S.ICZ a.s.

Na hřebenech II 1718/10

140 00 Praha 4

Na posouzení právních aspektů spolupracovala

PIERSTONE s.r.o., advokátní kancelář

Na Příkopě 9

110 00 Praha 1

Modelová DPIA a analýza rizik pro zpracování osobních údajů v Microsoft Office 365

Studie zpracovaná na základě poptávky Microsoft s.r.o.

Dokument:	MICR01817-STUDIE-110.docx		
Zakázka:	MICR.01817	**Verze:**	1.1
Zpracoval:	Kolektiv autorů S.ICZ	**Stav:**	finální
Datum:	10.4.2017	**Počet stran:**	137

1 PREAMBULE

1.1 IDENTIFIKACE DOKUMENTU

Název dokumentu je „Modelové posouzení vlivu na ochranu osobních údajů podle GDPR (DPIA dle nařízení GDPR, článek 35) pro zpracování osobních údajů v Microsoft Office 365, se zapracováním požadavků na VIS dle ZoKB/VoKB“ a je zpracován na základě smlouvy o dílo MICR.01817 (S.ICZ) a obj. č. 97848454 (Microsoft) mezi objednatelem Microsoft s.r.o. a zhotovitelem S.ICZ a.s.

1.2 ROZSAH DOKUMENTU

Tento dokument obsahuje studii, v rámci které

- byly identifikovány požadavky na zabezpečení osobních údajů uvedené v 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 (dále jenom „GDPR“) a zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jenom „ZoOOÚ“) a následně identifikována opatření pro pokrytí těchto požadavků ve vybraných službách Microsoft Office 365,
- bylo vypracováno modelové posouzení vlivu na ochranu osobních údajů podle GDPR, článek 35 pro zpracování osobních údajů ve vybraných službách Microsoft Office 365; v rámci tohoto posouzení byla mj.provedena analýza rizik a identifikována opatření pro zabezpečení informací uložených ve vybraných službách Microsoft Office 365,
- byla popsána organizační a technická opatření ve vybraných službách Microsoft Office 365.

Dokument obsahuje pět hlavní části:

- Definice vzorových scénářů
- Identifikace a analýza požadavků relevantních pro zpracování osobních údajů
- Modelové posouzení vlivu na ochranu osobních údajů pro popsané scénáře
- Popis organizačních opatření zajištěných v prostředí Microsoft Office 365
- Popis technických opatření zajištěných v prostředí Microsoft Office 365

1.3 UŽIVATELÉ DOKUMENTU

Dokument je určen k výhradnímu užití následující skupinou osob:

- Microsoft s.r.o.
- Osoby určené společností Microsoft s.r.o.

1.4 HISTORIE DOKUMENTU

Tab. 1 Historie dokumentu

Verze	Datum	Autor	Poznámka
0.5	8.3.2017	Ondřej Steiner, Petr Řehoř	Pracovní verze k připomínkám
1.0	31.3.2017	Ondřej Steiner, Petr Řehoř, Jakub Řehák	Finální verze
1.1	10.4.2017	Ondřej Steiner	Zapracování připomínek

2 OBSAH

3 SEZNAM TABULEK A OBRÁZKŮ

3.1 SEZNAM TABULEK

3.2 SEZNAM OBRÁZKŮ

4 ÚVOD

Cílem studie je poskytnout modelové posouzení vlivu na ochranu osobních údajů podle GDPR (článek 35) obsahující analýzu rizik z pohledu subjektů údajů, která bude zároveň vycházet z požadavků zákona č. 181/2014 Sb. (o kybernetické bezpečnosti; dále jenom „ZoKB“) resp. vyhlášky č. 316/2014 Sb. (o kybernetické bezpečnosti; dále jenom „VoKB“) na analýzu rizik, a to pro případ zpracování osobních údajů ve vybraných službách Microsoft Office 365, konkrétně SharePoint Online, Exchange Online / Outlook a Skype for Business.

Kromě toho je cílem studie identifikovat organizační a technická bezpečnostní opatření, která jsou potřeba pro pokrytí identifikovaných rizik nebo explitních požadavků na bezpečnostní opatření uvedených ve GDPR, VoKB a zákonu č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále i jenom „ZoOOÚ“), nebo identifikace oblastí, kde potřebná bezpečnostní opatření nebyla nalezena.

Studie předpokládá, že ve službě Microsoft Office 365 jsou zpravovánány osobní údaje a mohou být zpracovávány i citlivé (osobní) údaje podle ZoOOÚ neboli zvláštní kategorie osobních údajů podle GDPR.

Studie neobsahuje podrobnou analýzu naplnění požadavků ZoKB/VoKB neboť této oblasti je věnovaná samostatná studie Protecting Data in Microsoft Online Services (Studie zpracovaná na základě poptávky Microsoft s.r.o.) – viz [1], na kterou tímto odkazujeme.

5 MANAŽERSKÉ SHRNUTÍ

Úroveň a způsob realizace bezpečnostních opatření v cloudových službách Microsoft Online Services (Microsoft Office 365) umožňuje pro níže uvedené scénáře zahrnující

- **používání služby SharePoint Online,**
- **používání služby Exchange Online a**
- **používání služby Skype for Business**

ukládání a zpracování osobních nebo citlivých údajů podle zákona č. 101/2000 Sb., o ochraně osobních údajů, a do budoucna i nařízení Evropského parlamentu a Rady (EU) 2016/679.

Úroveň a způsob realizace bezpečnostních opatření umožňuje pokrytí relevantních legislativních požadavků, a to konkrétně požadavků

- zákona č. 101/2000 Sb., o ochraně osobních údajů (viz [82]) a
- nařízení Evropského parlamentu a Rady (EU) 2016/679 (viz [81]).

Podmínkou ukládání a zpracování osobních a citlivých (osobních) údajů je však výběr a implementace potřebných opatření z oblasti organizační a technické bezpečnosti, což zejména zahrnuje

- výběr a implementaci technických opatření ve formě níže uvedených cloudových technologií a služeb a
- výběr a implementaci organizačních opatření v prostředí správce.

V tomto případě je nezbytné, aby bezpečnostní opatření realizovaná společností Microsoft v cloudových službách Microsoft Online Services (která jsou vyspělá a na vysoké úrovni) byla podporována bezpečnostními opatřeními správce (pověřené osoby)[1], neboť ani ta sebelepší technická opatření nemohou bez podpory organizačních opatření poskytnout odpovídající záruky.

[1] Pojmy pověřená osoba a správce mají v dokumentu ten samý význam..

6 DEFINICE SCÉNÁŘŮ

Tato kapitola obsahuje definici scénářů pro potřeby analýzy rizik a návrhu bezpečnostních opatření.

6.1 SCÉNÁŘ 1 – SHAREPOINT ONLINE

Povinná osoba (správce) využívá cloudovou službu Office 365 SharePoint Online pro ukládání a zpracování dokumentů, seznamů a dalších dat, které mohou obsahovat osobní nebo citlivé (osobní) údaje, zejména pro:

- Uložení dokumentů do dokumentových knihoven a sdílený přístup k nim.
- Zpracování uložených dokumentů a seznamů prostřednictvím pracovních postupů (Workflow).
- Zpracování uložených dokumentů, seznamů a dat pomocí aplikací vyvinutých pro prostředí SharePoint Online.

Scénář uložení dat v SharePoint Online zahrnuje:

- Uložení dokumentů do dokumentových knihoven a sdílený přístup k nim.
- Zpracování uložených dokumentů a seznamů prostřednictvím pracovních postupů (Workflow).
- Správu uživatelských účtů a skupin v Azure AD.
- Přístup ke službě SharePoint Online prostřednictvím veřejné počítačové sítě Internet.

Scénář uložení dat v SharePoint Online nezahrnuje:

- Zpracování uložených dokumentů, seznamů a dat pomocí aplikací vyvinutých pro prostředí SharePoint Online.
- Rozhraní (interface) na externí systémy v hybridním scénáři nebo na externí systémy třetích stran.
- Klientská zařízení.
- Zařízení interních sítí a Internetu.

V tomto scénáři jsou použity následující cloudové služby:

- Office 365 SharePoint Online – Platforma pro vytváření webových aplikací a zpracování dat.
- Azure AD – Adresářová služba obsahující účty uživatelů a jejich skupiny.

Podle požadovaného stupně zabezpečení mohou být dále použity cloudové služby:

- Office 365 Per-File Encryption – šifrování souborů uložených v Sharepoint Online symetrickým klíčem, způsobu správy klíčů je uveden v dokumentu [8].
- Office 365 Advanced Encryption – soubory uložené v Sharepoint Online jsou šifrovány symetrickým klíčem uloženým v Azure KeyVault.
- Azure KeyVault – cloudová služba umožňující ukládat asymetrické a symetrické šifrovací klíče, přihlašovací údaje a podobné sensitivní údaje do HSM provozovaným v Azure. Řešení je možné rozšířit o synchronizaci těchto údajů z on-premis HSM v síti zákazníka.
- Customer Lockbox for Office 365 – umožňuje zákazníkovi schvalovat přístup zaměstnanců Microsoft k citlivým datům zákazníka uloženým v Office 365 pokud potřebují přístup k datům při během technické podpory.
- Azure Rights Management Service – umožňuje šifrovat maily a přílohy a řídit přístup k nim. Klient musí podporovat technologii Microsoft Rights Management Service.

- Azure Log Analytics – pokročilé zpracování logů pro cloudové služby Office 365 a Azure i pro on-premise servery a zařízení.

6.2 SCÉNÁŘ 2 – EXCHANGE ONLINE / OUTLOOK

Povinná osoba (správce) využívá cloudovou službu Office 365 Exchange Online pro sběr a distribuci informací a pro skupinovou spolupráci využívající emaily, kontakty, kalendáře, úkoly a poznámky které mohou obsahovat osobní nebo citlivé (osobní) údaje, tedy pro:

- Práci s osobními a skupinovými emaily.
- Práci s osobními a skupinovými adresáři kontaktů.
- Práci s osobními a skupinovými kalendáři.
- Práci s osobními a skupinovými seznamy úkolů.
- Práci s osobními a sdílenými poznámkami.
- Práce s připojenými dokumenty.

Scénář uložení dat v Exchange Online zahrnuje:

- Uložení emailů, kontaktů, událostí, úkolů, poznámek a připojených dokumentů do emailové schránky a jejich zpracování.
- Odesílání a příjem zpráv elektronické pošty prostřednictvím standardních protokolů (SMTP).
- Správu uživatelských účtů a skupin v Azure AD.
- Přístup ke službě Exchange Online prostřednictvím veřejné počítačové sítě Internet.

Scénář uložení dat v Exchange Online nezahrnuje:

- Rozhraní (interface) na externí systémy v hybridním scénáři nebo na externí systémy třetích stran s výjimkou SMTP komunikace, pro kterou budou navržena dostupná bezpečnostní opatření.
- Klientská zařízení.
- Zařízení interních sítí a Internetu.

V tomto scénáři jsou použity cloudové služby:

- Office 365 Exchange Online – Platforma pro skupinovou spolupráci využívající emaily, kontakty, kalendáře a úkoly.
- Azure AD – Adresářová služba obsahující účty uživatelů a jejich skupiny.

Podle požadovaného stupně zabezpečení mohou být dále použity cloudové služby:

- Office 365 Message Encryption – umožňuje šifrovat maily externím uživatelům i v případě že jejich klient nepodporuje S/MIME nebo Microsoft Rights Management Service.
- Office 365 Advanced Encryption – maily, přílohy, kalendáře, úkoly a poznámky v Exchange Online jsou šifrovány symetrickým klíčem uloženým v Azure KeyVault.
- Customer Lockbox for Office 365 – umožňuje zákazníkovi schvalovat přístup zaměstnanců Microsoft k citlivým datům zákazníka uloženým v Office 365 pokud potřebují přístup k datům při během technické podpory.
- Azure KeyVault – cloudová služba umožňující ukládat asymetrické a symetrické šifrovací klíče, přihlašovací údaje a podobné sensitivní údaje do HSM provozovaným v Azure. Řešení je možné rozšířit o synchronizaci těchto údajů z on-premis HSM v síti zákazníka.
- Azure Rights Management Service – umožňuje šifrovat maily a přílohy a řídit přístup k nim. Klient musí podporovat technologii Microsoft Rights Management Service.
- Azure Log Analytics – pokročilé zpracování logů pro cloudové služby Office 365 a Azure i pro on-premise servery a zařízení.

6.3 SCÉNÁŘ 3 – SKYPE FOR BUSINESS

Povinná osoba (správce) využívá cloudovou službu Office 365 Skype for Business pro osobní a skupinovou komunikaci využívající audio i video, která umožňuje přenášet data ve formě souborů mezi účastníky komunikace a nahrávky uskutečněné komunikace, které mohou obsahovat osobní nebo citlivé (osobní) údaje, tedy pro:

- Telefonní a video hovory mezi dvěma účastníky a konference více účastníků.
- Chat mezi dvěma nebo více účasníky.
- Přenos souborů mezi dvěma nebo více účastníky během telefonních a video hovorech, při chatu i mimo tyto aktivity včetně případů kdy je příjemce offline.
- Přístup k archivu nahrávek telefonních a video hovorů a konferencí, záznamů chatů a uložených souborů.

Scénář zpracování dat v Skype for Business zahrnuje:

- Telefonní a video hovory mezi dvěma účastníky a konference více účastníků.
- Chat mezi dvěma nebo více účasníky.
- Přenos souborů mezi dvěma nebo více účastníky během telefonních a video hovorech, při chatu i mimo tyto aktivity včetně případů kdy je příjemce offline.
- Přístup k archivu nahrávek telefonních a video hovorů a konferencí, záznamů chatů a uložených souborů.
- Správu uživatelských účtů a skupin v Azure AD.
- Přístup ke službě Skype for Business prostřednictvím veřejné počítačové sítě Internet.

Scénář zpracování dat v Skype for Business nezahrnuje:

- Rozhraní (interface) na externí systémy v hybridním scénáři nebo na externí systémy třetích stran.
- Klientská zařízení.
- Zařízení interních sítí a Internetu.

V tomto scénáři jsou být použity cloudové služby:

- Office 365 Skype for Business – Platforma pro osobní a skupinovou komunikaci a spolupráci.
- Azure AD – Adresářová služba obsahující účty uživatelů a jejich skupiny.

Podle požadovaného stupně zabezpečení mohou být dále použity cloudové služby:

- Office 365 Per-File Encryption – Skype for Bussiness ukládá soubory do Sharepoint Online, kde jsou šifrovány symetrickým klíčem, způsobu správy klíčů je uveden v dokumentu [4].
- Office 365 Advanced Encryption – Skype for Bussiness ukládá soubory do Sharepoint Online, kde jsou šifrovány symetrickým klíčem uloženým v Azure KeyVault.
- Customer Lockbox for Office 365 – umožňuje zákazníkovi schvalovat přístup zaměstnanců Microsoft k citlivým datům zákazníka uloženým v Office 365 pokud potřebují přístup k datům při během technické podpory.
- Azure KeyVault – cloudová služba umožňující ukládat asymetrické a symetrické šifrovací klíče, přihlašovací údaje a podobné sensitivní údaje do HSM provozovaným v Azure. Řešení je možné rozšířit o synchronizaci těchto údajů z on-premis HSM v síti zákazníka.
- Azure Rights Management Service – umožňuje šifrovat maily a přílohy a řídit přístup k nim. Klient musí podporovat technologii Microsoft Rights Management Service.
- Azure Log Analytics – pokročilé zpracování logů pro cloudové služby Office 365 a Azure i pro on-premise servery a zařízení.

7 IDENTIFIKACE A ANALÝZA LEGISLATIVNÍCH POŽADAVKŮ

V rámci této kapitoly je provedena analýza, zda jsou smluvní ustanovení a technická specifikace služeb (včetně technické dokumentace) společnosti Microsoft v souladu s vybranými legislativními požadavky vztahujícími se na zpracování osobních údajů v cloudovém prostředí. Tato kapitola neobsahuje úplný výčet legislativních požadavků, které se na využití cloud vztahují, ale analyzuje vybraná důležitá ustanovení týkající se ochrany osobních údajů se zaměřením na ustanovení kladoucí požadavky na smlouvu mezi společností Microsoft jakožto poskytovatelem cloudu a jeho zákazníky jakožto správci osobních údajů.

U každého požadavku je následně uvedeno, zda a jakým způsobem je daný požadavek v cloudovém prostředí Microsoft Office 365 pokryt podle Podmínek pro služby online platných k 1. únoru 2017 (dále jen „**PSO**“), které stanoví podmínky pro užívání služeb online, včetně Microsoft Office 365. Smluvní vztah mezi společností Microsoft a zákazníky není stanoven pouze v PSO, ale také v dalších dokumentech uzavíraných zákazníkem při nákupu služby Microsoft Office 365; mezi tyto patří např. Master Business and Services Agreement (Smlouva Business and Services), Enterprise Agreement (Smlouva Enterprise), Enterprise Enrollment for Server and Cloud (Prováděcí smlouva Enterprise) a další. Tato kapitola analyzuje, zda vybrané legislativní požadavky jsou pokryty smluvními závazky společnosti Microsoft v PSO. V níže identifikovaných případech je posuzováno, (i) zda ustanovení smluvní dokumentace, zejména PSO, reflektují vybrané legislativní požadavky, a (ii) jakým způsobem je legislativní požadavek zajištěn z technického hlediska a zda je služba Microsoft Office 365 schopná splnit tyto legislativní požadavky.

Nad rámec posouzení smluvní dokumentace, zejména PSO, obsahuje tato kapitola ve vybraných případech posouzení, zda legislativní požadavky nejsou pokryty technickými specifikacemi služeb nebo zda tyto požadavky lze pokrýt na aplikační úrovni.

V níže identifikovaných případech je předpokládáno, že poskytovatel cloudových služeb vystupuje v roli zpracovatele osobních údajů, což je v souladu s publikovaným názorem Úřadu pro ochranu osobních údajů – viz [83], [84] a [85]. Dále v kontextu tohoto dokumentu není předpokládáno, že by poskytovatel cloudových služeb vystupoval (a to ani částečně) také v roli správce osobních údajů.

7.1 OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (EU)

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 (dále jen „obecné nařízení o ochraně osobních údajů“ nebo „GDPR“) vstoupí v účinnost 25. 5. 2018, a to plošně ve všech státech EU. GDPR stanoví obecná pravidla pro správu a zpracování osobních údajů a od chvíle, kdy vstoupí v účinnost, bude platit jako přímo aplikovatelná legislativa v České republice. Očekává se, že v rámci zákonodárného procesu na národní úrovni bude stávající zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) této situaci přizpůsoben.

Pozn: Požadavky uvedené v této kapitole nemusí být v současnosti zcela pokryty, neboť GDPR vstoupí v účinnost až 25. 5. 2018.

