení dokumentace systému řízení osobních údajů

V rámci ověření dokumentace systému řízení osobních údajů se auditoři zabývali, zda jsou procesy zpracování osobních údajů a související procesy řádně dokumentovány. V této souvislosti auditoři prověřili existenci bezpečnostní politiky nebo jiných pravidel upravujících zásady ochrany osobních údajů. Auditoři také prověřili, zda je zdokumentováno rozdělení pravomocí a odpovědností za řízení a ochranu osobních údajů. Součástí ověření byla také metodika pro identifikaci a hodnocení aktiv a rizik. Auditoři se zabývali také existencí plánů zvládání rizik a plánů pro řízení kontinuity. Předmětem auditu byly i smlouvy se zpracovateli osobních údajů a s třetími stranami.

1.4 Organizační opatření

Auditoři prověří, zda jsou zavedena následující organizační opatření:

- nastavení pravomocí a odpovědností,
- identifikace a evidence aktiv,
- řízení rizik,
- zohledňování vlivu změn v rámci a vně organizace na systém řízení osobních údajů,

- řízení dokumentace,
- Identity Management - řízení životního cyklu uživatelů a úrovně jejich přístupu k osobním údajům,
- procesy pro řízení vztahů se zpracovateli a dalšími dodavateli,
- řízení a zvládání bezpečnostních incidentů,
- plány kontinuity,
- procesy pro komunikaci s Úřadem pro ochranu osobních údajů.

1.5 Řízení lidských zdrojů z pohledu bezpečnosti osobních údajů

Auditoři se budou zabývat také řízením lidských zdrojů z pohledu bezpečnosti osobních údajů. V této souvislosti ověří nastavení a fungování procesů pro řízení lidských zdrojů, včetně získávání a výběru zaměstnanců, uzavírání pracovněprávních smluv, motivace a rozvoje lidských zdrojů a také ukončování pracovněprávních vztahů. Auditoři se také budou zabývat zajištěním povinnosti mlčenlivosti ve vztahu k osobním údajům.

1.6 Technická opatření

Auditoři ověří, zda jsou zavedena následující organizační opatření:

- nástroje pro řízení přístupových oprávnění,
- nástroje pro ověřování identity uživatelů,
- klíčové hospodářství,
- prostředky pro zamezení neoprávněného přístupu do prostor či k osobním údajům,
- integrita komunikačních cest (např. ochranou a segmentací sítě, jejího oddělení od vnější sítě a řízením přístupů k síti, bezpečné předávání papírové dokumentace),
- používání nástroje pro ochranu před škodlivým kódem,
- nástroje pro zaznamenávání vykonávaných činností a osobními údaji v informačních systémech,
- nástroje pro sledování a vyhodnocování hrozeb v souvislosti s osobními údaji,
- používání kryptografických prostředků.

1.7 Přihlédnutí k řadě norem ISO/IEC 27000

Vzhledem k tomu, že GDPR neposkytuje podrobnější vodítka k nastavení a hodnocení systému ochrany osobních údajů, auditoři v rámci auditu přiměřeně přihlédnou k mezinárodně uznávaným standardům v oblasti řízení bezpečnosti informací, a to k normám řady ISO/IEC 27000. Auditoři s ohledem na kontext požadavků ochrany osobních údajů zvolí pro provádění auditu následující normy:

- ISO/IEC 27000: 2016 - Přehled a slovník ISMS,
- ISO/IEC 27001: 2013 - Systémy řízení bezpečnosti informací - Požadavky,
- ISO/IEC 27002: 2013 - Soubor postupů pro řízení bezpečnosti informací,

- ISO/IEC 27005: 2013 - Řízení rizik bezpečnosti informací,
- ISO/IEC 27007: 2011 - Směrnice pro auditování systému řízení bezpečnosti informací.

2. OBLASTI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

V rámci předběžného šetření auditoři identifikují tzv. oblasti zpracování osobních údajů - logické celky opakujících se činností, v rámci kterých dochází ke zpracování osobních údajů. Strukturování předmětu ověřování zvyšuje efektivitu a spolehlivost analýzy. Na základě dosavadních zkušeností se auditoři domnívají, že předmět ověřování bude možné u zadavatele rozdělit do následujících logických celků:

- výkon agend v rámci samostatné a přenesené působnosti orgány obce,
- propagační aktivity, např. uveřejňování fotografií a video a zvukových záznamů na webu nebo sociálních sítích,
- zajištění personální činnosti a zpracování mezd,
- zajištění provozních aktivit jako je např. nákup,
- vedení účetnictví,
- zajištění fyzické bezpečnosti, např. provoz kamerového systému.

U podřízených organizací lze identifikovat obdobné podpůrné procesy jako u zadavatele, tedy např. personalistiku, účetnictví atd. Mezi hlavní oblasti bude patřit např.:

- zajištění bezpečnosti a pořádku (městská policie),
- poskytování vzdělávání,
- poskytování sociálních služeb,
- poskytování knihovnických služeb a
- poskytování služeb muzeí a vystavovatelských služeb.

3. SPECIFIKA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ OBCEMI A JIMI ZŘIZOVANÝMI ORGANIZACEMI

3.1 Právní rámec

Zpracování osobních údajů se u obcí a jimi zřizovaných organizací řídí následujícími právními předpisy:

- zákon č. 101/2000 Sb., o ochraně osobních údajů,
- **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) - s účinností od** 25. května 2018.

Při posouzení dodržování základních zásad zpracování osobních údajů (zejm. zákonnost zpracování) je třeba také přihlédnout ke specifickým právním předpisům. Jde např. o zákony, které upravují působnost orgánu veřejné moci či mu stanoví úkoly,

a dále obecně zákony, které stanoví správci osobních údajů povinnost, s kterou se váže nutnost zpracovávat osobní údaje. V případě obcí a jimi zřizovaných organizací může jít např. o:

- zákon č. 128/2000 Sb., o obcích,
- zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů,
- zákon č. 320/2001 Sb., o finanční kontrole,
- zákon č. 255/2012 Sb., kontrolní řád,
- zákon č. 553/1991 Sb., o obecní policii,
- zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech,
- zákon č. 132/2006 Sb., o kronikách obcí,
- zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku,
- zákon č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání,
- zákon č. 108/2006 Sb., o sociálních službách,
- zákon č. 257/2001 Sb., knihovní zákon,
- zákon č. 262/2006 Sb., zákoník práce,
- zákon č. 435/2004 Sb., zákon o zaměstnanosti,
- zákon č. 48/1997 Sb., o veřejném zdravotním pojištění,
- zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení,
- zákon č. 280/2009 Sb., daňový řád,
- zákon č. 563/1991 Sb., zákon o účetnictví,
- zákon č. 499/2004 Sb., o archivnictví a spisové službě.

3.2 Typická rizika

Během auditů se u správců osobních údajů nejčastěji setkáváme s následujícími nedostatky:

- nedostatečná úprava odpovědnosti v souvislosti se zpracováním osobních údajů,
- nedostatečná úprava pravidel v oblasti IT (např. politiky přístupů nebo správy hesel, včetně zavedení technických opatření vynucujících uplatnění těchto pravidel),
- neplnění informační povinnosti vůči subjektům údajů (povinnost poskytovat informace o kategoriích zpracovávaných osobních údajů, účelech zpracování, příjemcích údajů a o právech subjektů údajů),
- neexistence registru zpracovávaných osobních údajů, který by obsahoval zejm. kategorie zpracovávaných osobních údajů, kategorie subjektů údajů, povahu a účely zpracování, místo, kde jsou osobní údaje shromažďovány a odpovědnost za jednotlivé fáze zpracování osobních údajů, lhůty, po které mají být osobní údaje zpracovávány a právní tituly opravňující správce k jejich zpracování,