Tab. 2 Požadavky obecného nařízení o ochraně osobních údajů a jejich pokrytí dle PSO

ID požadavku	**Stručný popis**	**Podrobnější popis** (znění právního předpisu)	**Popis pokrytí**
Článek 28, odst. 1	Poskytnutí záruk zpracovatelem	Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.	**Vyhodnocení:** v souladu s GDPR Microsoft implementoval technická a organizační opatření podle níže uvedených ISO standardů a mnohá další opatření, která jsou specifikována v PSO v části „Podmínky zpracování dat – Zabezpečení“ na str. 11–12 PSO. Na základě toho se domníváme, že správce údajů (zákazník Microsoftu) naplní povinnosti tohoto požadavku, pokud se rozhodne pro Microsoft jakožto zpracovatele osobních údajů. V konkrétním případě zpracování údajů má zákazník (správce údajů) právo vyžádat si další specifické záruky, které by musely být řešeny na individuální bázi. **Relevantní ustanovení PSO:** *Zabezpečení (str. 8)* Prioritou společnosti Microsoft je napomáhat při ochraně bezpečnosti informací zákazníka. Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením. *Zabezpečení (str. 11)* Společnost Microsoft implementovala a pro služby online bude v souvislosti se závazky k zabezpečení uvedenými v podmínkách pro služby online udržovat a dodržovat následující bezpečnostní opatření, která představují jedinou odpovědnost společnosti Microsoft s ohledem

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			na zabezpečení zákaznických dat. *Zásady zabezpečení informací služeb online (str. 12)* Každá služba online se řídí písemnými zásadami zabezpečení dat („zásady zabezpečení informací“), které odpovídají standardům a rámcům řízení uvedeným v tabulce níže. (níže je uvedená tabulka, podle které zabezpečení služeb „Office 365“ odpovídají standardům ISO 27001, ISO 27002, ISO 27018 a dalším). **Relevantní opatření:** Tento obecný požadavek je pokryt všemi organizačními opatřeními uvedenými v kapitole 9 a výběrem relevantních technických opatření uvedených v kapitole 10 a je provedený na základě hodnocení (analýzy) rizik. Opatření: všechna z 9 a výběr z 10
Článek 28, odst. 2	Zapojení dalšího zpracovatele	Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Použití dodavatelů (str. 8)* Společnost Microsoft může najmout subdodavatele za účelem poskytování služeb jejím jménem. Tito subdodavatelé budou smět zákaznická data získat pouze za účelem poskytování služeb, k jejichž poskytování se zavázali, a nebudou smět tato data používat za jakýmkoli jiným účelem. Společnost Microsoft zůstává odpovědná za dodržování souladu s povinnostmi stanovenými v těchto podmínkách služeb online svými subdodavateli. Zákazník již dříve souhlasil s tím, že společnost Microsoft smí přenést zákaznická data k subdodavatelům podle popisu v těchto podmínkách pro služby online. *Soukromí – Předávání subdodavatelům (str. 11)* Společnost Microsoft může najmout subdodavatele za účelem poskytování určitých omezených nebo pomocných služeb jejím jménem. Subdodavatelé, kterým společnost Microsoft předává zákaznická data, i ta používaná pro účely uchovávání, uzavřou se společností Microsoft písemné dohody, které nabízejí stejnou ochranu jako podmínky zpracování údajů. Zákazník již dříve souhlasil s tím, že společnost Microsoft smí předávat zákaznická data subdodavatelům

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			podle popisu v těchto podmínkách zpracování údajů. Není-li v podmínkách zpracování údajů stanoveno jinak, nebo pokud zákazník nesvolí jinak, společnost Microsoft nebude předávat jakékoli třetí straně (a to ani za účelem ukládání) osobní údaje, které zákazník poskytne společnosti Microsoft prostřednictvím užívání služeb online. Společnost Microsoft poskytuje web, který uvádí subdodavatele oprávněné k přístupu k zákaznickým datům ve službách online i omezené nebo pomocné služby, které poskytují. Minimálně 6 měsíců před poskytnutím oprávnění novému subdodavateli k přístupu k zákaznickým datům společnost Microsoft tento web aktualizuje a poskytne zákazníkovi mechanismus k obdržení upozornění na tuto aktualizaci. Pokud zákazník nového subdodavatele neschválí, může dotčenou službu online ukončit bez postihu, a to předložením písemné výpovědi před koncem informační lhůty, která vysvětluje důvody neschválení subdodavatele. Pokud je dotčená služba online součástí sady (nebo podobného jednotlivého nákupu služeb), bude se ukončení vztahovat na celou sadu. Po ukončení společnost Microsoft odstraní platební závazky k ukončeným službám online z následujících faktur zákazníka. **Relevantní opatření:** Opatření: 9.5
Článek 28, odst. 3	Smlouva se zpracovatelem – základní požadavky	Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:	**Vyhodnocení:** v souladu s GDPR Zpracování osobních údajů je prováděno na základě smluvního ujednání, zejména pak na základě PSO, které společně s dalšími smluvními dokumenty tvoří smlouvu o zpracování mezi zákazníkem (správcem údajů) a společností Microsoft (zpracovatelem údajů). **Relevantní ustanovení PSO:** *Podmínky zpracování dat (str. 9)* (…) podmínky v multilicenční smlouvě zákazníka, včetně podmínek zpracování údajů, představují smlouvu o zpracování údajů, podle které je společnost Microsoft zpracovatelem údajů; a (…) **Relevantní opatření:** Opatření: 9.5
		(…) v nichž je stanoven předmět a doba trvání zpracování (…)	**Vyhodnocení:** v souladu s GDPR

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
			Relevantní ustanovení PSO: *Definice (str. 4)* „Zákaznická data“ označují všechna data včetně veškerých textových, zvukových, video nebo obrazových souborů a softwaru poskytnutých společnosti Microsoft zákazníkem či jeho afilacemi, případně jejich jménem, během používání služby online ze strany zákazníka. *Použití zákaznických dat (str. 7)* Zákaznická data budou použita pouze pro poskytování služeb online zákazníkovi, včetně účelů kompatibilních s poskytováním těchto služeb. Společnost Microsoft nebude zákaznická data využívat ani z nich nebude odvozovat informace pro žádné reklamní či podobné komerční účely. Platí ustanovení mezi smluvními stranami, že si zákazník zachová všechna práva, duševní vlastnictví a zájem týkající se zákaznických dat. Společnost Microsoft nezískává k zákaznickým datům žádná práva s výjimkou práv, která společnosti Microsoft přidělí zákazník pro poskytování služeb online zákazníkovi. Tento odstavec nemá vliv na práva společnosti Microsoft k softwaru nebo službám, které společnost Microsoft licencuje zákazníkovi. *Trvání a objekt zpracování údajů (str. 10)* Údaje budou zpracovávány po dobu určenou v multilicenční smlouvě zákazníka. Cílem zpracovávání údajů je výkon služeb online. *Dodatek 1 (str. 32)* Data budou zpracovávána po dobu uvedenou v příslušné multilicenční smlouvě uzavřené mezi vývozcem údajů a právnickou osobou společností Microsoft, ke které jsou přiloženy tyto standardní smluvní doložky („Microsoft“). Cílem zpracovávání údajů je výkon služeb online.

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
		(…) povaha a účel zpracování (…)	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Použití zákaznických dat (str. 7)* Zákaznická data budou použita pouze pro poskytování služeb online zákazníkovi, včetně účelů kompatibilních s poskytováním těchto služeb. *Úmysl stran (str. 10)* V případě služeb online představuje společnost Microsoft zpracovatele (nebo dílčího zpracovatele) údajů, který zastupuje zákazníka. Jako zpracovatel (nebo dílčí zpracovatel) údajů bude společnost Microsoft jednat na základě pokynů zákazníka. Podmínky pro služby online a multilicenční smlouva zákazníka (včetně podmínek a ujednání začleněných do nich odkazem) společně se zákazníkovým užíváním a konfigurací funkcí služeb online představují úplné a konečné pokyny zákazníka pro společnost Microsoft ohledně zpracování zákaznických dat. Jakékoli další nebo alternativní pokyny musí být dohodnuty v souladu s procesem doplnění multilicenční smlouvy zákazníka. *Rozsah a účel zpracování (str. 11)* Rozsah a účel zpracování zákaznických dat, včetně jakýchkoli osobních údajů obsažených v zákaznických datech, je popsán v podmínkách zpracování údajů a v multilicenční smlouvě zákazníka.
		(…) typ osobních údajů (…)	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Definice (str. 4)* „Zákaznická data“ označují všechna data včetně veškerých textových, zvukových, video nebo obrazových souborů a softwaru poskytnutých společnosti Microsoft zákazníkem či jeho afilacemi, případně jejich jménem, během používání služby online ze strany zákazníka. *Podmínky zpracování dat (str. 9)* V podmínkách zpracování údajů se pojem „služby online“ vztahuje pouze na služby uvedené v tabulce níže, s výjimkou náhledů, a pojem

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
			„zákaznická data“ zahrnuje pouze zákaznická data, která jsou poskytována prostřednictvím těchto služeb online.
		(…) kategorie subjektů údajů (…)	**Vyhodnocení:** pravděpodobně v souladu s GDPR PSO výslovně neuvádí, zda jsou v rámci online služeb zpracovávány např. citlivé údaje či jiné „zvláštní kategorie“ osobních údajů uvedené v článku 9 GDPR. Na druhou stranu v Dodatku č. 1 ke Standardním smluvním doložkám se stanoví, že mezi zpracovávané údaje patří např. e-mail, dokumenty a ostatní data v elektronickém formátu. Vzhledem k tomu, že v současné době není zřejmé, jakým způsobem bude vykládán pojem „kategorie dat“ dle článku 28 GDPR, nelze definitivně posoudit, zda Microsoft v PSO tuto povinnou náležitost zpracovatelské smlouvy splňuje či nikoliv. Vzhledem k tomu, že PSO v definici „zákaznických dat“ stanoví, že se může jednat o všechna data poskytnutá společnosti Microsoft, a dále druhy údajů specifikuje pro účely transferu do zahraničí ve Standardních smluvních doložkách, domníváme se, že PSO jsou pravděpodobně v souladu s GDPR. Zároveň společnost Microsoft nabízí množinu dodatečných technických bezpečnostních opatření, která může zákazník implementovat na základě své volby a potřeby s ohledem na zpracovávané kategorie údajů. Zároveň společnost Microsoft implementovala a nadále udržuje svá bezpečnostní opatření na vysoké úrovni (v souladu se standardy řady ISO/IEC 27000, auditní zprávou systému řízení podle ISO/IEC 27001 a auditními zprávami SOC 1 a SOC 2, typ II). **Relevantní ustanovení PSO:** *Definice (str. 4)* „Zákaznická data“ označují všechna data včetně veškerých textových, zvukových, video nebo obrazových souborů a softwaru poskytnutých společnosti Microsoft zákazníkem či jeho afilacemi, případně jejich jménem, během používání služby online ze strany zákazníka. *Dodatek 1 (str. 32)* Kategorie údajů: Mezi přenášené osobní údaje patří e-mail, dokumenty a ostatní data v elektronickém formátu v kontextu služeb online.

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
		(…) povinnosti a práva správce (…)	**Vyhodnocení:** v souladu s GDPR Jednotlivá práva a povinnosti smluvních stran jsou uvedené napříč PSO a jsou dostatečně specifická.
Článek 28, odst. 3, písm. a)	Smlouva se zpracovatelem – bližší specifikace	Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel: a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;	**Vyhodnocení:** v souladu s GDPR Microsoft zpracovává osobní údaje pouze na základě pokynů zákazníka. Z ustanovení PSO není výslovně zřejmé, zda jsou pokyny zákazníka ve vztahu ke zpracování zákaznických dat „doložené“ dle požadavků GDPR. V PSO se stanoví, že Microsoft bude jednat na základě pokynů zákazníka, které jsou představovány mj. „zákazníkovým užíváním a konfigurací funkcí služeb online“. Jakékoliv užívání či konfigurace služeb jsou dostatečně zdokumentované a doložitelné v rámci záznamů a „logů“ veškerých operací: Domníváme se proto, že PSO a online služby jsou v souladu s GDPR. **Relevantní ustanovení PSO:** *Úmysl stran (str. 10)* Úmysl stran. V případě služeb online představuje společnost Microsoft zpracovatele (nebo dílčího zpracovatele) údajů, který zastupuje zákazníka. Jako zpracovatel (nebo dílčí zpracovatel) údajů bude společnost Microsoft jednat na základě pokynů zákazníka. Podmínky pro služby online a multilicenční smlouva zákazníka (včetně podmínek a ujednání začleněných do nich odkazem) společně se zákazníkovým užíváním a konfigurací funkcí služeb online představují úplné a konečné pokyny zákazníka pro společnost Microsoft ohledně zpracování zákaznických dat. Jakékoli další nebo alternativní pokyny musí být dohodnuty v souladu s procesem doplnění multilicenční smlouvy zákazníka. **Relevantní opatření:** Tyto oblasti upravují všeobecné obchodní podmínky: Podmínky pro služby online, viz [4].

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
Článek 28, odst. 3, písm. b)		b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Pracovníci společnosti Microsoft (str. 10)* Pracovníci společnosti Microsoft nebudou zákaznická data zpracovávat bez svolení zákazníka. Pracovníci společnosti Microsoft musí zákaznická data uchovávat v bezpečí a v tajnosti tak, jak je popsáno v podmínkách zpracování údajů, a tato povinnost platí i po ukončení jejich závazků. *Dodatek 2 (str. 33)* Pracovníci dovozce údajů nebudou zákaznická data zpracovávat bez oprávnění. Pracovníci musí zachovávat důvěrnost zákaznických dat a tato povinnost platí i po ukončení jejich závazků.
Článek 28, odst. 3, písm. c)		c) přijme všechna opatření požadovaná podle článku 32;	**Vyhodnocení:** Viz posouzení článku 32 GDPR níže
Článek 28, odst. 3, písm. d)		d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;	**Vyhodnocení:** v souladu s GDPR PSO garantují, že společnost Microsoft se svými sub-dodavateli uzavře dohodu se stejnou úrovní ochrany, jakou poskytuje Microsoft na základě PSO. PSO výslovně neuvádí přesnější specifikaci požadovaných opatření. **Relevantní ustanovení PSO:** *Předávání subdodavatelům (str. 10)* Společnost Microsoft může najmout subdodavatele za účelem poskytování určitých omezených nebo pomocných služeb jejím jménem. Subdodavatelé, kterým společnost Microsoft předává zákaznická data, i ta používaná pro účely uchovávání, uzavřou se společností Microsoft písemné dohody, které nabízejí stejnou ochranu jako podmínky zpracování údajů. *Dodatek 1 (str. 33)* Dovozce údajů může najmout jiné společnosti za účelem poskytování omezených služeb jeho jménem, například k poskytování zákaznické

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			podpory. Tito subdodavatelé budou smět zákaznická data získat pouze za účelem poskytování služeb, k jejichž poskytování se zavázali, a nebudou smět tato data používat za jakýmkoli jiným účelem.
Článek 28, odst. 3, písm. e)		e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;	**Vyhodnocení:** v souladu s GDPR PSO stanoví obecné povinnosti, na základě kterých společnost Microsoft může zpracovávat osobní údaje pouze na základě instrukcí od svých zákazníků. PSO stanoví, že v určitých situacích buď poskytne zákazníkovi možnost opravit, odstranit či zablokovat osobní údaje subjektů údajů nebo tak učiní sám Microsoft, pokud tak stanoví příslušné předpisy. Ačkoliv tedy PSO výslovně nestanoví, že společnost Microsoft má obecnou povinnost být nápomocna správci (svým zákazníkům) konkrétně pro účel naplnění povinnosti reagovat na žádosti subjektů údajů, jak předpokládá toto ustanovení GDPR, jsme toho názoru, že společnost Microsoft je v souladu s obecnými požadavky GDPR, neboť se zavazuje řídit pokyny správce údajů. **Relevantní ustanovení PSO:** *Přístup k zákaznickým datům (str. 11)* Po dobu určenou v multilicenční smlouvě zákazníka bude společnost Microsoft podle svého rozhodnutí a podle potřeby na základě rozhodného práva a s použitím článku 12(b) směrnice o ochraně osobních údajů EU buď: (1) poskytovat zákazníkovi možnost opravit, odstranit nebo zablokovat zákaznická data, nebo (2) provádět takové opravy, odstranění nebo blokování jménem zákazníka.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
Článek 28, odst. 3, písm. f)		f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zp racování a informací, jež má zpracovatel k dispozici;	**Vyhodnocení:** v souladu s GDPR Ačkoliv PSO neobsahují konkrétní závazek společnosti Microsoft, že bude nápomocna svým zákazníkům za účelem zajištění souladu s bezpečnostními normami ve vztahu k osobním údajům, zavazuje se společnost Microsoft jednat v souladu s pokyny svých zákazníků. Navíc PSO výslovně stanoví pravidla pro asistenci s blokací, opravou či odstranění údajů o subjekt údajů. **Relevantní ustanovení PSO:** *Přístup k zákaznickým datům (str. 11)* Po dobu určenou v multilicenční smlouvě zákazníka bude společnost Microsoft podle svého rozhodnutí a podle potřeby na základě rozhodného práva a s použitím článku 12(b) směrnice o ochraně osobních údajů EU buď: (1) poskytovat zákazníkovi možnost opravit, odstranit nebo zablokovat zákaznická data, nebo (2) provádět takové opravy, odstranění nebo blokování jménem zákazníka.
		g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;	**Vyhodnocení**: v souladu s GDPR Ačkoliv společnost Microsoft v PSO výslovně neumožňuje svým zákazníkům vybrat si mezi smazáním a vrácením osobních údajů po ukončení poskytování služeb, jak je předpokládáno GDPR, společnost Microsoft splňuje tento požadavek, jelikož umožňuje po určitou dobu po ukončení poskytování služeb všem zákazníkům přístup ke svým datům, která si mohou extrahovat. Pro případ exportu velkých objemů dat ze služby Office 365 nabízí Microsoft službu „Azure Import/Export“, v rámci které je transfer zajištěn za pomocí pevných disků se zabezpečením šifrování dat, zaslaných kurýrní službou. Microsoft tak nabízí službu „vrácení“ dat svým zákazníkům. V případě, že si zákazník data sám neextrahuje Microsoft dané údaje vymaže. Ačkoliv to není výslovně uvedeno v PSO, je požadavek GDPR na možnost zákazníka si vybrat mezi smazáním a vrácením osobních údajů po ukončení poskytování online služeb fakticky naplněn. **Relevantní ustanovení PSO:** *Uchování dat (str. 4)*

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			Kdykoli během doby platnosti odběru zákazníka bude mít zákazník možnost přistupovat k zákaznickým datům uloženým v každé ze služeb online a tato data získávat. S výjimkou bezplatných zkušebních verzí společnost Microsoft uchová všechna zákaznická data uložená ve službě online s omezenou funkčností po dobu nejméně 90 dnů od uplynutí doby účinnosti nebo vypovězení platnosti předplatného zákazníka, aby si zákazník tato data mohl vyzvednout. Po uplynutí 90denního období uchování společnost Microsoft účet zákazníka deaktivuje a odstraní zákaznická data. *Dodatek 1 - Operace zpracování (str. 32* Při uplynutí nebo ukončení doby účinnosti užívání služeb online vývozcem údajů může vývozce údajů extrahovat zákaznická data a dovozce údajů odstraní zákaznická data, a to v souladu s podmínkami služeb online platnými pro danou smlouvu. *Soukromí (str. 10)* Nejpozději 180 dní od uplynutí doby účinnosti nebo ukončení používání služby online zákazníkem společnost Microsoft účet deaktivuje a odstraní z něj zákaznická data.
Článek 28, odst. 4	Zpracování dalším zpracovatelem	Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení. Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení POS:** *Použití dodavatelů (str. 8)* Společnost Microsoft může najmout subdodavatele za účelem poskytování služeb jejím jménem. Tito subdodavatelé budou smět zákaznická data získat pouze za účelem poskytování služeb, k jejichž poskytování se zavázali, a nebudou smět tato data používat za jakýmkoli jiným účelem. Společnost Microsoft zůstává odpovědná za dodržování souladu s povinnostmi stanovenými v těchto podmínkách služeb online svými subdodavateli. Zákazník již dříve souhlasil s tím, že společnost Microsoft smí přenést zákaznická data k subdodavatelům podle popisu v těchto podmínkách pro služby online. *Soukromí – Předávání subdodavatelům (str. 11)* Společnost Microsoft může najmout subdodavatele za účelem poskytování určitých omezených nebo pomocných služeb jejím

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			jménem. Subdodavatelé, kterým společnost Microsoft předává zákaznická data, i ta používaná pro účely uchovávání, uzavřou se společností Microsoft písemné dohody, které nabízejí stejnou ochranu jako podmínky zpracování údajů. Zákazník již dříve souhlasil s tím, že společnost Microsoft smí předávat zákaznická data subdodavatelům podle popisu v těchto podmínkách zpracování údajů. Není-li v podmínkách zpracování údajů stanoveno jinak, nebo pokud zákazník nesvolí jinak, společnost Microsoft nebude předávat jakékoli třetí straně (a to ani za účelem ukládání) osobní údaje, které zákazník poskytne společnosti Microsoft prostřednictvím užívání služeb online. Společnost Microsoft poskytuje web, který uvádí subdodavatele oprávněné k přístupu k zákaznickým datům ve službách online i omezené nebo pomocné služby, které poskytují. Minimálně 6 měsíců před poskytnutím oprávnění novému subdodavateli k přístupu k zákaznickým datům společnost Microsoft tento web aktualizuje a poskytne zákazníkovi mechanismus k obdržení upozornění na tuto aktualizaci. Pokud zákazník nového subdodavatele neschválí, může dotčenou službu online ukončit bez postihu, a to předložením písemné výpovědi před koncem informační lhůty, která vysvětluje důvody neschválení subdodavatele. Pokud je dotčená služba online součástí sady (nebo podobného jednotlivého nákupu služeb), bude se ukončení vztahovat na celou sadu. Po ukončení společnost Microsoft odstraní platební závazky k ukončeným službám online z následujících faktur zákazníka.
Článek 28, odst. 5, 6, 7 a 8	Kodex chování, osvědčení a standardní smluvní doložky	5. Jedním z prvků, jimiž lze doložit dostatečné záruky podle odstavců 1 a 4 tohoto článku, je skutečnost, že zpracovatel dodržuje schválený kodex chování uvedených v článku 40 nebo schválený mechanismus pro vydávání osvědčení uvedený v článku 42. 6. Aniž jsou dotčeny individuální smlouvy mezi správcem a zpracovatelem, mohou být smlouvy nebo jiné právní akty podle odstavců 3 a 4 tohoto článku založeny zcela nebo částečně na standardních smluvních doložkách podle odstavců 7 a 8 tohoto článku, mimo jiné i v případě, že jsou součástí osvědčení uděleného správci či zpracovateli podle článků 42 a 43. 7. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku	**Vyhodnocení:** V současnosti neexistují schválené kodexy schování, osvědčení či smluvní doložky, na základě kterých bude možno doložit určité povinnosti stanovené v odst. 3 a 4 tohoto článku.

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
		může standardní smluvní doložky stanovit Komise přezkumným postupem podle čl. 93 odst. 2. 8. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky přijmout dozorový úřad v souladu s mechanismem jednotnosti uvedeným v článku 63.	
Článek 28, odst. 9	Písemná smlouva se zpracovatelem	Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně, v to počítaje i elektronickou formu.	**Vyhodnocení:** v souladu s GDPR
Článek 28, odst. 10	Považování zpracovatele za správce	Aniž jsou dotčeny články 82, 83 a 84, pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.	**Vyhodnocení**: V případě, že společnost Microsoft určuje účel a prostředky zpracování, bude považována za správce údajů se všemi závazky a veškerou odpovědnosti vztahující se na správce. V tomto dokumentu nepředpokládáme, že se Microsoft dostane do pozice správce údajů, jelikož společnost Microsoft dle PSO vždy postupuje na základě pokynů zákazníka.
Článek 32, odst. 1	Zabezpečení zpracování	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:	**Vyhodnocení:** v souladu s GDPR S přihlédnutím k širokému rozsahu zabezpečení, které se Microsoft podle PSO zavazuje přijmout a provést, je dle našeho názoru Microsoft v souladu s GDPR co do přijetí vhodných technických a organizačních opatření. Domníváme se, že Microsoft je v souladu s GDPR co do povinnosti provést analýzu rizika, jelikož PSO výslovně stanoví, že Microsoft provedl posouzení rizik. Pro potvrzení, zda k posouzení rizik došlo s „přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování“, může společnost Microsoft pod povinností mlčenlivost poskytnout na požádání zákazníkovi metodiky posouzení rizik a seznam zbytkových rizik. **Relevantní ustanovení PSO:** *Zabezpečení (str. 8)* Prioritou společnosti Microsoft je napomáhat při ochraně bezpečnosti informací zákazníka. Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			Zabezpečení – Obecné postupy (str. 11) Společnost Microsoft implementovala a pro služby online bude v souvislosti se závazky k zabezpečení uvedenými v podmínkách pro služby online udržovat a dodržovat následující bezpečnostní opatření, která představují jedinou odpovědnost společnosti Microsoft s ohledem na zabezpečení zákaznických dat. *Organizace zabezpečení informací – Program řízení rizik (str. 11)* Před zpracováním zákaznických dat nebo spuštěním služeb online společnost Microsoft provedla posouzení rizik. **Relevantní opatření:** Tento obecný požadavek je pokryt všemi organizačními opatřeními uvedenými v kapitole 9 a výběrem relevantních technických opatření uvedených v kapitole 10 provedený na základě hodnocení (analýzy) rizik. Poskytovatel cloudových služeb provádí v rámci nabízených služeb posouzení rizik a na základě jejích výsledků upravuje existující bezpečnostní opatření. Jedná se však o rizika vztažená ke společnosti Microsoft a jí nabízeným službám, která nezohledňují specifický charakter konkrétních dat správce. Správce tedy musí provést vlastní hodnocení rizik, které bude hodnotit úroveň rizik z pohledu správce při zohlednění všech záruk a popsaných bezpečnostních opatření nabízených poskytovatelem cloudových služeb. Opatření: všechna z 9 a výběr z 10
Článek 32, odst. 1, písm. a)	Zabezpečení zpracování	a) pseudonymizace a šifrování osobních údajů;	**Vyhodnocení:** částečně v souladu s GDPR, k doplnění volbou nastavení služby Pro scénáře zpracování elektronické pošty a elektronické formy nestrukturovaných dat či dokumentů, u kterých je třeba zachovat interoperabilitu a přenositelnost mimo hranice organizace zpracovatele i správce (typicky soubory typu .DOCX, .XLSX, PPTX, PDF, JPG atd.), není prakticky proveditelné obecně zavádět pseudonymizaci osobních údajů, které se mohou v těchto souborech vyskytovat. Pseudonymizací by společnost Microsoft zasahovala do integrity zákaznických dokumentů, což by bylo v rozporu s povahou služby.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			Společnost Microsoft se proto zaměřuje na několik úrovní zajištění ochrany a případně i integrity osobních údajů šifrováním osobních údajů, čímž je ochrana osobních údajů nestrukturovaných dat dostatečně zajištěna a zároveň je zachována funkcionalita dokumentů. **Pseudonymizace:** Ačkoliv prostředí Microsoft Office 365 nenabízí automatizované nástroje pro zajištění pseudonymizace, správce údajů (zákazník společnosti Microsoft) má možnost nastavit interní procesy či zajistit řešení na aplikační úrovni takovým způsobem, kdy budou moci být údaje ukládány do prostředí Office 365 pseudonymizované. **Šifrování:** Společnost Microsoft v rámci Office 365 nabízí zabezpečení ochrany osobních údajů šifrováním osobních údajů s využitím kontrolních součtů (tzv. „hash“). Všechny soubory v úložišti SharePoint online a OneDrive for Business jsou vždy defaultně šifrovány způsobem „Per-File Encryption“ (viz dokumentace). Správce může navíc zvolit další vrstvu zabezpečení pomocí služby „Rights Management Services - (RMS)“, která umožňuje řízení přístupu na konkrétní fyzickou osobu, ochranu důvěrnosti šifrováním i zabezpečení integrity kontrolními součty. U služby elektronické pošty Exchange Online se pro přenos osobních údajů nad rámec identifikace odesílatele a příjemce předpokládá rovněž využití zabezpečení technikou RMS. Navíc je v režimu „preview“ k dispozici služba Office 365 Advanced Encryption, která umožní celé mailboxy uživatelů a celé úložiště SharePoint Online a OneDrive for Business zabezpečit šifrováním, kdy správa vrchních přístupových klíčů bude plně pod kontrolou administrátora správce osobních údajů pomocí Microsoft Azure Key Vault. Kromě výše uvedených možností nabízí Exchange Online funkcionalitu „Office 365 Message Encryption“, která umožňuje odeslat uživatelům uvnitř i vně organizace zašifrovanou zprávu, bez ohledu na to jakou emailovou adresu a klienta používají. Zprávy jsou příjemci následně dešifrovány a zobrazeny po zadání jednorázového

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			hesla, nebo po ověření Microsoft nebo Office 365 účtem. Na zprávy je možné aplikovat vlastní úpravy v podobě loga společnosti a dodatečných informací či právních informací. Služba nevyžaduje žádné dodatečné certifikáty, jako veřejný klíč je použita emailová adresa příjemce. Na straně koncového poštovního klienta, například Microsoft Outlook, je možné využít zabezpečení S/MIME které dovoluje podepsání a šifrování e-mailových zpráv na straně odesílatele a jejich dešifrování a verifikaci integrity a ověření zdroje této zprávy na straně příjemce. Služba využívá digitální certifikáty od akreditovaných certifikačních autorit (pro interní využití může být využita interní PKI infrastruktura). Služba Skype for Business využívá k ochraně důvěrnosti hlasových nebo video konferencí tzv. streamingový šifrovaný protokol SRTP. Dále, jak stanoví PSO, společnost Microsoft vždy šifruje údaje při přenosech prostřednictvím veřejných sítí (na transportní vrstvě protokolem HTTPS TLS 1.2). Posouzení, který konkrétní typ nebo kombinaci šifrování v daném případě zvolit, se musí provádět s ohledem na druh a výskyt zpracovávaných osobních údajů. **Relevantní ustanovení PSO:** *Sdělení a správa operací – Data mimo hranice (str. 11)* Společnost Microsoft šifruje nebo umožňuje zákazníkovi šifrovat zákaznická data, která jsou přenášena prostřednictvím veřejných sítí. **Relevantní opatření:** Služba Microsoft Office 365 nabízí mechanizmy pro šifrování osobních (i jiných) údajů jak při uložení, tak i při přenosu. Prostředí Microsoft Office 365 nenabízí nástroje pro zajištění pseudonymizace protože pseudonymizace by zasahovala do integrity dokumentů a byla tak v rozporu s povahou služby. Správce údajů může zavést opatření na aplikační úrovni nebo v rámci interních procesů, kterým pseudonymizaci osobních údajů vkládaných do Office 365 zajistí mimo samotné prostředí Office 365. Opatření: 10.13

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
Článek 32, odst. 1, písm. b)	Zabezpečení zpracování	b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;	**Vyhodnocení:** souladu s GDPR Společnost Microsoft dle našeho názoru zavedla dostatečná opatření, jež činí zpracování údajů na základě PSO v souladu s tímto požadavkem. **Relevantní ustanovení PSO:** Relevantní ustanovení jsou uvedena zejména v tabulce na str. 11–12 PSO. Další ustanovení týkající se zabezpečení zákaznických dat jsou pak stanovena např. v Dodatku č. 2 ke Standardním smluvním doložkám či na str. 8 PSO. **Relevantní opatření:** Tento obecný požadavek je pokryt všemi organizačními opatřeními uvedenými v kapitole 9 a výběrem relevantních technických opatření uvedených v kapitole 10 provedený na základě hodnocení (analýzy) rizik. Opatření: všechna z 9 a výběr z 10
Článek 32, odst. 1, písm. c)	Zabezpečení zpracování	c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Sdělení a správa operací – Postupy obnovení dat (str. 11)* - Společnost Microsoft uchovává průběžně a minimálně jednou týdně (pokud během tohoto období nebyla aktualizována žádná zákaznická data) několik kopií zákaznických dat, ze kterých lze data obnovit. - Společnost Microsoft uchovává kopie zákaznických dat a postupy obnovení dat na jiném místě, než na kterém se nachází primární počítačové vybavení zpracovávající zákaznická data. - Společnost Microsoft využívá konkrétní postupy, kterými se řídí přístup ke kopiím zákaznických dat. - Společnost Microsoft reviduje postupy obnovy dat minimálně každých 6 měsíců, a to s výjimkou postupů obnovy dat pro služby Azure pro státní správu, které jsou revidovány každých 12 měsíců. - Společnost Microsoft protokoluje pokusy o obnovení dat, včetně odpovědné osoby, popisu obnovených dat a případně odpovědné osoby a dále to, která data (pokud existují) bylo nutné během procesu

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			obnovení dat zadat ručně. **Relevantní opatření:** Prostředí Microsoft Office 365 a Microsoft's Cloud Infrastructure and Operations nabízí vysokou úroveň dostupnosti a schopnost se zotavit z výpadku. Opatření: 10.14
Článek 32, odst. 1, písm. d)	Zabezpečení zpracování	d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Zabezpečení (str. 11)* Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením. *Správa incidentů zabezpečení informací – Monitorování služby (str. 12)* Pracovníci zabezpečení společnosti Microsoft ověřují minimálně každých šest měsíců protokoly a v případě potřeby navrhují kroky remediace. **Relevantní opatření:** Prostředí Microsoft Office 365 a Microsoft's Cloud Infrastructure and Operations má zavedený systém řízení bezpečnosti informací v rámci certifikace ISO/IEC 27001. Opatření: 9.1
Článek 32, odst. 2	Zohlednění rizik	Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.	**Vyhodnocení:** v souladu s GDPR Microsoft před zpracováním zákaznických dat provedl posouzení rizik. Dle našeho názoru ustanovení PSO stanoví dostatečná opatření pro zajištění souladu s GDPR co do zajištění bezpečnosti dat. Zákazník (správce) by však měl (viz „Relevnantí opatření“ níže) sám provést zhodnocení rizik ve vztahu ke konkrétním údajům, které se v rámci

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			Office 365 budou zpracovávat pro účely daného zákazníka. **Relevantní ustanovení PSO:** *Zabezpečení (str. 8)* Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením. *Organizace zabezpečení informací – Program řízení rizik (str. 11)* Před zpracováním zákaznických dat nebo spuštěním služeb online společnost Microsoft provedla posouzení rizik. **Relevantní opatření:** Poskytovatel cloudových služeb provádí v rámci nabízených služeb posouzení rizik a na základě jejích výsledků upravuje existující bezpečnostní opatření. Jedná se však o rizika vztažená ke společnosti Microsoft a nabízeným službám, která nezohledňují specifický charakter konkrétních dat správce. Správce tedy musí provést vlastní hodnocení rizik, které bude hodnotit úroveň rizik z pohledu správce při zohlednění všech záruk a popsaných bezpečnostních opatření nabízených poskytovatelem služeb. Opatření: 9.2
Článek 32, odst. 3	Kodex chování	Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.	**Vyhodnocení:** Kodexy chování ani osvědčení zatím nebyly vydány.
Článek 32, odst. 4	Zpracování osobních údajů pouze na pokyn správce	Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.	**Vyhodnocení:** v souladu s GDPR **Relevantní ustanovení PSO:** *Úmysl stran (str. 10)* V případě služeb online představuje společnost Microsoft zpracovatele (nebo dílčího zpracovatele) údajů, který zastupuje zákazníka. Jako

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			zpracovatel (nebo dílčí zpracovatel) údajů bude společnost Microsoft jednat na základě pokynů zákazníka. Podmínky pro služby online a multilicenční smlouva zákazníka (včetně podmínek a ujednání začleněných do nich odkazem) společně se zákazníkovým užíváním a konfigurací funkcí služeb online představují úplné a konečné pokyny zákazníka pro společnost Microsoft ohledně zpracování zákaznických dat. Jakékoli další nebo alternativní pokyny musí být dohodnuty v souladu s procesem doplnění multilicenční smlouvy zákazníka. *Pracovníci společnosti Microsoft (str. 10)* Pracovníci společnosti Microsoft nebudou zákaznická data zpracovávat bez svolení zákazníka. Pracovníci společnosti Microsoft musí zákaznická data uchovávat v bezpečí a v tajnosti tak, jak je popsáno v podmínkách zpracování údajů, a tato povinnost platí i po ukončení jejich závazků. **Relevantní opatření:** Opatření: 9.5

Vzhledem k tomu, že GDPR nabývá účinnosti až od 25.května 2018, je společnost Microsoft nyní v procesu svého vlastního auditu souladu svých produktů a smluvních podmínek s požadavky této budoucí legislativy. Do roku 2018 může dojít k některý změnám smluvních podmínek nebo produktů společnosti Microsoft souvisejících s požadavky GDPR. Společnost Microsoft se však již nyní ve svých smluvních podmínkách zavazuje zajistit soulad svých produktů (včetně služby Office 365) a smluvních podmínek s platnou legislativou, tedy včetně GDPR. Tento smluvní závazek se vztahuje specificky i na právní úpravu oznámení narušení bezpečnosti (Sekce „Obecné podmínky“, odstavec „Dodržování zákonů“: „Společnost Microsoft dodrží veškeré zákony a předpisy, které se vztahují k provozování služeb online, včetně zákonů týkajících se oznámení narušení bezpečnosti“).