- nedostatky při práci se souhlasy se zpracováním osobních údajů (nesprávné vymezení, kde je souhlas nezbytný ke zpracování osobních údajů a kde je zpracování osobních údajů odůvodněno jiným právním titulem, např. smlouvou, oprávněnými zájmy atd., nejasné odlišení textu souhlasu od smluvních ujednání, neplnění informační povinnosti zejm. absence konkrétního vymezení účelu, pro který budou osobní údaje zpracovávány),
- nedostatečná úprava smluv mezi správcem a zpracovateli osobních údajů (např. absence ujednání o zárukách součinnosti zpracovatele v souvislosti s vyřízením požadavků subjektů údajů uplatněných u správce těchto údajů),
- nedostatečné nastavení postupů pro uchování a likvidaci osobních údajů, zejm. s ohledem na zásadu minimalizace osobních údajů a omezení uložení osobních údajů,
- nezvyšování povědomí zaměstnanců v oblasti ochrany osobních údajů a jejich zabezpečení (např. zajištění školení),
- absence postupů pro případ narušení ochrany osobních údajů,
- absence postupů pro komunikaci s Úřadem pro ochranu osobních údajů,

Obce a se podle našich zkušeností nadto potýkají např. s následujícím:

- neplnění zákonných požadavků pro uveřejnění osobních údajů jubilantů, nebo fotografií a záznamů, které jsou osobními údaji, z veřejných akcí,
- poskytování zápisů z jednání zastupitelstva nebo pořizování a uveřejňování záznamů z jednání zastupitelstva, které obsahují osobní údaje jiných osob než členů zastupitelstva a osob vystupujících v rámci jednání, a které zaznějí na jednání zastupitelstva při projednávání jednotlivých bodů,
- nedodržení zásady minimalizace osobních údajů při vedení obecních kronik.

4. POSTUP ANALÝZY

4.1 Předběžné šetření

4.1.1 Porozumění organizaci a analýza interní dokumentace

V rámci předběžného šetření auditoři shromáždí základní informace o předmětu a charakteru činnosti zadavatele a jím zřízených organizací. Za tímto účelem auditoři mj. posoudí vnitřní předpisy, politiky, směrnice, metodiky a další podklady týkající se předmětu analýzy.

4.1.2 Dotazníkové šetření

Před započetím ověření na místě auditoři dále připraví dotazník a rozešlou jej příslušným odborům městského úřadu a zřizovaným organizacím. Prostřednictvím dotazníku budou zjišťovat typy zpracovávaných osobních údajů, povahu zpracovávaných údajů (citlivé údaje, údaje nezletilých), subjekty osobních údajů, objem subjektů údajů, účel zpracování osobních údajů, právní základ zpracování, organizační zajištění zpracování osobních údajů, toky osobních údajů, uložení, uchování a likvidaci osobních údajů a použití bezpečnostních opatření.

V případě, že si to zadavatel vyžádá, dotazování budou mít k dispozici také e-learning obsahující kurz „Nové povinnosti v ochraně osobních údajů", akreditovaný Ministerstvem vnitra pod číslem AK/PV-389/2017[1]. Použití e-learningu přispěje ke zvýšení spolehlivost získaných informací.

4.1.3 Závěr předběžného šetření

Na základě získaných informací auditoři identifikují oblasti zpracování osobních údajů. V rámci posouzení uvedených podkladů auditoři předběžně zhodnotí nastavení bezpečnostních opatření a rizika pro organizaci i pro subjekty osobních údajů, jak to vyžaduje GDPR. Na základě těchto analytických postupů auditoři stanoví základní soubory u jednotlivých oblastí analýzy a auditní vzorky pro provedení testů organizačních a bezpečnostních opatření.

4.2 Ověření procesů a opatření

Auditoři shromáždí potřebné informace a dokumenty, uskuteční rozhovory se zaměstnanci zadavatele a jím zřízených organizací, jako jsou vlastníci aktiv, IT celků, správci provozních postupů a aplikací, bezpečnostní pracovníci, a provedou plánované testy a analýzy dat. Součástí této fáze bude i fyzická prověrka prostor, v nichž jsou umístěny osobní údaje (resp. zařízení, které je zpracovávají).