7.2 ZÁKON Č. 101/2000 SB., O OCHRANĚ OSOBNÍCH ÚDAJŮ

Jedná se o zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Tento zákon definuje následující požadavky na poskytovatele cloudových služeb v roli zpracovatele osobních údajů:

Tab. 3 Požadavky zákona č. 101/2000 Sb, o ochraně osobních údajů a jejich pokrytí dle PSO

ID požadavku	**Stručný popis**	**Podrobnější popis** (znění právního předpisu)	**Popis pokrytí**
§ 6	Smlouva se zpracovatelem	Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.	**Vyhodnocení**: v souladu se zákonem Pro bližší posouzení vizte analýzu souladu smluvní dokumentace s článkem 28 GDPR, konkrétně s článkem 28 odst. 3, a dále s článkem 32 GDPR. **Relevantní ustanovení PSO:** *Podmínky zpracování dat (str. 9)* (…) podmínky v multilicenční smlouvě zákazníka, včetně podmínek zpracování údajů, představují smlouvu o zpracování údajů, podle které je společnost Microsoft zpracovatelem údajů; a (…)
	Smlouva se zpracovatelem – náležitosti	(…) v jakém rozsahu, za jakým účelem (…)	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Definice (str. 4)* „Zákaznická data“ označují všechna data včetně veškerých textových, zvukových, video nebo obrazových souborů a softwaru poskytnutých společnosti Microsoft zákazníkem či jeho afilacemi, případně jejich jménem, během používání služby online ze strany zákazníka. *Použití zákaznických dat (str. 7)* Zákaznická data budou použita pouze pro poskytování služeb online zákazníkovi, včetně účelů kompatibilních s poskytováním těchto služeb. *Úmysl stran (str. 10)* V případě služeb online představuje společnost Microsoft zpracovatele (nebo dílčího zpracovatele) údajů, který zastupuje zákazníka. Jako zpracovatel (nebo dílčí zpracovatel) údajů bude společnost Microsoft jednat na základě pokynů zákazníka. Podmínky pro služby online a

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
			multilicenční smlouva zákazníka (včetně podmínek a ujednání začleněných do nich odkazem) společně se zákazníkovým užíváním a konfigurací funkcí služeb online představují úplné a konečné pokyny zákazníka pro společnost Microsoft ohledně zpracování zákaznických dat. Jakékoli další nebo alternativní pokyny musí být dohodnuty v souladu s procesem doplnění multilicenční smlouvy zákazníka. *Rozsah a účel zpracování údajů (str. 11)* Rozsah a účel zpracování zákaznických dat, včetně jakýchkoli osobních údajů obsažených v zákaznických datech, je popsán v podmínkách zpracování údajů a v multilicenční smlouvě zákazníka.
	Smlouva se zpracovatelem – náležitosti	(…) na jakou dobu (…)	**Vyhodnocení**: v souladu se zákonem *Trvání a objekt zpracování údajů (str. 10)* Údaje budou zpracovávány po dobu určenou v multilicenční smlouvě zákazníka. Cílem zpracovávání údajů je výkon služeb online. *Dodatek 1 (str. 32)* Data budou zpracovávána po dobu uvedenou v příslušné multilicenční smlouvě uzavřené mezi vývozcem údajů a právnickou osobou společností Microsoft, ke které jsou přiloženy tyto standardní smluvní doložky („Microsoft“). Cílem zpracovávání údajů je výkon služeb online.
	Smlouva se zpracovatelem – náležitosti	(…) musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.	**Vyhodnocení**: v souladu se zákonem Viz posouzení článku 32 GDPR výše.
§ 8	Porušení povinnosti správcem	Jestliže zpracovatel zjistí, že správce porušuje povinnosti stanovené tímto zákonem, je povinen jej na to neprodleně upozornit a ukončit zpracování osobních údajů. Pokud tak neučiní, odpovídá za škodu, která subjektu údajů vznikla, společně a nerozdílně se správcem údajů. Tím není dotčena jeho odpovědnost podle tohoto zákona.	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Zásady přijatelného užívání (str. 5)* Ani zákazník, ani uživatelé, kteří přistupují ke službě online prostřednictvím zákazníka, ji nesmějí používat: (…) • způsobem, který je zakázán zákonem, předpisem, vládním nařízením

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	**Popis pokrytí**
			či vyhláškou, (…). Porušení podmínek tohoto oddílu může mít za následek pozastavení služby online. Společnost Microsoft pozastaví službu online pouze v přiměřeně nutném rozsahu. Společnost Microsoft oznámí pozastavení služby online předem s výjimkou případů, kdy bude mít důvod se domnívat, že je službu nutné pozastavit okamžitě. *Dodržování zákonů (str. 5)* Společnost Microsoft dodrží veškeré zákony a předpisy, které se vztahují k provozování služeb online, včetně zákonů týkajících se oznámení narušení bezpečnosti.
§ 13, odst. 1	Přijetí opatření proti neoprávněnému zpracování osobních údajů	Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Zabezpečení (str. 8)* Prioritou společnosti Microsoft je napomáhat při ochraně bezpečnosti informací zákazníka. Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením. *Zabezpečení (str. 11)* Obecné postupy. Společnost Microsoft implementovala a pro služby online bude v souvislosti se závazky k zabezpečení uvedenými v podmínkách pro služby online udržovat a dodržovat následující bezpečnostní opatření, která představují jedinou odpovědnost společnosti Microsoft s ohledem na zabezpečení zákaznických dat. Bližší specifikace viz tabulka na str. 11–12 *Dodatek 2 (str. 33)* Technická a organizační opatření. Dovozce údajů implementoval a bude udržovat příslušná technická a organizační opatření, interní kontroly a rutiny zabezpečení informací určené k ochraně zákaznických dat definovaných v podmínkách zpracování údajů před náhodnou ztrátou,

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	**Popis pokrytí**
			zničením či změnou, neoprávněným zveřejněním nebo přístupem a před neoprávněným zničením, a to následovně: Technická a organizační opatření, interní kontroly a rutiny zabezpečení informací popsané v podmínkách zpracování údajů jsou tímto začleněny do tohoto dodatku 2 tímto odkazem a jsou závazné pro dovozce údajů, jako by byly všechny uvedeny v tomto dodatku 2.
§ 13, odst. 2	Dokumentace opatření	Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Organizace zabezpečení informací (str. 11)* Poté, co bezpečnostní dokumenty společnosti Microsoft již nebudou platit, je společnost uchová v souladu se svými požadavky na uchovávání. *Sdělení a správa operací (str. 11)* Společnost Microsoft uchovává bezpečnostní dokumenty popisující její bezpečnostní opatření a relevantní postupy a odpovědnosti jejích pracovníků. **Relevantní opatření:** Poskytovatel cloudových služeb svoje zavedená bezpečnostní opatření dokumentuje – viz dokumenty odkazované v kapitole 9 nebo dokumenty uvedené v [1], kapitola 9.
§ 13, odst. 3	Posuzování rizik	V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům, b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování, c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.	**Vyhodnocení**: v souladu se zákonem Microsoft před zpracováním zákaznických dat provedl posouzení rizik. Společnost Microsoft v oblastech, za které odpovídá výhradně, implementovala a nadále udržuje systém bezpečnostních opatření, které jsou na vysoké úrovni (v souladu se standardy řady ISO/IEC 27000, auditní zprávou systému řízení podle ISO/IEC 27001 a auditními zprávami SOC 1 a SOC 2, typ II). V ostatních oblastech nabízí množinu (zejména technických) bezpečnostních opatření, která umožní dosáhnout obdobné úrovně bezpečnosti; o výběru a implementaci těchto opatření však rozhoduje sám zákazník. Dle našeho názoru ustanovení PSO stanoví obecně dostačující opatření

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	**Popis pokrytí**
			pro zajištění souladu se zákonem. **Relevantní ustanovení PSO:** *Zabezpečení (str. 8)* Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením. *Organizace zabezpečení informací – Program řízení rizik (str. 11)* Před zpracováním zákaznických dat nebo spuštěním služeb online společnost Microsoft provedla posouzení rizik. **Relevantní opatření:** Poskytovatel cloudových služeb provádí v rámci nabízených služeb posouzení rizik a na základě jejích výsledků upravuje existující bezpečnostní opatření. Jedná se však o rizika vztažená ke společnosti MS a nabízeným službám, která nezohledňují specifický charakter konkrétních dat správce. Správce tedy musí provést vlastní hodnocení rizik, které bude hodnotit úroveň rizik z pohledu správce při zohlednění všech záruk a popsaných bezpečnostních opatření nabízených poskytovatelem služeb. Opatření: 9.2

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
§ 13, odst. 4	Opatření pro automatizované zpracování osobních údajů	V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Organizace zabezpečení informací (str. 11)* Vlastnictví zabezpečení. Společnost Microsoft určila jednoho nebo více pracovníků zabezpečení odpovědných za koordinaci a monitorování pravidel a postupů zabezpečení. Role a povinnosti v otázce zabezpečení. Pracovníci společnosti Microsoft s přístupem k zákaznickým datům jsou vázáni závazky důvěrnosti. *Řízení přístupu (str. 12)* Zásady přístupu. Společnost Microsoft uchovává záznam o oprávnění zabezpečení osob, které mají přístup k zákaznickým datům. Společnost Microsoft uchovává a aktualizuje záznam pracovníků oprávněných k přístupu k systémům společnosti Microsoft, které obsahují zákaznická data. Společnost Microsoft omezuje přístup k zákaznickým datům pouze na osoby, které tento přístup vyžadují k vykonávání své funkce. Společnost Microsoft používá opatření k zabránění osobám v získání přístupových práv, která jim nebyla udělena, k získání přístupu k zákaznickým datům, pokud k tomuto přístupu nemají oprávnění. **Relevantní opatření:** V prostředí Microsoft Office 365 a Microsoft's Cloud Infrastructure and Operations jsou nasazeny mechanizmy identifikace a autentizace. Opatření: 10.6
	Opatření pro automatizované zpracování osobních údajů	b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,	**Vyhodnocení**: v souladu se zákonem Viz posouzení souladu s § 13 odst. 4 písm. a) zákona. **Relevantní opatření:** Opatření: 10.7

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
	Opatření pro automatizované zpracování osobních údajů	c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 12)* Společnost Microsoft protokoluje nebo umožňuje zákazníkovi protokolovat informační systémy obsahující zákaznická data, která registrují ID přístupu, čas, přidělené nebo zamítnuté oprávnění a příslušnou činnost, a k těmto informačním systémům přistupovat a používat je. *Řízení přístupu (str. 12)* Společnost Microsoft uchovává záznam o oprávnění zabezpečení osob, které mají přístup k zákaznickým datům. - Společnost Microsoft používá standardní postupy odvětví k identifikaci a ověření uživatelů, kteří se pokusí o přístup do informačních systémů. - Pokud jsou mechanismy ověřování založeny na heslech, společnost Microsoft vyžaduje jejich pravidelné obnovování. - Pokud jsou mechanismy ověřování založeny na heslech, společnost Microsoft vyžaduje, aby heslo obsahovalo alespoň osm znaků. - Společnost Microsoft zajišťuje, že deaktivovaná ID nebo ID s ukončenou platností nejsou přidělena dalším osobám. - Společnost Microsoft monitoruje nebo umožní zákazníkovi monitorovat opakované pokusy o získání přístupu k informačnímu systému pomocí neplatného hesla. - Společnost Microsoft udržuje standardní postupy odvětví k deaktivaci hesel, která byla poškozena nebo neúmyslně zveřejněna. - Společnost Microsoft používá standardní postupy ochrany hesel odvětví, včetně postupů určených k zachování důvěrnosti a integrity hesel při přiřazování nebo distribuci a během uchovávání.

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	Popis pokrytí
			Relevantní opatření: V prostředí Microsoft Office 365 a Microsoft's Cloud Infrastructure and Operations jsou nasazeny mechanizmy záznamu činnosti. Opatření: 10.9
	Opatření pro automatizované zpracování osobních údajů 4 – řízení přístupu	d) zabránit neoprávněnému přístupu k datovým nosičům.	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Inventář prostředků (str. 11)* Společnost Microsoft udržuje inventář všech médií, na kterých jsou uchovávána zákaznická data. Přístup k inventářům těchto médií je přísně omezen na pracovníky společnosti Microsoft, kteří tento přístup získali na základě písemného pověření. *Zpracovávání prostředků (str. 11)* Společnost Microsoft klasifikuje zákaznická data za účelem usnadnění jejich identifikace a příslušného omezení přístupu k nim. Společnost Microsoft určila omezení pro tištěná zákaznická data a využívá postupy pro likvidaci tištěných materiálů, které zákaznická data obsahují. Pracovníci společnosti Microsoft musí před uložením zákaznických dat na přenosných zařízeních, vzdáleným přístupem k zákaznickým datům nebo zpracováním zákaznických dat mimo zařízení společnosti Microsoft získat od společnosti Microsoft oprávnění. *Fyzické zabezpečení (str. 11)* Fyzický přístup do zařízení. Společnost Microsoft omezuje přístup do zařízení, ve kterých se nacházejí informační systémy zpracovávající zákaznická data, na identifikované oprávněné osoby. Fyzický přístup ke komponentám. Společnost Microsoft uchovává záznamy o příchozích a odchozích médiích obsahujících zákaznická data, včetně typu média, autorizovaného odesilatele a příjemců, data a času, počtu médií a typů zákaznických dat, které obsahují. **Relevantní opatření:**

ID požadavku	Stručný popis	**Podrobnější popis** (znění právního předpisu)	**Popis pokrytí**
			V prostředí Microsoft Office 365 a Microsoft's Cloud Infrastructure and Operations jsou nasazeny mechanizmy řízení přístupu a mohou být nasazeny mechanizmy šifrování. Opatření: 10.4, 10.7, 10.13
§ 27, odst. 2–3	Předání údajů do třetích zemí	2) Do třetích zemí mohou být osobní údaje předány, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament souhlas, a kterou je Česká republika vázána,[1a]) nebo jsou osobní údaje předány na základě rozhodnutí orgánu Evropské unie. Informace o těchto rozhodnutích zveřejňuje Úřad ve Věstníku. (3) Není-li podmínka podle odstavců 1 a 2 splněna, může být předání osobních údajů uskutečněno, jestliže správce prokáže, že … b) jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo pokud smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu, …	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:** *Soukromí (str. 10)* Pokud se zákazník neodhlásil ze standardních smluvních doložek, bude se veškerý přenos zákaznických dat z Evropské unie, Evropského hospodářského prostoru a Švýcarska řídit standardními smluvními doložkami. Společnosti Microsoft se bude řídit požadavky Evropského hospodářského prostoru a švýcarského zákona o ochraně dat ohledně shromažďování, používání, přenosu, uchovávání a dalšího zpracování osobních údajů z Evropského hospodářského prostoru a Švýcarska. **Relevantní opatření:** Součástí všeobecné obchodní podmínky: Volume Licensing – Podmínky pro služby online, je standardní smluvní doložka pro zpracovatele. Předávání se tedy provádí na základě této smluvní doložky. Kromě toho může správce zvolit ukládání údajů výhradně v zemích EHP/EU. Opatření: 9.5

7.3 ZÁKON Č. 181/2014 SB. A NÁVAZNÁ VYHLÁŠKA Č. 316/2014 SB.

Studie neobsahuje podrobnou analýzu naplnění požadavků ZoKB/VoKB neboť této oblasti je věnovaná samostatná studie Protecting Data in Microsoft Online Services (Studie zpracovaná na základě poptávky Microsoft s.r.o.) – viz [1], na kterou tímto odkazujeme.

Skutečnost, že jednotlivé oblasti požadované ZoKB/VoKB jsou pokryty bezpečnostními opatřeními, vyplývá z vlastního obsahu kapitol 9 a 10.

8 MODELOVÁ POSOUZENÍ VLIVU NA OCHRANU OSOBNÍCH ÚDAJŮ

Tato kapitola obsahuje modelová posouzení vlivu na ochranu osobních údajů pro scénáře popsané v kapitole 6.

Při provádění posouzení pro konkrétní případ mohou správci osobních údajů využívající produkt Microsoft Office 365 využít tato modelová posouzení jako podklad, ze kterého mohou vycházet. V tomto modelovém posouzení jsou pokryta rizika, která lze zajistit a zabezpečit ze strany společnosti Microsoft jako zpracovatele osobních údajů v Office 365. V modelovém zpracování jsou však kromě toho předjímána také rizika, která musí být vyhodnocena každým správcem samostatně na úrovni organizace správce s ohledem na konkrétní povahu, rozsah, kontext a účely zpracování osobních údajů. Níže na tato rizika upozorňujeme.

Vzhledem ke skutečnosti, že se jedná o modelové posouzení vlivu na ochranu osobních údajů a nikoliv posouzení vlivu pro konkrétní případ zpracování u konkrétního správce osobních údajů, je v tomto posouzení pracováno s následujícími předpoklady:

Předpoklad 1:

Analýza rizik provedená v rámci každého posouzení se vzhledem ke skutečnosti, že jsou analyzována rizika z pohledu subjektu údajů, zaměřuje v rámci služeb Microsoft Office 365 na rizika spojená s konkrétním porušením zabezpečení osobních údajů (porušením důvěrnosti, integrity a dostupnosti), tedy na případy, které mohou mít dopad na konkrétní subjekt údajů.

Rizika správce spojená se zpracováním osobních údajů jsou v tomto modelovém posouzení zahrnuta co do posouzení zabezpečení osobních údajů podle článků 28 a 32 GDPR. Ostatní rizika správce jsou v této analýze zohledněna pouze formou navržených kategorií rizik ke zhodnocení a doplnění ze strany správce. Příslušné kombinace aktiva, hrozby (a případně zranitelnosti) jsou v následujích kapitolách zmíněny pro upozornění správce, která další rizika musí samostatně zohlednit nad rámec tohoto posouzení.

Podobně, vzhledem k vymezení rizik nejsou analyzována specifická rizika regulatorního nesouladu pro správce nebo poskytovatele cloudových služeb v roli zpracovatele, neboť tato rizika nemají na subjekt údajů dopad. Je však analyzováno obecné riziko porušení zabezpečení osobních údajů a regulatorního nesouladu v důsledku aktivity nebo naopak nečinnosti poskytovatele.

Předpoklad 2:

Uvedené způsoby zpracování a účely zpracování jsou vzorové a nemusí přímo odpovídat způsobu zpracování a účelům zpracování jednotlivých organizací (správců).

Předpoklad 3:

U rizik, jejichž snížení nezávisí výhradně na opatřeních správce, ale na kombinaci opatření poskytovatele cloudových služeb a opatření u správce, je předpokládáno, že opatření správce nesnižují úroveň opatření poskytovatele cloudových služeb.

Příkladem mohou býti rizika spojená s hrozbou „Vydávání se za někoho jiného interními pracovníky“, kde kromě mechanizmů identifikace, autentizace a autorizace je nezbytné i organizačně zajistit správnou správu autentizačních informací (například, že nebude používán jeden sdílený účet a heslo). Tuto oblast nemůže pokrýt poskytovatel cloudových služeb a zároveň nedostatky v této oblasti mohou výrazně degradovat jinak silná a odpovídající bezpečností opatření.

Další předpoklady jsou uvedeny u konkrétních scénářů.

8.1 DPIA PRO SCÉNÁŘ 1 – SHAREPOINT ONLINE

V případě tohoto scénáře je kromě výše uvedených předpokladů navíc počítáno s následujícími dodatečnými předpoklady:

Předpoklad 4:

U uvedeného systému postaveného nad SharePoint Online není předpokládána interoperabilita v rámci národního systému eHealth.

Předpoklad 5:

Bezpečnost přístupu externích pracovníků přistupujících k osobním údajům (zahrnující i nastavení potřebné úrovně zabezpečení) bude zajištěna na úrovni organizačních opatření mezi správcem a externím pracovníkem resp. subjektem tohoto pracovníka zastřešujícím.

To například zahrnuje zajištění bezpečnosti pracovní stanice, ze které externí pracovník přistupuje na osobní údaje.

8.1.1 ROZSAH DPIA

8.1.1.1 POPIS HODNOCENÉHO PROCESU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Vymezení správce a typu zpracovávaných údajů

Správcem v rámci tohoto zpracování osobních údajů bude ambulantní zdravotnické zařízení (o více než jednom lékaři), které v rámci služby SharePoint Online vytváří, ukládá a zpracovává

- seznam pacientů včetně jejich kontaktů, záznamů o návštěvách a poznámek (zpráv) z vyšetření a
- dokumenty obsahující zprávy nebo potvrzení o zdravotním vyšetření (vstupní prohlídky) pro zaměstnavatele.

Správce tedy zpracovává osobní údaje a citlivé (osobní) údaje podle ZoOOÚ.

Účel zpracování

Zpracování osobních údajů bude probíhat výhradně za účelem poskytování zdravotní péče v potřebné kvalitě (vedení záznamů o pacientovi, komunikace s pacientem).

Při tomto zpracování budou použity následující tituly zpracování:

- preventivní nebo pracovní lékařství, posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní péče či léčby,
- plnění právní povinnosti, a to konkrétně vedení podkladů[2] pro zdravotnickou dokumentaci,
- ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (kontaktní údaje telefonní číslo a e-mail) a
- souhlas udělený subjektem údajů[3] (pro případy, které nespadají pod výše uvedené tituly, zejména pod GDPR, článek 9, odstavec 2, bod h).

[2] Tato studie předpokládá, že ve službě SharePoint Online jsou zpracovávány pouze podklady zdravotnické dokumentace a nikoliv zdravotnická dokumentace samotná; tato je souběžně vedena buď v papírové podobě nebo i v elektronické podobě (v externím systému).
[3] V uvedeném případě musí správce vlastními prostředky zajistit zajištění souhlasu a jeho další správu.

Popis operací zpracování

Osobní údaje budou zpracovávány (vytvářeny, upravovány a čteny) výhradně v rámci činnosti poskytování zdravotní péče, a to jak při osobní návštěvě pacienta, tak i při konzultaci prostřednictvím telefonu nebo jiného kanálu; údaje však budou vždy dostupné výhradně v rámci prostředí správce.

Dále budou osobní údaje zpracovávány v rámci vytváření výpisu ze zdravotnické dokumentace či kopií zdravotnické dokumentace celé a nebo při nahlížení v souladu se zákonem č. 372/2011 Sb., o zdravotních službách, a to buď prostřednictvím pracovníků správce nebo přímým přístupem.

Kromě výše uvedeného běžného zpracování osobních údajů bude probíhat vyřazování zdravotnické dokumentace formou skartačního řízení.

Jiné operace zpracování nebudou povoleny.

Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů[4]

Správce v rámci nezbytnosti a přiměřenosti řádně vyhodnotil rizika, že by zpracování mohlo omezit práva subjektů údajů jakož i výhody a dodatečné záruky, které zpracování pro práva subjektů údajů přináší. Správce dospěl při tomto vyhodnocení k závěru, že zpracování je prováděno pouze v rámci původního účelu a nijak nezasahuje do práv a oprávněných zájmů subjektů údajů.

Správce pečlivě vyhodnotil a buď produktovým nastavením či v rámci smluvních podmínek sjednaných se zpracovatelem zajistil, že všechna zákonná práva subjektů údajů zůstanou zpracováním nedotčena. Správce považuje za důležité, že zpracovatel poskytl v kapitole „Použití zákaznických dat“ PSO smluvní záruky, že zpracovávaná „data budou použita jen pro vlastní poskytování služby zákazníkovi“, že zpracovatel „nebude zákaznická data využívat ani z nich nebude odvozovat informace pro žádné reklamní či podobné komerční účely“ a že zpracovatel „nezískává k zákaznickým datům žádná práva s výjimkou práv, která společnosti Microsoft přidělí zákazník pro poskytování služeb online zákazníkovi.“

Zpracování na druhou stranu přináší následující výhody a dodateční záruky pro subjekty údajů spočívající v zajištění důvěrnosti, integrity a dostupnosti zpracovávaných údajů a odolnosti systémů a služeb zpracování, a to jak na technické, tak i na organizační úrovni.

Bezpečnostní požadavky

Technologie zajišťující uvedené zpracování dat budou splňovat následující minimání bezpečnostní požadavky:

- pokrytí explicitních požadavků GDPR a ZoOOÚ – viz kapitola 8.1.1.5,
- identifikace a autentizace všech osob přistupujících k datům,
- řízení přístupu k datům dle rolí,
- šifrování přenosů dat přes nedůvěryhodné prostředí,
- zajištění integrity uložených dat (jejich ochrany) před poškozením v důsledku akce neoprávněné osoby,
- zajištění integrity uložených dat (jejich ochrany) před poškozením v důsledku chyby hardware,
- audit všech přístupů na údaje a možnost prohlížení těchto záznamů o přístupech a
- cíl dostupnosti: RPO maximálně 5 minut a RTO maximálně 1 hodina.

[4] Jedná se zde o vzorový text, který musí daný správce upravit dle svojí skutečné situace.

Přístup k údajům

K údajům budou mít přístup

- pracovníci správce, přičemž přístup je rozdělen dle následujících rolí:
  - administrativní personál – obecné osobní údaje,
  - zdravotnický personál – všechny údaje (obecné osobní údaje a citlivé osobní údaje)
- externí pracovníci (zdravotnický personál) při nahlížení v souladu se zákonem č. 372/2011 Sb.

Pacient (subjekt údajů) bude mít k údajům přístup pouze prostřednictvím pracovníků správce.

Zpřístupnění údajů

Údaje budou sdílené výhradně v rámci plnění povinností dle zákonač. 372/2011 Sb., o zdravotních službách (vytváření výpisu ze zdravotnické dokumentace, vytváření kopie zdravotní dokumentace nebo nahlížení do dokumentace).

8.1.1.2 POPIS HODNOCENÉHO INFORMAČNÍHO SYSTÉMU NEBO SLUŽBY

Základní popis logické a fyzické architektury

Posuzovaný informační systém se bude skládat z následujících částí:

- pracovní stanice správce (lékaře, administrativního pracovníka) nebo externího pracovníka vybavené OS, prohlížečem a kancelářským software MS Office,
- komunikačních linek (LAN, internet),
- služeb SharePoint Online, konkrétně
  - zpracování uložených dokumentů, seznamů a dat pomocí aplikací vyvinutých pro prostředí SharePoint Online,
  - uložení dokumentů do dokumentových knihoven a sdílený přístup k nim,
- služeb Azure, konkrétně služeb Azure AD pro správu uživatelů Office 365.

Pracovní stanice a komunikační linky LAN správce se budou nacházet v prostorách správce, ostatní části budou mimo tyto prostory nebo dokonce mimo Českou republiku.

Struktura zpracovávaných informací

Všechny zpracovávané informace budou primárně uloženy v rámci služby SharePoint Online a to konkrétně

- v rámci aplikace pro evidenci pacientů (subjektu údajů), jejich kontaktních údajů a návštěv
  - jméno, popřípadě jména, příjmení pacienta,
  - datum narození, rodné číslo, číslo pojištěnce veřejného zdravotního pojištění a kód zdravotní pojišťovny,
  - adresa místa trvalého pobytu,
  - e-mail a telefon,
  - naplánované a proběhlé termíny schůzek,
- v rámci jednotlivých nestrukturovaných dokumentů obsahujících záznamy o vyšetření nebo obsahujících vystavená potvrzení (kancelářské dokumenty, obrázky, videa, …).

Popis datových toků

Při zpracování údajů v informačním systému budou existovat následující datové toky:

- Pro strukturované osobní údaje (v rámci aplikace pro evidenci pacientů)
  - Pracovník správce (uživatel) vkládá strukturované osobní údaje do služby SharePoint Online, která tyto informace ukládá do interního uložiště služby.
  - Pracovník správce (uživatel) čte strukturované osobní údaje ze služby SharePoint Online, která tyto informace získává z interního uložiště služby.
  - Pracovník správce (uživatel) upravuje strukturované osobní údaje ve službě SharePoint Online, která tyto informace mění v interním uložišti služby.
  - Pracovník správce (uživatel) odstraňuje v rámci vyřazování strukturované osobní údaje ze služby SharePoint Online, která tyto informace odstraňuje z interního uložiště služby.
- Pro nestrukturované osobní údaje
  - Pracovník správce (uživatel) vkládá nestrukturované osobní údaje a citlivé (osobní) údaje do služby SharePoint Online, která tyto informace ukládá do interního uložiště služby ve formě jednotlivých dokumentů.
  - Pracovník správce (uživatel) nebo externí pracovník čte nestrukturované osobní údaje a citlivé (osobní) údaje ze služby SharePoint Online, která tyto informace získává z interního uložiště služby ve formě jednotlivých dokumentů.
  - Pracovník správce (uživatel) upravuje nestrukturované osobní údaje a citlivé (osobní) údaje ve službě SharePoint Online, která tyto informace mění v interním uložišti služby ve formě jednotlivých dokumentů.
  - Pracovník správce (uživatel) odstraňuje v rámci vyřazování nestrukturované osobní údaje a citlivé (osobní) údaje ze služby SharePoint Online, která tyto informace odstraňuje z interního uložiště služby ve formě jednotlivých dokumentů.

Popis rozhraní

Ve všech výše uvedených případech budou používána dvě rozhraní:

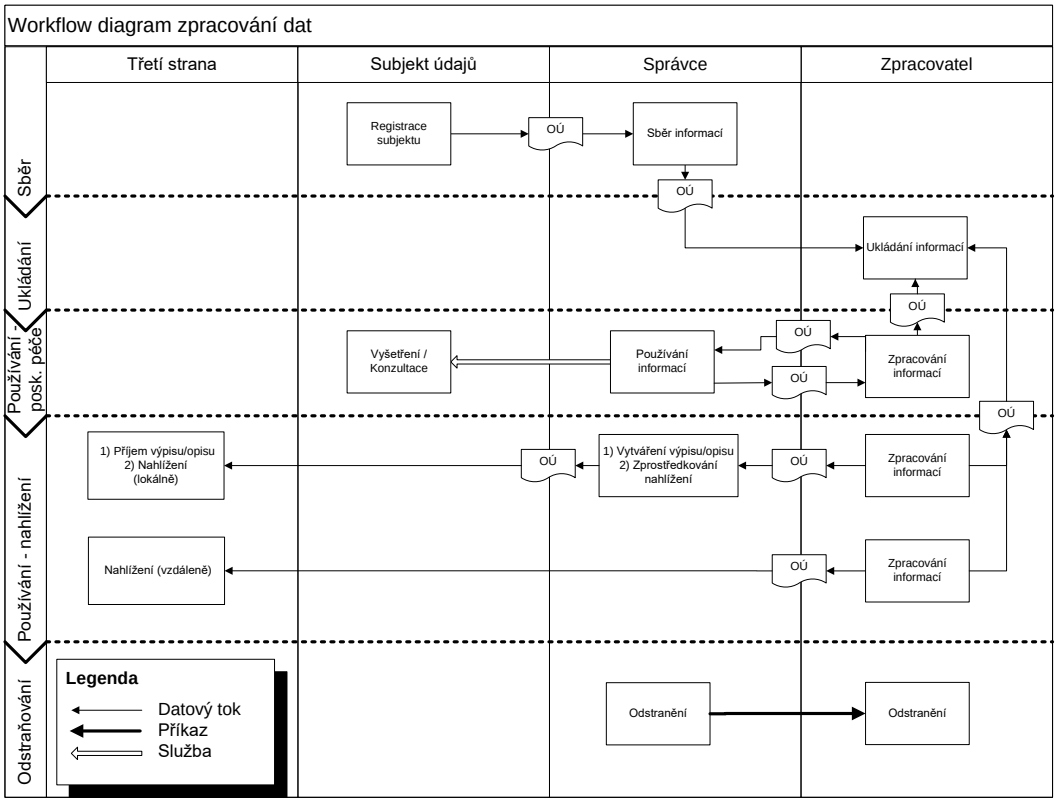
- Uživatelské rozhraní mezi pracovní stanicí a uživatelem ve formě prohlížeče nebo software balíku MS Office.
- Technické rozhraní ve formě rozhraní služby Office 365 SharePoint Online dostupného protokolem HTTPS (HTTP přes TLS).

Podmínkou je autentizace pracovníka správce (uživatele) ke službě Office 365 SharePoint Online.

Workflow diagram zpracování dat

Metody zpracování dat je jsou graficky zobrazeny na následujícím obrázku:

Obr. 1
Workflow diagram pro scénář 1



8.1.1.3 POPIS OPERAČNÍCH POSTUPŮ

Podle [33] je vhodné v rámci DPIA popsat plánované operační postupy správy a používání informačního systému, které mohu mít vliv na bezpečnost osobních údajů, zejména:

- koncept správy interních uživatelů a jejich oprávnění,
- koncept správy externích pracovníků (osob, kterým bylo umožněno nahlédnout do příslušného dokumentu) a jejich oprávnění,
- koncept zajištění výkonu práv subjektu údajů, tedy jakým způsobem bude postupováno v jednotlivých případech, kdy subjekt údajů uplatné své právo[5],
- koncept provozu systému (služby), přičemž zde musí být uvedeno, že část systému je provozována externě, konkrétně v cloudové službě typu SaaS Office 365 SharePoint Online,
- koncept zajištění podpory informačního systému, přičemž zde musí být zejména uvedeny subjekty, které se budou podílet na podpoře informačního systému včetně informací, zdali budou mít přístup k osobním údajům a případně odkud,
- koncept vytváření záznamů o činnosti pracovníků správce, externích pracovníků a pracovníků podpory a vlastního systému (logování) včetně plánů na jejich další uchování,
- plány zálohování a obnovy (které mohou být vzhledem k plánovanému využití cloudové SaaS služby poměrně jednoduché),
- ochrana a správa metadat (pokud existují, což v tomto případě není nezbytné),
- plány na uchování a odstranění dat a likvidaci médií (zohledňující zejména přílohu vyhlášky č. 98/2012 Sb. o zdravotnické dokumentaci),

[5] V prostředí SharePoint Online nabízí provozovatel služby podporu činností spojených s uplatněním práv subjektů v podobě standardních nástrojů typu vyhledávání, eDiscovery a řízení přístupu (například pro případ zablokování přístupu).

- koncept zrušení informačního systému (ukončení smlouvy a případně postup vrácením osobních údajů správci).

Pozn: Vzhledem ke skutečnost, že uvedené oblasti nesouvisí přímo s analyzovanou službou a přitom jsou úzce spojené s konkrétní organizací, je vysoce pravděpodobné, že se budou v závislosti na organizaci správce lišit. V rámci této vzorové DPIA tedy není vypracován plnohodnotný vzor, ale pouze identifikovány doporučené oblasti pro další rozpracování.

8.1.1.4 POPIS INTERAKCE SE SUBJEKTEM ÚDAJŮ

Interakce s pacientem (subjektem údajů) se bude skládat z

- informování subjektu údajů,
- poskytování údajů subjektem údajů (např. v rámci vyšetření nebo konzultací),
- výkonu práv subjektu údajů (přístup k osobním údajům, oprava, výmaz, omezení zpracování a vznesení námitky).

Subjekt údajů bude informován o:

Tab. 4 Oblasti informování subjektu pro scénář 1

Požadavek GDPR	Komentář
Totožnost a kontaktní údaje správce a jeho případného zástupce	
Kontaktní údaje případného pověřence pro ochranu osobních údajů	Tento bod se uplatní dle rozsahu zpracování (jednotlivý lékař nemusí, nemocnice musí).
Účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování	Zpracování osobních údajů probíhá výhradně za účelem poskytování zdravotní péče v potřebné kvalitě (vedení záznamů o pacientovi, komunikace s pacientem). Právním základem (titulem) pro zpracování je: Preventivní nebo pracovní lékařství, posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní péče či léčby. Plnění legislativní povinnosti, a to konkrétně vedení podkladů pro zdravotnickou dokumentaci. Ochrana životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby (kontaktní údaje telefonní číslo a email). Souhlas udělený subjektem údajů (pro případy, které nespadají pod výše uvedené tituly nebo pod GDPR, článek 9, odstavec 2, bod h).
Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);	Pravděpodobně se neuplatní.
Případné příjemce nebo kategorie příjemců osobních údajů	Kromě subjektu údajů a pracovníků správce k údajům mohou mít přístup pouze osoby uvedené v § 65 zákona č. 372/2011 Sb. o zdravotních službách

Požadavek GDPR	Komentář
Případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny	Osobní údaje v případě využití Office 365 jsou předávány do zahraničí na základě článku 46 odst. 2 písm. c) GDPR, tedy na základě Standardních smluvních doložek přijatých Komisí podle čl. 93 odst. 2. Údaje o vhodných zárukách jsou uvedeny v rámci veřejně přístupných PSO, resp. Přílohy č. 2 PSO – Standardních smluvních doložkách.
Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby	Doba uložení a zpracování je daná přílohou č. 3 k vyhlášce č. 98/2012 Sb.
Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů	PSO stanoví v kap. „Použití zákaznických dat“, že správce osobních údajů (zákazník) si zachová všechna práva týkající se zákaznických dat. Z pohledu zpracovatele osobních údajů stanoví PSO v kap. „Přístup k zákaznickým datům“: (1) poskytovat zákazníkovi možnost opravit, odstranit nebo zablokovat zákaznická data, nebo (2) provádět takové opravy, odstranění nebo blokování jménem zákazníka. Správce osobních údajů má za tímto účelem k dispozici nástroje služby Office 365 jako jsou vyhledávání obsahu, eDiscovery (viz [34]), a auditní logy pro změny nebo výmazy obsahu.
Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním	
Existence práva podat stížnost u dozorového úřadu	
Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů	Pravděpodobně se neuplatní
Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů	Pravděpodobně se neuplatní

Výkon práv subjektu údajů bude možné vykonávat stejným způsobem, jakým dochází ke sběru údajů – osobní návštěvou a žádostí u pracovníka správce nebo komunikací s dozorovým úřadem.

8.1.1.5 POŽADAVKY NA SOUKROMÍ A ZABEZPEČENÍ

Explicitní požadavky na soukromí a zabezpečení jsou dané

- zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (aktuálně) a
- nařízením 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 (od 25. 5. 2018).

Další požadavky na zabezpečení vyplývají z analýzy rizik.

8.1.2 ANALÝZA RIZIK

V této kapitole je vypracována vzorová analýza rizik v rámci DPIA, tedy posouzení rizik pro práva a svobody subjektů. Při této analýze rizik je postupováno podle metodiky vycházející z požadavků VoKB, ale upravené v oblasti dopadů tak, aby zohledňovala dopad na subjekt údajů (pacienta) – viz příloha č. 1.

8.1.2.1 KRITÉRIA PRO AKCEPTACI RIZIK

Kritéria pro aceptaci rizik jsou uvedena v příloze 1 (Metodika analýzy rizik), kapitole 3.2. U jednotlivých rizik je uvedena osoba, která může příslušnou úroveň zbytkového rizika akceptovat a zda-li se jedná o vysoké riziko pro práva a svobody fyzických osob dle GDPR, které před zahájením zpracování vyžaduje konzultaci s dozorovým úřadem.

8.1.2.2 AKTIVA A JEJICH HODNOTY

Uložená nejvíce citlivá **datová aktiva** jsou z pohledu důvěrnosti, integrity a dostupnosti **ohodnocena** podle vodítek uvedených v příloze č. 1 hodnotami uvedenými v následující tabulce.

Tab. 5
Ohodnocení dat pro scénář 1

Aspekt	Úroveň	Zdůvodnění
Důvěrnost	Vysoká	Subjekt údajů bude vystaven vážným nepříjemnostem, které bude schopen překonat pouze se značnými obtížemi (zpronevěra finančních prostředků, blacklisting ze strany bank, škody na majetku, ztráta zaměstnání, předvolání k soudu, zhoršení zdravotního stavu, atd.) Zde předpokládán scénář přes dopad na soukromý život – konkrétně odmítnutí zaměstnání.
Integrita	Kritický	Subjekt údajů bude vystaven extrémním nebo nezvratným důsledků, které nemusí být schopen překonat (finanční tíseň spočívající v neschopnosti splácet půjčku, pracovní neschopnost, dlouhodobé psychické nebo fyzické onemocnění, úmrtí atd.) Zde předpokládán scénář poškození záznamů a zptáty infornace o alergiích, což může vést k předepsaní nevhodných léků vedoucímu k závažným komplikacím a v extrémním případě až úmrtí.
Dostupnost	Střední	Subjekt údajů bude vystaven značným nepříjemnostem, které bude schopen za cenu jistých potíží překonat (zvýšení nákladů, odepření služby, strach, nepochopení, stress, malá fyzická újma, atd.). Zde předpokládán scénář předobjednání; kritické případy mohou volat pohotovost.

Aspekt	Úroveň	Zdůvodnění
Ztráta	Vysoká	Subjekt údajů bude vystaven vážným nepříjemnostem, které bude schopen překonat pouze se značnými obtížemi (zpronevěra finančních prostředků, blacklisting ze strany bank, škody na majetku, ztráta zaměstnání, předvolání k soudu, zhoršení zdravotního stavu, atd.). Zde předpokládán scénář ztráty historických záznamů a anamnéz, což může vést ke zhoršení zdravotního stavu.

Nepřímé újmy (např. subjekt utrpí psychickou újmu a následně bude muset podstoupit psychiatrickou léčbu) nemůže správce a ani zpracovatel předjímat a proto tato rizika nejsou zahrnuta.

V následující tabulce je uveden seznam všech identifikovaných aktiv s uvedením jejich popisu spolu s jejich typem podle přílohy č. 1.

Tab. 6
Seznam aktiv pro scénář 1

Typ aktiva	Aktivum	Popis
Datová aktiva	Uložená data	Strukturovaná data využívaná v rámci aplikace pro evidenci pacientů Nestrukturovaná data obsahující údaje o zdravotním stavu pacienta (soubory)
Služby	Služba SharePoint Online	Rozhraní pro zápis a čtení dat v rámci služby SharePoint Online
	Služba Azure AD	Rozhraní pro správu identit, autentizačních údajů a oprávnění

Vlastní ohodnocení identifikovaných aktiv vychází z výše uvedeného ohodnocení dat.

Tab. 7
Ohodnocení aktiv pro scénář 1

Aktivum	Důvěrnost	Integrita	Dostupnost	Ztráta
Uložená	Vysoká	Kritická	Střední	Vysoká
Služba SharePoint Online	Vysoká	Kritická	Střední	-
Služba Azure AD	Střední	Kritická	Střední	-

8.1.2.3 HROZBY A ZRANITELNOSTI

Seznam uvažovaných hrozeb je uveden v příloze č. 1, kapitola 2.2.1.