Získané informace auditoři vyhodnotí. Auditoři zejm. posoudí správnost existujících postupů a dokumentace a rizika procesů zpracování osobních údajů.

4.3 Závěr analýzy

Na základě zhodnocených důkazů a informací auditoři připraví návrhy zpráv za každý subjekt zvlášť, ve kterých popíšou stav a zmapované procesy zpracování osobních údajů, dále závěry z auditu, včetně zjištěných nedostatků a identifikovaných rizik, a navrhnou změny v nastavení procesů zpracování osobních údajů a další opatření k ošetření zjištěných skutečností. Návrh zpráv projednají s příslušnými zástupci klienta a na základě výsledků projednání připraví konečnou verzi zprávy. Auditoři připraví také shrnutí za všechny ověřované organizace.

4.4 Závěrečný workshop

Po dokončení našich prací budou výstupy prezentovány formou závěrečného workshopu odpovědným zástupcům jednotlivých subjektů. Jeho obsahem bude zejména:

- Prezentace souhrnné analýzy.
- Prezentace jednotlivých detekovaných neshod a jejich možných řešení.
- Vyhodnocení rizik a jejich případných dopadů.
- Prezentace našeho systému vzdělávání pracovníků subjektů řešených na základě této zakázky.
- Panelová diskuze ohledně možných řešení.

[1] BDO Audit s.r.o. je akreditovaná vzdělávací instituce, číslo akreditace AK/I-24/2017

5. HARMONOGRAM ANALÝZY

Zahájení analýzy	T + 0 (nejpozději do 10 dnů od podpisu smlouvy)
• Úvodní setkání - kick off meeting • Rozeslání dotazníku • Rozeslání požadavků na podklady	T + 1
Analýza získaných podkladů	T + 2
• Analýza výstupů z dotazníkového šetření • Zahájení ověření na místě	T + 3
Prezentace předběžných závěrů	T + 3
Analýza získaných informací	T + 6
Příprava návrhu zpráv a celkového shrnutí	T + 7
Předání návrhu zpráv a celkového shrnutí	T + 8 (nejpozději do 30. 4. 2018)
Prezentace našich závěrů a jejich možných dopadů	T + 8 (nejpozději do 30. 4. 2018)

Týden Fáze	1	2	3	4	5	6	7	8
Zahájení auditu								
Příprava auditu								
Realizace ověření na místě								
Závěr auditu								

6. ZDROJE INFORMACÍ

Hlavním zdrojem informací budou obdržené písemné podklady a rozhovory se zaměstnanci a dalšími osobami odpovědnými za činnosti související se zpracováním osobních údajů a bezpečnost IT. Mezi dílčí zdroje patří realizace analýzy fyzické a logické architektury s ohledem na zajištění bezpečnosti informací a dat, zavedených politik pro organizaci bezpečnosti IT, řízení přístupů, zajištění fyzické bezpečnosti, řízení změn, zajištění kontinuity činnosti.

Veškeré naše ověření je vždy analyzováno vzhledem k analýze možných rizik z pohledu požadavků GDPR.

Součástí našich prací je také analýza využívaných informačních systémů. V případě, že jsou poskytovány formou služby, tak také smluvní zajištění bezpečnosti a identifikovaných rizik při zpracování osobních údajů.

7. UKÁZKA ZJIŠTĚNÍ A DOPORUČENÍ

1.		Neexistence registru osobních údajů
Zjištění:		Podle čl. 24 odst. 1 GDPR je správce povinen zavést vhodná technická a organizační opatření, aby zajistil, že zpracování osobních údajů bude v souladu s požadavky GDPR. Aniž by měl správce osobních údajů přehled o zpracovávaných osobních údajích, nemůže účinně řídit a kontrolovat nakládání s těmito údaji a jejich zabezpečení. Auditoři zjistili, že správce nevede evidenci zpracovávaných osobních údajů.
Doporučení:		Vytvořit přehledný registr zpracovávaných osobních údajů, který by obsahoval zejm. kategorie zpracovávaných osobních údajů, kategorie subjektů údajů, povahu a účely zpracování, místo, kde jsou osobní údaje shromažďovány a odpovědnost za jednotlivé fáze zpracování osobních údajů, lhůty, po které mají být osobní údaje zpracovávány, a právní tituly opravňující správce k jejich zpracování.