V případě **ohodnocení úrovní hrozeb** a **zranitelností** jsou hodnoty úrovní uvedeny přímo v tabulkách analýzy rizik (příslušné hodnoty se liší v závislosti na scénáři a aktivu, a proto není možné definovat jednu celkovou úroveň).

V této analýze uvedené hodnoty budou potom v případě konkrétní analýzy rizik IS správce nahrazeny hodnotami vycházejícími z charakteristik prostředí konkrétního správce.

8.1.2.4 OHODNOCENÍ RIZIK

Na uvedená aktiva byly namapovány relevantní hrozby uvedené v příloze č. 1, pro které byla určena jejich úroveň a následně i úroveň zranitelnosti, to vše za předpokladu neexistence bezpečnostních standardních opatření (jedná se tedy o teoretickou maximální hodnotu rizika uváděnou zejména za účelem porovnání s výslednou úrovní zbytkového rizika po implementaci opatření). Na základě toho byla určena **inherentní rizika** uvedená v tabulce Tab. 8 (sloupec „Inher. riziko“).

Následně byla rizika s úrovní vyšší než nízká (v tabulce případně označena zeleně) snížena opatřeními nabízenými poskytovatelem cloudových služeb a byla určena **zbytková rizika** uvedená ve stejné tabulce Tab. 8 (sloupec „Zbytkové riziko“).

Tab. 8 Rizika pro scénář 1

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbytkové riziko
Datová aktiva					
	Uložená data	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky správce	8	8
	Uložená data	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky poskytovatele	8	5
	Uložená data	Nesprávné řízení bezpečnosti	Nesprávné vyhodnocení SLA	7	7
	Uložená data	Nesprávné řízení bezpečnosti	Regulatorní nesoulad způsobený poskytovatelem	7	5
Služby					
	Služba SharePoint Online	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	9	5
	Služba SharePoint Online	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	10	5
	Služba SharePoint Online	Zneužití systémových zdrojů	Obecná zranitelnost u správce	7	7
	Služba SharePoint Online	Zavedení škodlivého software	Obecná zranitelnost ze strany správce	9	5
	Služba SharePoint Online	Popření	Obecná zranitelnost	8	5
	Služba SharePoint Online	Napadení komunikace	Obecná zranitelnost	8	5
	Služba SharePoint Online	Přerušení komunikace	Obecná zranitelnost	6	5
	Služba SharePoint Online	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	10	5
	Služba SharePoint Online	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele	8	4
	Služba SharePoint Online	Selhání software	Obecná zranitelnost u poskytovatele	8	4
	Služba SharePoint Online	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele	6	2
	Služba SharePoint Online	Selhání údržby	Obecná zranitelnost u poskytovatele	8	4
	Služba SharePoint Online	Chyba uživatele	Obecná zranitelnost u správce	8	7
	Služba SharePoint Online	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	7	4
	Služba SharePoint Online	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)	5	3
	Služba SharePoint Online	Úmyslné poškození externími pracovníky	Obecná zranitelnost	5	2
	Služba SharePoint Online	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	8	4
	Služba Azure AD	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	9	5

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbytkové riziko
	Služba Azure AD	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	10	5
	Služba Azure AD	Popření	Obecná zranitelnost	8	5
	Služba Azure AD	Napadení komunikace	Obecná zranitelnost	8	5
	Služba Azure AD	Přerušení komunikace	Obecná zranitelnost	6	5
	Služba Azure AD	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	10	5
	Služba Azure AD	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele	8	4
	Služba Azure AD	Selhání software	Obecná zranitelnost u poskytovatele	8	4
	Služba Azure AD	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele	6	2
	Služba Azure AD	Selhání údržby	Obecná zranitelnost u poskytovatele	8	4
	Služba Azure AD	Chyba uživatele	Obecná zranitelnost u správce	8	7
	Služba Azure AD	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	6	3
	Služba Azure AD	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)	5	3
	Služba Azure AD	Úmyslné poškození externími pracovníky	Obecná zranitelnost	5	2
	Služba Azure AD	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	8	4

Detailní seznam inherentních a zbytkových rizik je uveden v příloze č. 2

Úroveň některých rizik snížena nebyla, neboť se jedná o rizika, která musí být snížena opatřeními na úrovni správce (příslušné oblasti jsou zcela mimo vliv poskytovatele cloudových služeb). Jedná se zejména o tyto kombinace hrozeb a zranitelností:

- Zneužití práv (neoprávněná akce obsluhy) – Zneužití pracovníky správce,
- Nesprávné řízení bezpečnosti – Nesprávné vyhodnocení SLA,
- Zneužití systémových zdrojů - Obecná zranitelnost u správce,
- Chyba uživatele – Obecná zranitelnost u správce.

S výjimkou rizik, která musí být snížena opatřeními na úrovni správce, **byla implementací opatření ostatní rizika snížena až na úroveň 5**, což je ve spodní části střední úrovně rizik (jedná se tedy o rizika, která **mohou být akceptovaná**, ale měla by být nadále sledovaná).

Pro snížení rizik byla použita opatření uvedená v kapitole 8.1.3 (sloupec AR).

Mapování opatření na rizika, která snižují, je uvedeno v příloze č. 2.

Rizika správce

V rámci analýzy rizik v rámci DPIA, která bude prováděna pro celý informační systém a nikoliv pouze pro služby SharePoint Online, je nutné analyzovat nejenom rizika spojená se službami Office 365, ale i rizika spojená s zařízeními plně ve správě správce, na jejichž úroveň nemá společnost Microsoft v roli poskytovatele služeb SharePoint Online žádný vliv.

V rámci DPIA tedy bude nutné navíc analyzovat následující rizika (popsaná kombinací akivum – hrozba - zranitelnost):

- Aktivum: Pracovní stanice
  - Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb – Obecná zranitelnost (Nedostatek opatření)
  - Neoprávněný přístup k aktivu cizími osobami – Obecná zranitelnost (Nedostatek opatření)
  - Zneužití práv (neoprávněná akce obsluhy) – Obecná zranitelnost (Nedostatek opatření)
  - Zneužití systémových zdrojů – Obecná zranitelnost (Nedostatek opatření)
  - Popření – Obecná zranitelnost (Nedostatek opatření)
  - Kybernetický útok z komunikační sítě – Obecná zranitelnost (Nedostatek opatření)
  - Zavedení škodlivého software – Obecná zranitelnost (Nedostatek opatření)
  - Selhání hardware nebo média – Obecná zranitelnost (Nedostatek opatření)
  - Selhání software – Obecná zranitelnost (Nedostatek opatření)
  - Selhání údržby – Obecná zranitelnost (Nedostatek opatření)
  - Chyba uživatele – Obecná zranitelnost (Nedostatek opatření)
  - Prozrazení informaci z vyřazené komponenty nebo média – Obecná zranitelnost (Nedostatek opatření)
  - Ztráta zařízení, média a dokumentu – Obecná zranitelnost (Nedostatek opatření)
  - Krádež interními pracovníky – Obecná zranitelnost (Nedostatek opatření)
  - Krádež externími pracovníky (včetně vybavení nebo dat) – Obecná zranitelnost (Nedostatek opatření)
  - Úmyslné poškození interními pracovníky – Obecná zranitelnost (Nedostatek opatření)
  - Úmyslné poškození externími pracovníky – Obecná zranitelnost (Nedostatek opatření)
- Aktivum: Komunikační linky
  - Přerušení komunikace – Nedostatečná SLA linky nebo nedostatek záložních linek

Pozn: Vzhledem ke skutečnosti, že uvedené oblasti nesouvisí přímo s analyzovanou službou a přitom jsou úzce spojené s konkrétní organizací, je vysoce pravděpodobné, že se budou v závislosti na organizaci správce lišit. V rámci této vzorové DPIA tedy není vypracován plnohodnotný vzor, ale pouze identifikována rizika, která musí být dále ohodnocena.

8.1.2.5 ANALÝZA SHODY

Tato DPIA je vytvářená z pohledu subjektu údajů, kdy jsou analyzovány dopady porušení zabezpečení osobních údajů na konkrétní subjekt údajů (pacienta), je tato kapitola omezena na splnění konkrétních požadavků stávající a budoucí legislativy zaměřených na zabezpečení informačního systému. Ostatní požadavky, které přímo nesouvisející s vlastním zabezpečením dat, jsou analyzovány v samostatné kapitole 7.

Požadavky GDPR

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
Článek 32, odst. 1	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:		
Článek 32, odst. 1, písm. a)	a) pseudonymizace a šifrování osobních údajů;	II-10-1 II-10-2 II-12	10.13 10.15
Článek 32, odst. 1, písm. b)	b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;	I-1-0 I-2-0 I-3-0 I-4-0 I-5-0 I-6-0 I-7-0 I-8-0 I-9-0 I-10-0 I-11-0 I-12-0 I-13-0 II-1-0 II-2-0 II-3-0 II-4-0 II-5-0 II-6-0 II-7-0 II-8-0 II-9-0 II-10-1 II-10-2 II-11-0	všechna z 9 a 10
Článek 32, odst. 1, písm. c)	c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;	I-12-0 I-13-0 II-11-0	9.12 9.13 10.14

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
Článek 32, odst. 1, písm. d)	d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.	I-11-0 II-9-0	9.11 10.12

Požadavky ZoOOÚ

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
§ 13, odst. 1	Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.	I-1-0 I-2-0 I-3-0 I-4-0 I-5-0 I-6-0 I-7-0 I-8-0 I-9-0 I-10-0 I-11-0 I-12-0 I-13-0 II-1-0 II-2-0 II-3-0 II-4-0 II-5-0 II-6-0 II-7-0 II-8-0 II-9-0 II-10-1 II-10-2 II-11-0	všechna z 9 a 10
§ 13, odst. 2	Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.	I-3-0	9.3
§ 13, odst. 4	V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také		
	a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,	I-9-0 II-3-0 II-4-0	9.9 10.6 10.7
	b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,	I-9-0 II-3-0 II-4-0	9.9 10.6 10.7
	c) pořizovat elektronické záznamy, které umožní	II-6-0	10.9

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
	určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a	II-8-0	10.11
	d) zabránit neoprávněnému přístupu k datovým nosičům.	I-9-0 II-1-0 II-3-0 II-4-0 II-10-1	9.9 10.4 10.6 10.7 10.13

8.1.3 IDENTIFIKOVANÁ OPATŘENÍ

V rámci analýzy rizik a identifikace opatření pro pokrytí legislativních požadavků byla identifikována následující bezpečnostní opatření:

Tab. 9
Opatření scénáře 1

ID	Kapitola	Název opatření	AR	Shoda
I-1-0	9.1	Systém řízení bezpečnosti informací	ano	ano
I-2-0	9.2	Řízení rizik	ano	ano
I-3-0	9.3	Bezpečnostní politika	ano	ano
I-4-0	9.4	Organizační bezpečnost	ano	ano
I-5-0	9.5	Stanovení bezpečnostních požadavků pro dodavatele	ano	ano
I-6-0	9.6	Řízení aktiv	ano	ano
I-7-0	9.7	Bezpečnost lidských zdrojů	ano	ano
I-8-0	9.8	Řízení provozu a komunikací	ano	ano
I-9-0	9.9	Řízení přístupu osob	ano	ano
I-10-0	9.10	Akvizice, vývoj a údržba	ano	ano
I-11-0	9.11	Kontrola a audit	ano	ano
I-12-0	9.12	Zvládání bezpečnostních událostí a bezpečnostních incidentů	ano	ano
I-13-0	9.13	Řízení kontinuity činností	ano	ano
II-1-0	10.4	Fyzická bezpečnost	ano	ano
II-2-0	10.5	Nástroj pro ochranu integrity komunikačních sítí	ano	ano
II-3-0	10.6	Nástroj pro ověřování identity uživatelů	ano	ano
II-4-0	10.7	Nástroj pro řízení přístupových oprávnění	ano	ano
II-5-0	10.8	Nástroj pro ochranu před škodlivým kódem	ano	ano
II-6-0	10.9	Nástroj pro zaznamenávání činnosti	ano	ano
II-7-0	10.10	Nástroj pro detekci kybernetických bezpečnostních událostí	ano	ano
II-8-0	10.11	Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	ano	ano
II-9-0	10.12	Aplikační bezpečnost	ano	ano
II-10-1	10.13	Kryptografické prostředky ochrana dat (v klidu)	ano	ano
II-10-2	10.13	Kryptografické prostředky ochrana dat (při přenosu)	ano	ano
II-11	10.14	Nástroj pro zajišťování úrovně dostupnosti informací	ano	ano
II-12	10.15	Pseudonymizace	částečně	částečně

Popis jednotlivých opatření je uveden v kapitolách č. 9 a 10.

8.2 DPIA PRO SCÉNÁŘ 2 – EXCHANGE ONLINE / OUTLOOK

V případě tohoto scénáře je kromě výše uvedených předpokladů navíc počítáno s následujícími dodatečnými předpoklady:

Předpoklad 4:

Bezpečnost přístupu externích pracovníků (smluvních partnerů) přistupujících k osobním údajům (zahrnující i nastavení potřebné úrovně zabezpečení) bude zajištěna na úrovni organizačních opatření mezi správcem a externím pracovníkem, resp. subjektem tohoto pracovníka zastřešujícím (smluvním partnerem).

To například zahrnuje zajištění bezpečnosti pracovní stanice, ze které externí pracovník přistupuje na osobní údaje.

8.2.1 ROZSAH DPIA

8.2.1.1 POPIS HODNOCENÉHO PROCESU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Vymezení správce a typu zpracovávaných údajů

Správcem v rámci tohoto zpracování osobních údajů bude městská organizace komunálních služeb, která v aplikaci SharePoint Online vede smlouvy o odvozu odpadu nebo o dodávkách pitné vody (obsahují údaje občanů – subjektů údajů) a pomocí cloudové služby Office 365 Exchange Online

- vyřizuje běžnou komunikaci se svými zákazníky, tedy subjekty údajů (obsahuje obecné osobní údaje, jako jsou e-mail, telefon, příp. i číslo bankovního účtu); charakter této komunikace je externí,
- zajišťuje skupinovou spolupráci pro své pracovníky (jak zaměstnance, tak i smluvní partnery), pro kterou využívá osobní i skupinové e-maily, kontakty, kalendáře, úkoly a poznámky (mohou obsahovat osobní údaje).

Správce tedy zpracovává osobní údaje podle ZoOOÚ.

Účel zpracování

Zpracování osobních údajů bude probíhat výhradně za účelem

- sběru informací od subjektu údajů a distribuce informací subjektům údajů, aby správce mohl poskytovat služby v požadované kvalitě a
- vyměňování a sdílení informací v rámci skupinové spolupráce, aby správce mohl řádně vykonávat své činnosti.

Při tomto zpracování budou použity následující tituly zpracování:

- plnění smlouvy mezi správcem a subjekty údajů,
- souhlas udělený subjektem údajů[6] (pro případy, které nespadají pod výše uvedený titul).

Popis operací zpracování

Osobní údaje budou zpracovávány (vytvářeny, upravovány, odesílány, přijímány a čteny) výhradně v rámci činnosti správce za účelem poskytování jeho služeb svým zákazníkům.

Dále budou osobní údaje zpracovávány (vytvářeny, upravovány a čteny) v rámci interních činností správce, a to především formou předávání a sdílení osobních údajů v adresářích, kalendářích, úkolech, poznámkách a případně i v připojených dokumentech.

[6] V uvedeném případě musí správce vlastními prostředky zajistit zajištění souhlasu a jeho další správu.

Výše uvedené zpracování bude probíhat ve formě

- odesílání a příjmu zpráv elektronické pošty prostřednictvím standardních protokolů (SMTP, MAPI a dalších) a
- uložení emailů, kontaktů, událostí, úkolů, poznámek a připojených dokumentů do emailové schránky a jejich zpracování.

Výše uvedené operace zpracování jsou nezbytné pro plnění smlouvy mezi správcem a subjekty údajů.

Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů[7]

Správce v rámci nezbytnosti a přiměřenosti řádně vyhodnotil rizika, že by zpracování mohlo omezit práva subjektů údajů jakož i výhody a dodatečné záruky, které zpracování pro práva subjektů údajů přináší. Správce dospěl při tomto vyhodnocení k závěru, že zpracování je prováděno pouze v rámci původního účelu a nijak nezasahuje do práv a oprávněných zájmů subjektů údajů.

Správce pečlivě vyhodnotil a buď produktovým nastavením či v rámci smluvních podmínek sjednaných se zpracovatelem zajistil, že všechna zákonná práva subjektů údajů zůstanou zpracováním nedotčena. Správce považuje za důležité, že zpracovatel poskytl v kapitole „Použití zákaznických dat“ PSO smluvní záruky, že zpracovávaná „data budou použita jen pro vlastní poskytování služby zákazníkovi“, že zpracovatel „nebude zákaznická data využívat ani z nich nebude odvozovat informace pro žádné reklamní či podobné komerční účely“ a že zpracovatel „nezískává k zákaznickým datům žádná práva s výjimkou práv, která společnosti Microsoft přidělí zákazník pro poskytování služeb online zákazníkovi.“

Zpracování na druhou stranu přináší následující výhody a dodateční záruky pro subjekty údajů spočívající v zajištění důvěrnosti, integrity a dostupnosti zpracovávaných údajů a odolnosti systémů a služeb zpracování, a to jak na technické, tak i na organizační úrovni.

Bezpečnostní požadavky

Technologie zajišťující uvedené zpracování dat v systémech správce[8] budou splňovat následující minimání bezpečnostní požadavky:

- pokrytí explicitních požadavků GDPR a ZoOOÚ – viz kapitola 8.2.1.5,
- identifikace a autentizace všech osob přistupujících k datům uložených v systémech správce,
- šifrování přenosů mezi klienskou aplikací a systémem správce dat přes nedůvěryhodné prostředí,
- zajištění integrity uložených dat (jejich ochrany) před poškozením v důsledku akce neoprávněné osoby,
- zajištění integrity uložených dat (jejich ochrany) před poškozením v důsledku chyby hardware a
- cíl dostupnosti: RPO maximálně 5 minut a RTO maximálně 1 hodina.

[7] [7] Jedná se zde o vzorový text, který musí daný správce upravit dle svojí skutečné situace.
[8] U tohoto scénáře je nutné si uvědomit, že zajištění ochrany dat ze strany subjektů komunikujích se správcem (zejména subjektů odesílajících e-mailové zprávy nebo naopak přijímající e-mailové zprávy) je mimo kontrolu správce. Proto se uvedené požadavky týkají pouze ochrany údajů uložených v systémech správce.

Přístup k údajům

K údajům v systému správce budou mít přístup pouze pracovníci správce (zaměstnanci nebo smluvní partneři).

Zpřístupnění údajů

Údaje budou používané výhradně v rámci vlastních činností správce a nebudou sdílné mimo prostředí správce nebo jeho smluvních partnerů (odesílání nebo příjem e-mailových zpráv není v rámci této DPIA považováno za sdílení).

8.2.1.2 POPIS HODNOCENÉHO INFORMAČNÍHO SYSTÉMU NEBO SLUŽBY

Základní popis logické a fyzické architektury

Posuzovaný informační systém se bude skládat z následujících částí:

- pracovních stanic pracovníků správce vybavené OS, prohlížečem a kancelářským software MS Office,
- komunikačních linek (LAN, internet),
- služeb Exchange Online, konkrétně
  - odesílání a příjem zpráv elektronické pošty mezi správcem a subjekty údajů a mezi pracovníky správce navzájem,
  - přístup do osobní (nebo sdílené) e-mailové schránky, adresáře, kalendáře, úkolů a poznámek,
- služeb Azure, konkrétně služeb Azure AD pro správu uživatelů Office 365.

Pracovní stanice a komunikační linky LAN správce nebo jeho smluvních partnerů se budou nacházet v prostorách správce nebo jeho smluvních partnerů, ostatní části budou mimo tyto prostory nebo dokonce mimo Českou republiku.

Struktura zpracovávaných informací

Všechny zpracovávané informace budou primárně uloženy v rámci služby Exchange Online a to konkrétně

- v rámci jednotlivých e-mailových schránek (e-maily, kontakty, kalendáře, úkoly, poznámky) mohou obsahovat
  - jméno, popřípadě jména, příjmení zákazníků,
  - datum narození, rodné číslo,
  - adresa místa trvalého pobytu,
  - e-mail a telefon,
  - čísla bankovních spojení,
  - platby za služby, přeplatky resp. nedoplatky,
  - odebírané, nově objednávané nebo rušené služby;
- v rámci jednotlivých nestrukturovaných dokumentů (ve formě připojených dokumentů k e-mailovým zprávám), kterými mohou být např. výpisy z bankovních účtů, potvrzení, naskenované dokumenty apod.

Popis datových toků

Při zpracování údajů v informačním systému budou existovat následující datové toky:

- Pracovník správce (uživatel) vkládá nestrukturované osobní údaje do služby Exchange Online, která tyto informace ukládá do interního uložiště služby ve formě jednotlivých objektů (e-mailová zpráva, dokument, kalendář, adresář, úkoly, poznámky).
- Pracovník správce (uživatel) čte nestrukturované osobní údaje ze služby Exchange Online, která tyto informace získává z interního uložiště služby ve formě jednotlivých objektů.
- Pracovník správce (uživatel) upravuje nestrukturované osobní údaje ve službě Exchange Online, která tyto informace mění v interním uložišti služby ve formě jednotlivých objektů.
- Pracovník správce (uživatel) odstraňuje nestrukturované osobní údaje ze služby Exchange Online, která tyto informace odstraňuje z interního uložiště služby ve formě jednotlivých objektů.
- Pracovník správce (uživatel) zasílá nestrukturované osobní údaje externímu subjektu.
- Pracovník správce (uživatel) přijímá nestrukturované osobní údaje od externího subjektu.

Popis rozhraní

Ve všech výše uvedených případech budou pro přístup k systémům správce používána následujcí rozhraní:

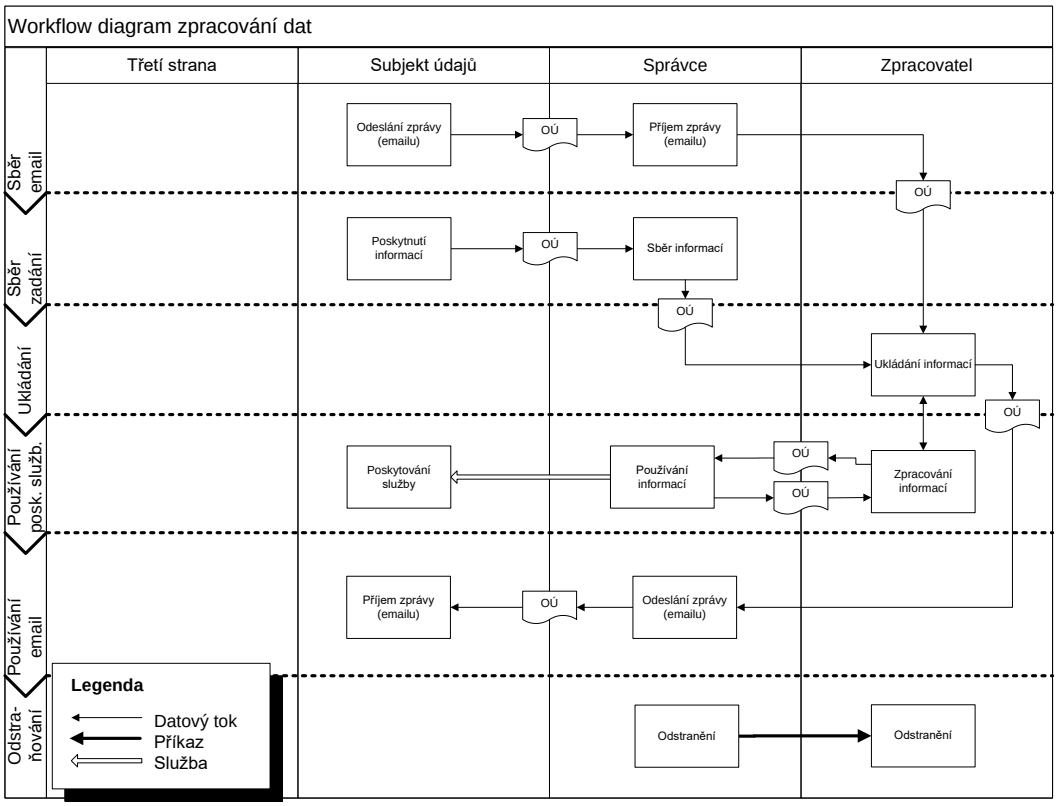
- Uživatelské rozhraní mezi pracovní stanicí a uživatelem ve formě prohlížeče nebo software balíku MS Office, případně ve formě poštovního klienta v mobilním zařízení.
- Technické rozhraní ve formě rozhraní služby Office 365 Exchange Online dostupného protokolem HTTPS (HTTP přes TLS) a SMTP rozhraní pro příjem e-mailových zpráv od externích subjektů.

Podmínkou (s výjimkou SMTP rozhraní) je autentizace pracovníka správce (uživatele) ke službě Office 365 Exchange Online.

Workflow diagram zpracování dat

Metody zpracování dat jsou graficky zobrazeny na následujícím obrázku:

Obr. 2
Workflow diagram pro scénář 2



8.2.1.3 POPIS OPERAČNÍCH POSTUPŮ

Podle [33] je vhodné v rámci DPIA popsat plánované operační postupy správy a používání informačního systému, které mohu mít vliv na bezpečnost osobních údajů, zejména:

- koncept správy uživatelů (pracovníků správce) a jejich oprávnění,
- koncept zajištění výkonu práv subjektu údajů, tedy jakým způsobem bude postupováno v jednotlivých případech, kdy subjekt údajů uplatné své právo[9],
- koncept provozu systému (služby), přičemž zde musí být uvedeno, že část systému je provozována externě, konkrétně v cloudové službě typu SaaS Office 365 Exchange Online,
- koncept zajištění podpory informačního systému, přičemž zde musí být zejména uvedeny subjekty, které se budou podílet na podpoře informačního systému včetně informací, zdali budou mít přístup k osobním údajům a případně odkud,
- koncept vytváření záznamů o činnosti pracovníků správce (zaměstnanců správce, pracovníků smluvních partnerů) a pracovníků podpory a vlastního systému (logování) včetně plánů na jejich další uchování,
- plány zálohování a obnovy (které mohou být vzhledem k plánovanému využití cloudové SaaS služby poměrně jednoduché),
- ochrana a správa metadat (pokud existují, což v tomto případě není nezbytné),

[9] V prostředí Exchange Online nabízí poskytovatel služby podporu činností spojených s uplatněním práv subjektů v podobě standardních nástrojů typu vyhledávání, eDiscovery a řízení přístupu (například pro případ zablokování přístupu).

- plány na uchování a odstranění dat a likvidaci médií,
- koncept zrušení informačního systému (ukončení smlouvy a případně postup vrácením osobních údajů správci).

Pozn: Vzhledem ke skutečnost, že uvedené oblasti nesouvisí přímo s analyzovanou službou a přitom jsou úzce spojené s konkrétní organizací, je vysoce pravděpodobné, že se budou v závislosti na organizaci správce lišit. V rámci této vzorové DPIA tedy není vypracován plnohodnotný vzor, ale pouze identifikovány doporučené oblasti pro další rozpracování.

8.2.1.4 POPIS INTERAKCE SE SUBJEKTEM ÚDAJŮ

Interakce se zákazníkem (subjektem údajů) se bude skládat z

- informování subjektu údajů,
- poskytování údajů subjektem údajů (např. v rámci přihlášení se k odběru vody nebo svozu odpadu),
- poskytování údajů subjektu údajů (např. o typu a množství odebraných služeb),
- výkonu práv subjektu údajů (přístup k osobním údajům, oprava, výmaz, omezení zpracování a vznesení námitky).

Subjekt údajů bude informován o:

Tab. 10 Oblasti informování subjektu pro scénář 2

Požadavek GDPR	Komentář
Totožnost a kontaktní údaje správce a jeho případného zástupce	
Kontaktní údaje případného pověřence pro ochranu osobních údajů	Tento bod se v tomto scénáři pravděpodobně neuplatní.
Účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování	Zpracování osobních údajů probíhá výhradně za účelem ■ sběru informací od subjektu údajů a distribuce informací subjektům údajů, aby správce mohl poskytovat služby v požadované kvalitě a ■ vyměňování a sdílení informací v rámci skupinové spolupráce, aby správce mohl řádně vykonávat své činnosti. Právním základem (titulem) pro zpracování je: Plnění smlouvy mezi správcem a subjekty údajů. Souhlas udělený subjektem údajů (pro případy, které nespadají pod výše uvedené tituly).
Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);	Pravděpodobně se neuplatní (bez získání osobních údajů, nemůže správce poskytovat své služby)
Případné příjemce nebo kategorie příjemců osobních údajů	Kromě subjektu údajů a pracovníků správce (vč. jeho smluvních partnerů) k údajům mohou přistupovat pouze osoby, které mají tento přístup povolen speciálním zákonem.

Požadavek GDPR	Komentář
Případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny	Osobní údaje v případě využití Office 365 jsou předávány do zahraničí na základě článku 46 odst. 2 písm. c) GDPR, tedy na základě Standardních smluvních doložek přijatých Komisí podle čl. 93 odst. 2. Údaje o vhodných zárukách jsou uvedeny v rámci veřejně přístupných PSO, resp. Přílohy č. 2 PSO – Standardních smluvních doložkách.
Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby	
Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů	PSO stanoví v kap. „Použití zákaznických dat“, že správce osobních údajů (zákazník) si zachová všechna práva týkající se zákaznických dat. Z pohledu zpracovatele osobních údajů stanoví PSO v kap. „Přístup k zákaznickým datům“: (1) poskytovat zákazníkovi možnost opravit, odstranit nebo zablokovat zákaznická data, nebo (2) provádět takové opravy, odstranění nebo blokování jménem zákazníka. Správce osobních údajů má za tímto účelem k dispozici nástroje služby Office 365 jako jsou vyhledávání obsahu, eDiscovery (viz [34]), a auditní logy pro změny nebo výmazy obsahu.
Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním	
Existence práva podat stížnost u dozorového úřadu	
Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů	Správce uzavírá smlouvu se subjekty (o poskytování služeb jako např. o dodávce vody apod.) a potřebuje k tomu jejich osobní údaje.
Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů	Pravděpodobně se neuplatní

Výkon práv subjektu údajů bude možné vykonávat žádostí u pracovníka správce nebo komunikací s dozorovým úřadem.

8.2.1.5 POŽADAVKY NA SOUKROMÍ A ZABEZPEČENÍ

Explicitní požadavky na soukromí a zabezpečení jsou dané

- zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (aktuálně) a
- nařízením 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 (od 25. 5. 2018).

Další požadavky na zabezpečení vyplývají z analýzy rizik.

8.2.2 ANALÝZA RIZIK

V této kapitole je vypracována vzorová analýza rizik v rámci DPIA, tedy posouzení rizik pro práva a svobody subjektů. Při této analýze rizik je postupováno podle metodiky vycházející z požadavků VoKB, ale upravené v oblasti dopadů tak, aby zohledňovala dopad na subjekt údajů (zákazníka) – viz příloha č. 1.

8.2.2.1 KRITÉRIA PRO AKCEPTACI RIZIK

Kritéria pro aceptaci rizik jsou uvedena v příloze 1 (Metodika analýzy rizik), kapitole 3.2.
U jednotlivých rizik je uvedena osoba, která může příslušnou úroveň zbytkového rizika akceptovat a zda-li se jedná o vysoké riziko pro práva a svobody fyzických osob dle GDPR, které před zahájením zpracování vyžaduje konzultaci s dozorovým úřadem.

8.2.2.2 AKTIVA A JEJICH HODNOTY

Uložená nejvíce citlivá **datová aktiva** jsou z pohledu důvěrnosti, integrity a dostupnosti **ohodnocena** podle vodítek uvedených v příloze č. 1 hodnotami uvedenými v následující tabulce.

Tab. 11
Ohodnocení dat pro scénář 2

Aspekt	Úroveň	Zdůvodnění
Důvěrnost	Střední	Subjekt údajů bude vystaven značným nepříjemnostem, které bude schopen za cenu jistých potíží překonat (zvýšení nákladů, odepření služby, strach, nepochopení, stress, malá fyzická újma, atd.). Zde je předpokládán scénář zpřístupnění e-mailu s osobními údaji někomu jinému (např. jaké služby sujbekt odebrírá a v jakém rozsahu, informace o účtech, kolik osob je v domácnosti apod.).
Integrita	Nízká	Subjekt údajů buď nebude ovlivněn vůbec anebo bude vystaven drobným problémům, které bude schopen bez větších obtíží překonat (čas strávený opětovným zadání informací, nepříjemností, nepohodlí, podrážděnost, atd.). Zde předpokládám scénář modifikace záznamů (e-mailů), což vést k nutnosti opětovného poskytování, dohledávání a dokládání informací. Scénář nepředpokládá, že by touto cestou bylo možné měnit klíčové osobní údaje (například kontaktní údaje uvedené ve smlouvě).

Aspekt	Úroveň	Zdůvodnění
Dostupnost	Nízká	Subjekt údajů buď nebude ovlivněn vůbec anebo bude vystaven drobným problémům, které bude schopen bez větších obtíží překonat (čas strávený opětovným zadání informací, nepříjemností, nepohodlí, podrážděnost, atd.). Zde předpokládán scénář dočasného výpadku služeb zajišťující e-mailovou komunikaci, kdy bude např. potřeba použít telefon nebo osobní schůzku.
Ztráta	Nízká	Subjekt údajů buď nebude ovlivněn vůbec anebo bude vystaven drobným problémům, které bude schopen bez větších obtíží překonat (čas strávený opětovným zadání informací, nepříjemností, nepohodlí, podrážděnost, atd.). Zde předpokládán scénář ztráty záznamů o komunikaci nebo naplánovaných schůzkám, což může vést k potřebě znovuzaslání informací nebo přeplánování schůzky.

Nepřímé újmy nemůže správce a ani zpracovatel předjímat a proto tato rizika nejsou zahrnuta.

V následující tabulce je uveden seznam všech identifikovaných aktiv s uvedením jejich popisu spolu s jejich typem podle přílohy č. 1.

Tab. 12
Seznam aktiv pro scénář 2

Typ aktiva	Aktivum	Popis
Datová aktiva	Data zásilek	E-maily a připojené dokumenty
	Data interních objektů	Kontakty, události, úkoly, poznámky a připojené dokumenty do e-mailové schránky
Služby	Služba Exchange Online	Přístup ke službě (e-mailové schránky včetně osobních a skupinových e-mailů, kontaktů, událostí, úkolů, poznámek a připojených dokumentů)
	Komunikace s externími subjekty	Odesílání a příjem zpráv elektronické pošty prostřednictvím standardních protokolů (SMTP)
	Služba Azure AD	Rozhraní pro správu identit, autentizačních údajů a oprávnění

Vlastní ohodnocení identifikovaných aktiv vychází z výše uvedeného ohodnocení dat. V dalších částech analýzy se pro zjednodušení pracuje s Daty zásilek a s Daty interních objektů dohromady jako s Datovými aktivy.

Tab. 13
Ohodnocení aktiv pro scénář 2

Aktivum	Důvěrnost	Integrita	Dostupnost	Ztráta
Datová aktiva	Střední	Nízká	Nízká	Nízká
Služba Exchange Online	Střední	Nízká	Nízká	-

Aktivum	Důvěrnost	Integrita	Dostupnost	Ztráta
Služba komunikace s externími subjekty	Střední	Nízká	Nízká	-
Služba Azure AD	Střední	Střední	Nízká	-

8.2.2.3 HROZBY A ZRANITELNOSTI

Seznam uvažovaných hrozeb je uveden v příloze č. 1, kapitola 2.2.1.

V případě **ohodnocení úrovní hrozeb** a **zranitelností** jsou hodnoty úrovní uvedeny přímo v tabulkách analýzy rizik (příslušné hodnoty se liší v závislosti na scénáři a aktivu, a proto není možné definovat jednu celkovou úroveň).

V této analýze uvedené hodnoty budou potom v případě konkrétní analýzy rizik IS správce nahrazeny hodnotami vycházejícími z charakteristik prostředí konkrétního správce.

8.2.2.4 OHODNOCENÍ RIZIK

Na uvedená aktiva byly namapovány relevantní hrozby uvedené v příloze č. 1, pro které byla určena jejich úroveň a následně i úroveň zranitelnosti, to vše za předpokladu neexistence bezpečnostních standardních opatření (jedná se tedy o teoretickou maximální hodnotu rizika uváděnou zejména za účelem porovnání s výslednou úrovní zbytkového rizika po implementaci opatření). Na základě toho byla určena **inherentní rizika** uvedená v tabulce Tab. 14 (sloupec „Inher. riziko“).

Následně byla rizika s úrovní vyšší než nízká (v tabulce případně označena zeleně) snížena opatřeními nabízenými poskytovatelem cloudových služeb a byla určena **zbytková rizika** uvedená ve stejné tabulce Tab. 14 (sloupec „Zbytkové riziko“).

Tab. 14 Rizika pro scénář 2

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbytkové riziko
Datová aktiva					
	Datová aktiva	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky správce	6	6
	Datová aktiva	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky poskytovatele	6	3
	Datová aktiva	Nesprávné řízení bezpečnosti	Nesprávné vyhodnocení SLA	5	5
	Datová aktiva	Nesprávné řízení bezpečnosti	Regulatorní nesoulad způsobený poskytovatelem	5	3
Služby					
	Služba Exchange Online	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	7	3
	Služba Exchange Online	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	8	3
	Služba Exchange Online	Zneužití systémových zdrojů	Obecná zranitelnost u správce	5	5
	Služba Exchange Online	Zavedení škodlivého software	Obecná zranitelnost ze strany správce	7	3
	Služba Exchange Online	Popření	Obecná zranitelnost	6	3
	Služba Exchange Online	Napadení komunikace	Obecná zranitelnost	6	3
	Služba Exchange Online	Přerušení komunikace	Obecná zranitelnost	5	4
	Služba Exchange Online	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	8	3
	Služba Exchange Online	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele	5	1
	Služba Exchange Online	Selhání software	Obecná zranitelnost u poskytovatele	6	2
	Služba Exchange Online	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele	5	1
	Služba Exchange Online	Selhání údržby	Obecná zranitelnost u poskytovatele	6	2
	Služba Exchange Online	Chyba uživatele	Obecná zranitelnost u správce	6	5
	Služba Exchange Online	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	6	3
	Služba Exchange Online	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)	4	2
	Služba Exchange Online	Úmyslné poškození externími pracovníky	Obecná zranitelnost	4	1
	Služba Exchange Online	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	6	2
	Služba komunikace s externími IS	Zavedení škodlivého software	Zranitelnost u příchozích zpráv	7	4
	Služba komunikace s externími IS	Popření	Obecná zranitelnost	6	3

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbytkové riziko
	Služba komunikace s externími IS	Napadení komunikace	Zranitelnost u příchozích zpráv	7	7
	Služba komunikace s externími IS	Napadení komunikace	Zranitelnost u odchozích zpráv	7	5
	Služba komunikace s externími IS	Přerušení komunikace	Obecná zranitelnost	5	4
	Služba komunikace s externími IS	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	8	3
	Služba komunikace s externími IS	Náhodné přesměrování	Zranitelnost u odchozích zpráv	6	4
	Služba komunikace s externími IS	Chyba uživatele	Zranitelnost u odchozích zpráv	7	4
	Služba Azure AD	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	7	3
	Služba Azure AD	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	8	3
	Služba Azure AD	Popření	Obecná zranitelnost	6	3
	Služba Azure AD	Napadení komunikace	Obecná zranitelnost	6	3
	Služba Azure AD	Přerušení komunikace	Obecná zranitelnost	5	4
	Služba Azure AD	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	8	3
	Služba Azure AD	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele	6	2
	Služba Azure AD	Selhání software	Obecná zranitelnost u poskytovatele	6	2
	Služba Azure AD	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele	5	1
	Služba Azure AD	Selhání údržby	Obecná zranitelnost u poskytovatele	6	2
	Služba Azure AD	Chyba uživatele	Obecná zranitelnost u správce	6	5
	Služba Azure AD	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	6	2
	Služba Azure AD	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)	4	2
	Služba Azure AD	Úmyslné poškození externími pracovníky	Obecná zranitelnost	4	1
	Služba Azure AD	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	6	2

Detailní seznam inherentních a zbytkových rizik je uveden v příloze č. 3.