2.		Účtování nákladů při poskytování kopií osobních údajů
Zjištění:		Podle čl. 15 odst. 3 GDPR je správce povinen poskytnout kopii zpracovávaných osobních údajů. Za první kopii nemůže správce účtovat poplatek k úhradě vynaložených nákladů. Auditoři zjistili, že smlouva o poskytování sociální služby obsahuje informaci o možnosti nahlížet do sociální dokumentace. Pořízení výpisů, opisů nebo kopií z dokumentace na žádost klienta je však podle smlouvy fakultativní činností a klient se ve smlouvě zavazuje zaplatit za ni

	úhradu podle platného ceníku.
Doporučení:	Nejpozději od data účinnosti GDPR (25. 5. 2018) poskytovat první kopii osobních údajů subjektům údajů (např. klientům a zaměstnancům) bezplatně.

8. UKÁZKA VÝSTUPU Z ANALÝZY RIZIK

V rámci DPIA, která bude prováděna pro veškeré subjekty a jejich identifikované informační systémy jsou nejprve analyzována aktiva a následně s nimi spojená rizika.

Příkladem analyzovaného rizika je například:

Aktivum: Pracovní stanice		**Dopad**
Obecná zranitelnost	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	3
Obecná zranitelnost	Neoprávněný přístup k aktivu cizími osobami	3
Obecná zranitelnost	Zneužití práv (neoprávněná akce obsluhy)	3
Obecná zranitelnost	Zneužití systémových zdrojů	
Obecná zranitelnost	Popření	
Obecná zranitelnost	Kybernetický útok z komunikační sítě -	
Obecná zranitelnost	Zavedení škodlivého software	
Obecná zranitelnost	Selhání hardware nebo média	
Obecná zranitelnost	Selhání údržby	
Obecná zranitelnost	Chyba uživatele	
Obecná zranitelnost	Prozrazení informaci z vyřazené komponenty nebo média	
Obecná zranitelnost	Ztráta zařízení, média a dokumentu	

Obecná zranitelnost	Krádež interními pracovníky	
Obecná zranitelnost	Krádež externími pracovníky (včetně vybavení nebo dat)	
Obecná zranitelnost	Úmyslné poškození interními pracovníky	
Obecná zranitelnost	Úmyslné poškození externími pracovníky	

Naplnění požadavků GDPR je hodnoceno dle **stupňů vyzrálosti**, které jsou vyznačeny číslem a barvou od není realizováno až po plně realizováno:

1 2 3 4 bepečnostní činnosti a procesy nejsou realizovány,

1 **2** 3 4 bepečnostní činnosti a procesy jsou definovány a realizovány částečně,

1 2 **3** 4 bepečnostní činnosti a procesy jsou realizovány bez vyhodnocování,

1 2 3 **4** bepečnostní činnosti a procesy jsou realizovány a vyhodnocovány.

Ukázka vstupu:

Název oblasti	**Stav oblasti**
A.5 Politiky bezpečnosti informací	1 **2** 3 4
Popis k **politikám bezpečnosti informací**, včetně uvedení neshod, je uveden u procesu v bodě „5 Vůdčí role". Mimo návrhu politiky organizacea centrální politiky je v rámci koncernu xxx celkem 12 bezpečnostních politik pro jednotlivé oblasti bezpečnosti. Oblasti politik víceméně odpovídají oblastem normy ČSN yyy, obsahově však nejsou vždy totožné s požadavky normy. **Přezkoumání bezpečnostních politik** (dokumentace) organizace neprobíhá a ani pro něj není vytvořen proces.	
Neshody:	1. Přezkoumání bezpečnostních politik (dokumentace) ISMS neprobíhá a ani pro něj není vytvořen proces.

Název oblasti	Stav oblasti
A.6 Organizace bezpečnosti informací	1 **2** 3 4
Základní deklarace k organizaci ISMS v xxx je uveden v dokumentu *„Zahájení implementace ISO/IEC 27001-Systém řízení bezpečnosti informací v business unit zz"*. Základní popis organizace bezpečnosti na centrální úrovni, včetně popisu rolí, které budou využitelné pro ISMS je uveden v kapitole „Organizace informační bezpečnosti Organizace" v dokumentu *Rámcová směrnice pro informační bezpečnost*. Pro potřeby ISMS Organizace nesou stanoveny role bezpečnostního manažera /správce jednotky a představitele vedení jednotky. Princip oddělení povinností není stanoven, kontakty s příslušnými orgány, autoritami a zájmovými skupinami nejsou udržovány. Bezpečnost v projektech je dle vyjádření udržovány, ale chybí popis pravidel.	
Neshody:	2. Nejsou konkretizována pravidla organizace bezpečnosti informací.
	3. Nesou stanoveny role ISMS SIEMENS.
	4. Není popsáno oddělení povinností a neslučitelnost rolí v ISMS.
	5. Nejsou udržovány kontakty s příslušnými orgány a autoritami.
	6. Nejsou udržovány kontakty se zájmovými skupinami.
	7. Nejsou zpracovány postupy pro zajištění bezpečnosti informací v projektech.

Pro účely analýzy rizik je hodnota aktiva funkcí jeho nároků na zachování důvěrnosti, integrity a dostupnosti. Každý z těchto aspektů je hodnocen při řízeném pohovoru s garantem aktiva na stupnici Nízká - Střední - Vysoká. Jako hodnota aktiva pro další výpočet je brán součet takto získaných hodnot ve vyjádření Nízká = 1, Střední = 2, Vysoká = 3.

Hodnota aktiva je v tomto modelu reprezentována nároky aktiva na zachování bezpečnostních aspektů, tj. dostupnosti, důvěrnosti a integrity.

Vlastnost	Požadavek	Popis
Důvěrnost	Vysoká (V)	Ztráta důvěrnosti aktiva může způsobit ohrožení hlavních činností organizace, vážnou ztrátu důvěryhodnosti organizace, rozsáhlou negativní publicitu, sankce ve výši milionů korun a více
	Střední (S)	Ztráta důvěrnosti aktiva může způsobit ohrožení vedlejších činností organizace, narušení důvěryhodnosti organizace, občasnou negativní publicitu, sankce ve výši až statisíců korun
	Nízká (N)	Ztráta důvěrnosti aktiva nenaruší činnosti organizace, může způsobit ojedinělé stížnosti nebo sankce ve výši nejvýše desetitisíců korun
Dostupnost	Vysoká (V)	Aktivum musí být dostupné trvale, je možno tolerovat dobu nedostupnosti v řádu minut
	Střední (S)	Aktivum musí být dostupné v pracovní době, je možno tolerovat dobu nedostupnosti v řádu hodin
	Nízká (N)	Aktivum nemusí být trvale dostupné, je možno tolerovat dobu nedostupnosti v řádu dnů
Integrita	Vysoká (V)	Ztráta integrity může způsobit ohrožení hlavních činností organizace, nároky na vícepráci nebo hmotné ztráty v řádu milionů korun a více
	Střední (S)	Ztráta integrity může způsobit ohrožení vedlejších nebo omezení hlavních činností organizace, nároky na vícepráci nebo hmotné ztráty v řádu až statisíců korun
	Nízká (N)	Ztráta integrity aktiva může způsobit omezení vedlejších činností organizace, nároky na vícepráci nebo hmotné ztráty nejvýše v řádu desetitisíců korun

Následující tabulka uvádí aktiva, jejich nároky na bezpečnostní aspekty, vlastníky a respondent - ilustrativní příklad.

Skupina	Kód	Aktivum	Vlastník aktiva	Respon-dent	Požadavky na		
					Dostup-nost	Důvěr-nost	Integ-ritu
Informační aktiva	IA.1	Informace k obchodní činnosti			S	N	S
	IA.2	Informace o produktech			N	N	N
	IA.3	Informace k řízení organizace			N	N	N
	IA.4	Projektová dokumentace			S	V	S
	IA.5	Zdrojové kódy			S	V	S
	IA.6	Osobní údaje			N	V	S

Ukázka výsledné tabulky z analýzy rizik

	1 - Zápisy z porad odboru xxx	2 - Podání xxx	3 - Údaje z národního registru yyy	4 - Data sdílená s xxx	5 - Analýzy monitoringu trhu	6 - Analýzy monitoringu nad veřejně dostupnými daty	7 - Dokumentace a podklady k vyšetřovanému případu	8 - Dokumentace a podklady uzavřených vyšetřovaných případů	9 - Podpurné dokumenty a podklady vyšetřovaných případů	10 - Dokumenty a data získané při kontrole a místním šetření	11 - Manuály, příručky a informace pro xxx	12 - Emailová komunikace - běžná	13 - Dokumenty Interní	14 - Právní analýzy, vyjádření, stanoviska
Přerušení poskytování služeb			72	108	108		96							
Přerušení poskytování služeb elektronických komunikací			48	72	72		64							
Přerušení dodávky elektrické energie			96	144	144		128							
Selhání HW	16	12	12	72	72	32	96	72	72	96	6	24	20	40
Selhání SW	24	18	18	108	108	48	144	108	108	144	9	36	30	60
Selhání datového nosiče	8	6	12	72	72	32	96	72	72	96	6	24	20	20
Pochybení ze strany zaměstnanců	16	12	48	72	72	32	96	72	72	96	12	48	20	40
Zneužití vnitřních prostředků, sabotáž	16	12	48	72	72	32	96	72	72	96	6	48	20	40
Škodlivý kód	16	12	48	72	72	32	96	72	72	96	12	48	20	40
Nedostatečná ochrana vnějšího perimetru	36	9	54	243	243	36	216	162	162	216	27	162	90	90
Kybernetický útok	16	6	48	144	144	16	96	72	72	96	12	72	40	40
Trvale působící a pokročilé hrozby	16	6	48	144	144	16	96	72	72	96	12	72	40	40
Zneužití vyměnitelných technických nosičů dat	16	6	24	144	144	16	96	72	72	96	12	72	40	40

Neoprávněný přístup	16	6	48	144	144	16	96	72	72	96	12	72	40	40
Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	16	12	48	144	144	32	96	72	72	96	6	24	20	40
Nevhodné nastavení přístupových oprávnění	16	12	48	144	144	32	96	72	72	96	6	24	20	40
Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí	36	27	108	324	324	36	216	162	162	216	9	36	45	90

Popis výsledných stupňů rizik

Stupeň	Rozsah hodnot	Charakteristika
Nízké	do 20	Riziko je považováno za přijatelné.
Střední	21 - 50	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoké	51 - 200	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	200 a více	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

ID hrozby	Hrozba	Působí na:		
		Dostup-nost	Důvěr-nost	Integ-rita
Organizační nedostatky				
T.O.01	Porušení legislativních požadavků		ano	ano
T.O.02	Porušení smluvních požadavků	ano	ano	ano
T.O.03	Nevhodné nastavení přístupových oprávnění	ano	ano	ano
T.O.04	Nedostatky v nastavení a dokumentaci procesů, pravidel a rolí *(Neexistující, zastaralá, neúplná dokumentace, neseznámení zaměstnanců s dokumentací)*	ano	ano	
T.O.05	Nedostatečné monitorování činnosti uživatelů a administrátorů		ano	ano
T.O.06	Závady v komunikaci *(Mezi odděleními, mezi dodavatelem a zákazníkem...)*	ano	ano	
T.O.07	Nemožnost fyzického přístupu k technologiím	ano		
T.O.08	Nedostatečná údržba	ano		ano
T.O.09	Selhání služeb dodavatele	ano		
T.O.10	Nedostatek zdrojů *(Peněz, personálu...)*	ano		