Úroveň některých rizik snížena nebyla, neboť se jedná o rizika, která vznikají v souvislosti s komunikací s externími subjekty (příslušné oblasti jsou zcela nebo převážně mimo vliv poskytovatele cloudových služeb). Jedná se zejména o tyto kombinace hrozeb a zranitelností:

- Zneužití práv (neoprávněná akce obsluhy) – Zneužití pracovníky správce,
- Nesprávné řízení bezpečnosti – Nesprávné vyhodnocení SLA,
- Zneužití systémových zdrojů - Obecná zranitelnost u správce,
- Chyba uživatele – Obecná zranitelnost u správce a
- Napadení komunikace – Zranitelnost u příchozí komunikace (tato hrozba je mimo kontrolu správce).

S výjimkou rizik, která musí být snížena opatřeními na úrovni správce, **byla implementací opatření ostatní rizika snížena až na úroveň 5**, což je ve spodní části střední úrovně rizik (jedná se tedy o rizika, která **mohou být akceptovaná**, ale měla by být nadále sledovaná).

Pro snížení rizik byla použita opatření uvedená v kapitole 8.2.3 (sloupec AR).

Mapování opatření na rizika, která snižují, je uvedeno v příloze č. 3.

Rizika správce

V rámci analýzy rizik v rámci DPIA, která bude prováděna pro celý informační systém a nikoliv pouze pro služby Exchange Online, je nutné analyzovat nejenom rizika spojená se službami Office 365, ale i rizika spojená s zařízeními plně ve správě správce, na jejichž úroveň nemá společnost Microsoft v roli poskytovatele služeb Exchange Online žádný vliv.

V rámci DPIA tedy bude nutné navíc analyzovat následující rizika (popsaná kombinací akivum – hrozba – zranitelnost):

- Aktivum: Pracovní stanice
  - Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb – Obecná zranitelnost (Nedostatek opatření)
  - Neoprávněný přístup k aktivu cizími osobami – Obecná zranitelnost (Nedostatek opatření)
  - Zneužití práv (Neoprávněná akce obsluhy) – Obecná zranitelnost (Nedostatek opatření)
  - Zneužití systémových zdrojů – Obecná zranitelnost (Nedostatek opatření)
  - Popření – Obecná zranitelnost (Nedostatek opatření)
  - Kybernetický útok z komunikační sítě – Obecná zranitelnost (Nedostatek opatření)
  - Zavedení škodlivého software – Obecná zranitelnost (Nedostatek opatření)
  - Selhání hardware nebo média – Obecná zranitelnost (Nedostatek opatření)
  - Selhání software – Obecná zranitelnost (Nedostatek opatření)
  - Selhání údržby – Obecná zranitelnost (Nedostatek opatření)
  - Chyba uživatele – Obecná zranitelnost (Nedostatek opatření)
  - Prozrazení informaci z vyřazené komponenty nebo média – Obecná zranitelnost (Nedostatek opatření)
  - Ztráta zařízení, média a dokumentu – Obecná zranitelnost (Nedostatek opatření)
  - Krádež interními pracovníky – Obecná zranitelnost (Nedostatek opatření)
  - Krádež externími pracovníky (včetně vybavení nebo dat) – Obecná zranitelnost (Nedostatek opatření)

- Úmyslné poškození interními pracovníky – Obecná zranitelnost (Nedostatek opatření)
- Úmyslné poškození externími pracovníky – Obecná zranitelnost (Nedostatek opatření)

- Aktivum: Komunikační linky
  - Přerušení komunikace – Nedostatečná SLA linky nebo nedostatek záložních linek

Pozn: Vzhledem ke skutečnosti, že uvedené oblasti nesouvisí přímo s analyzovanou službou a přitom jsou úzce spojené s konkrétní organizací, je vysoce pravděpodobné, že se budou v závislosti na organizaci správce lišit. V rámci této vzorové DPIA tedy není vypracován plnohodnotný vzor, ale pouze identifikována rizika, která musí být dále ohodnocena.

8.2.2.5 ANALÝZA SHODY

Tato DPIA je vytvářená z pohledu subjektu údajů, kdy jsou analyzovány dopady porušení zabezpečení osobních údajů na konkrétní subjekt údajů (klienta), je tato kapitola omezena na splnění konkrétních požadavků stávající a budoucí legislativy zaměřených na zabezpečení informačního systému. Ostatní požadavky, které přímo nesouvisející s vlastním zabezpečením dat, jsou analyzovány v samostatné kapitole 7.

Požadavky GDPR

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
Článek 32, odst. 1	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:		
Článek 32, odst. 1, písm. a)	a) pseudonymizace a šifrování osobních údajů;	II-10-1 II-10-2 II-12	10.13 10.15
Článek 32, odst. 1, písm. b)	b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;	I-1-0 I-2-0 I-3-0 I-4-0 I-5-0 I-6-0 I-7-0 I-8-0 I-9-0 I-10-0 I-11-0 I-12-0 I-13-0 II-1-0 II-2-0 II-3-0 II-4-0 II-5-0 II-6-0 II-7-0 II-8-0 II-9-0 II-10-1 II-10-2 II-11-0	všechna z 9 a 10

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
Článek 32, odst. 1, písm. c)	c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;	I-12-0 I-13-0 II-11-0	9.12 9.13 10.14
Článek 32, odst. 1, písm. d)	d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.	I-11-0 II-9-0	9.11 10.12

Požadavky ZoOOÚ

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
§ 13, odst. 1	Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.	I-1-0 I-2-0 I-3-0 I-4-0 I-5-0 I-6-0 I-7-0 I-8-0 I-9-0 I-10-0 I-11-0 I-12-0 I-13-0 II-1-0 II-2-0 II-3-0 II-4-0 II-5-0 II-6-0 II-7-0 II-8-0 II-9-0 II-10-1 II-10-2 II-11-0	všechna z 9 a 10
§ 13, odst. 2	Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.	I-3-0	9.3
§ 13, odst. 4	V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také		
	a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,	I-9-0 II-3-0 II-4-0	9.9 10.6 10.7
	b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na	I-9-0 II-3-0 II-4-0	9.9 10.6 10.7

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
	základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,		
	c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a	II-6-0 II-8-0	10.9 10.11
	d) zabránit neoprávněnému přístupu k datovým nosičům.	I-9-0 II-1-0 II-3-0 II-4-0 II-10-1	9.9 10.4 10.6 10.7 10.13

8.2.3 IDENTIFIKOVANÁ OPATŘENÍ

V rámci analýzy rizik a identifkace opatření pro pokrytí legislativních požadavků byla identifikována následující bezpečnostní opatření:

Tab. 15
Opatření scénáře 2

ID	Kapitola	Název opatření	AR	Shoda
I-1-0	9.1	Systém řízení bezpečnosti informací	ano	ano
I-2-0	9.2	Řízení rizik	ano	ano
I-3-0	9.3	Bezpečnostní politika	ano	ano
I-4-0	9.4	Organizační bezpečnost	ano	ano
I-5-0	9.5	Stanovení bezpečnostních požadavků pro dodavatele	ano	ano
I-6-0	9.6	Řízení aktiv	ano	ano
I-7-0	9.7	Bezpečnost lidských zdrojů	ano	ano
I-8-0	9.8	Řízení provozu a komunikací	ano	ano
I-9-0	9.9	Řízení přístupu osob	ano	ano
I-10-0	9.10	Akvizice, vývoj a údržba	ano	ano
I-11-0	9.11	Kontrola a audit	ano	ano
I-12-0	9.12	Zvládání bezpečnostních událostí a bezpečnostních incidentů	ano	ano
I-13-0	9.13	Řízení kontinuity činností	ano	ano
II-1-0	10.4	Fyzická bezpečnost	ano	ano
II-2-0	10.5	Nástroj pro ochranu integrity komunikačních sítí	ano	ano
II-3-0	10.6	Nástroj pro ověřování identity uživatelů	ano	ano
II-4-0	10.7	Nástroj pro řízení přístupových oprávnění	ano	ano
II-5-0	10.8	Nástroj pro ochranu před škodlivým kódem	ano	ano
II-6-0	10.9	Nástroj pro zaznamenávání činnosti	ano	ano
II-7-0	10.10	Nástroj pro detekci kybernetických bezpečnostních událostí	ano	ano
II-8-0	10.11	Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	ano	ano
II-9-0	10.12	Aplikační bezpečnost	ano	ano
II-10-1	10.13	Kryptografické prostředky ochrana dat (v klidu)	ano	ano
II-10-2	10.13	Kryptografické prostředky ochrana dat (při přenosu)	ano	ano
II-11	10.14	Nástroj pro zajišťování úrovně dostupnosti informací	ano	ano
II-12	10.15	Pseudonymizace	ne	ne

Popis jednotlivých opatření je uveden v kapitolách č. 9 a 10.

8.3 DPIA PRO SCÉNÁŘ 3 – SKYPE FOR BUSINESS

V případě tohoto scénáře je kromě výše uvedených předpokladů navíc počítáno s následujícími dodatečnými předpoklady:

Předpoklad 4:

U uvedeného systému postaveného nad SharePoint Online není předpokládána interoperabilita v rámci národního systému eHealth.

Předpoklad 5:

Bezpečnost přístupu externích pracovníků (smluvních partnerů externích lékařských specialistů) přistupujících k osobním údajům (zahrnující i nastavení potřebné úrovně zabezpečení) bude zajištěna na úrovni organizačních opatření mezi správcem a externím pracovníkem, resp. subjektem tohoto pracovníka zastřešujícím (smluvním partnerem).

To například zahrnuje zajištění bezpečnosti pracovní stanice, ze které externí pracovník přistupuje na osobní údaje.

8.3.1 ROZSAH DPIA

8.3.1.1 POPIS HODNOCENÉHO PROCESU ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Vymezení správce a typu zpracovávaných údajů

Správcem v rámci tohoto zpracování osobních údajů bude zdravotnické zařízení (o více než jednom lékaři), které v rámci služby Skype for Business (česky Skype pro firmy) provádí audio a video hovory a chaty (včetně případého přenosu souborů) mezi

- ošetřujícím lékařem a pacientem nebo
- ošetřujícím lékařem a lékařem – specialistou,

a zpracovává tak

- údaje o pacientech včetně jejich anamnézy, záznamů o návštěvách a poznámek (zpráv) z vyšetření a
- dokumenty obsahující zprávy a informace o zdravotním vyšetření a zdravotním stavu.

Správce tedy zpracovává osobní údaje a citlivé (osobní) údaje podle ZoOOÚ.

Účel zpracování

Zpracování osobních údajů bude probíhat výhradně za účelem poskytování lékařské péče formou konzultací a/nebo konsilií.

Při tomto zpracování budou použity následující tituly zpracování:

- preventivní nebo pracovní lékařství, posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní péče či léčby a
- souhlas udělený subjektem údajů[10] (pro případy, které nespadají pod výše uvedené titul, zejména pod GDPR, článek 9, odstavec 2, bod h).

[10] V uvedeném případě musí správce vlastními prostředky zajistit zajištění souhlasu a jeho další správu.

Popis operací zpracování

Osobní údaje budou zpracovávány (přenášeny, odesílány, přijímány, ukládány, upravovány a čteny) výhradně v rámci činnosti poskytování zdravotní péče, a to v rámci konzultací a /nebo konsílií prostřednictvím

- telefonního a video hovoru mezi dvěma účastníky a konference více účastníků,
- chatu mezi dvěma nebo více účasníky,
- přenosu souborů mezi dvěma nebo více účastníky během telefonního a video hovoru, při chatu i mimo tyto aktivity včetně případů kdy je příjemce offline a
- přístup k archivu nahrávek telefonních a video hovorů a konferencí, záznamů chatů a uložených souborů[11].

Kromě výše uvedeného běžného zpracování osobních údajů bude probíhat výmaz těchto údajů po definovaném čase (viz [68] a [69]):

- Archiv nahrávek telefonních a video hovorů a záznamů chatů je uložen do mailboxu uživatele v Exchange Online a řídí se pravidly pro archivaci dat v mailboxu uživatele.
- Archiv nahrávek konferencí a uložených souborů je uložen ve službe Sharepoint Online po dobu maximálně 15 dní, v případě pravidelně opakované konference maximálně 15 dní od poslední konference v řadě.

Výše uvedené operace zpracování jsou nezbytné pro ochranu životně důležitých zájmů subjektu údajů. Jiné operace zpracování nebudou povoleny.

Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů[12]

Správce v rámci nezbytnosti a přiměřenosti řádně vyhodnotil rizika, že by zpracování mohlo omezit práva subjektů údajů jakož i výhody a dodatečné záruky, které zpracování pro práva subjektů údajů přináší. Správce dospěl při tomto vyhodnocení k závěru, že zpracování je prováděno pouze v rámci původního účelu a nijak nezasahuje do práv a oprávněných zájmů subjektů údajů.

Správce pečlivě vyhodnotil a buď produktovým nastavením či v rámci smluvních podmínek sjednaných se zpracovatelem zajistil, že všechna zákonná práva subjektů údajů zůstanou zpracováním nedotčena. Správce považuje za důležité, že zpracovatel poskytl v kapitole „Použití zákaznických dat“ PSO smluvní záruky, že zpracovávaná „data budou použita jen pro vlastní poskytování služby zákazníkovi“, že zpracovatel „nebude zákaznická data využívat ani z nich nebude odvozovat informace pro žádné reklamní či podobné komerční účely“ a že zpracovatel „nezískává k zákaznickým datům žádná práva s výjimkou práv, která společnosti Microsoft přidělí zákazník pro poskytování služeb online zákazníkovi.“

Zpracování na druhou stranu přináší následující výhody a dodateční záruky pro subjekty údajů spočívající v zajištění důvěrnosti, integrity a dostupnosti zpracovávaných údajů a odolnosti systémů a služeb zpracování, a to jak na technické, tak i na organizační úrovni.

[11] Jedná se archiv ve smyslu aplikace; toto ukládání nemá archivační charakter.
[12] Jedná se zde o vzorový text, který musí daný správce upravit dle svojí skutečné situace.

Bezpečnostní požadavky

Technologie zajišťující uvedené zpracování dat v systémech správce[13] budou splňovat následující minimání bezpečnostní požadavky:

- pokrytí explicitních požadavků GDPR a ZoOOÚ – viz kapitola 8.3.1.5,
- identifikace a autentizace všech osob přistupujících k datům v systémech správce,
- řízení přístupu k datům dle rolí,
- šifrování přenosů dat přes nedůvěryhodné prostředí,
- zajištění integrity uložených dat (jejich ochrany) před poškozením v důsledku akce neoprávněné osoby,
- zajištění integrity uložených dat (jejich ochrany) před poškozením v důsledku chyby hardware,
- audit všech přístupů na údaje a možnost prohlížení těchto záznamů o přístupech a
- cíl dostupnosti: RPO maximálně 5 minut a RTO maximálně 1 hodina.

Přístup k údajům

K údajům bude mít přístup

- pracovníci správce - zdravotnický personál a
- externí pracovníci (externí lékařští specialisté).

Pacient (subjekt údajů) bude mít k údajům přístup pouze prostřednictvím pracovníků správce; poskytování údajů v rámci konzultace není v této DPIA považováno za přístup k údajům.

Zpřístupnění údajů

Údaje budou sdílené výhradně v rámci zajištění poskytování zdravotní péče v případě konzultace s lékařem - specialistou.

8.3.1.2 POPIS HODNOCENÉHO INFORMAČNÍHO SYSTÉMU NEBO SLUŽBY

Základní popis logické a fyzické architektury

Posuzovaný informační systém se bude skládat z následujících částí:

- pracovní stanice správce (lékaře) nebo externího pracovníka vybavené OS, prohlížečem a kancelářským software MS Office nebo samostatným klientem Skype for Business,
- pracovní stanice pacienta,
- komunikační linky (LAN, internet),
- služeb Skype for Business, konkrétně
  - komunikace (telefonního a video hovor, chat, přenos souborů) a jejího záznamu do archivu a
  - přístup k informacím uloženým v archivu,
- služeb Azure, konkrétně služeb Azure AD pro správu uživatelů Office 365.

[13] U tohoto scénáře je nutné si uvědomit, že zajištění ochrany dat ze strany subjektů komunikujích se správcem (zejména subjektů a externích lékařu komunikujících pomocí služby Skype for Bussines) je mimo kontrolu správce. Proto se uvedené požadavky týkají pouze ochrany údajů uložených v systémech správce.

Pracovní stanice a komunikační linky LAN správce se budou nacházet v prostorách správce, pacientů a externích lékařských specialistů, ostatní části budou mimo tyto prostory nebo dokonce mimo Českou republiku.

Struktura zpracovávaných informací

Všechny zpracovávané informace budou primárně uloženy v rámci služby Skype for Business a to konkrétně

- v rámci telefonních a video hovorů, chatů
  - jméno, popřípadě jména, příjmení pacienta,
  - datum narození,
  - informace o zdravotním stavu a o výsledcích vyšetření pacientů,
- v rámci archivu nahrávky telefonních a video hovorů a konferencí, záznamy chatů a dalších uložených souborů ve výše uvedeném rozsahu.

Popis datových toků

Při zpracování údajů v informačním systému budou existovat následující datové toky:

- Pracovník správce (zaměstnanec nebo externí pracovník) nebo pacient (obecně uživatel) přenáší nestrukturované osobní a citlivé (osobní) údaje pomocí služby Skype for Business ve formě ve formě telefonních a video hovorů, konferencí, chatů a souvisejících dokumentů.
- Přenášené údaje jsou ukládané do archivu nahrávek telefonních a video hovorů a konferencí, záznamů chatů a uložených souborů služby Skype for Business, která tyto informace ukládá do interního uložiště služby ve formě jednotlivých dokumentů (nahrávek telefonních a video hovorů a konferencí, záznamů chatů a souvisejících dokumentů).
- Pracovník správce (uživatel) přistupuje do archivu a čte uložené nestrukturované osobní a citlivé (osobní) údaje ze služby Skype for Business, která tyto informace získává z interního uložiště služby ve formě jednotlivých dokumentů (nahrávek telefonních a video hovorů a konferencí, záznamů chatů a souvisejících dokumentů).
- Pracovník správce (uživatel) odstraňuje v rámci vyřazování z archivu nestrukturované osobní a citlivé (osobní) údaje ze služby Skype for Business, která tyto informace odstraňuje z interního uložiště služby ve formě jednotlivých dokumentů (nahrávek telefonních a video hovorů a konferencí, záznamů chatů a souvisejících dokumentů).

Popis rozhraní

Ve všech výše uvedených případech budou používána dvě rozhraní:

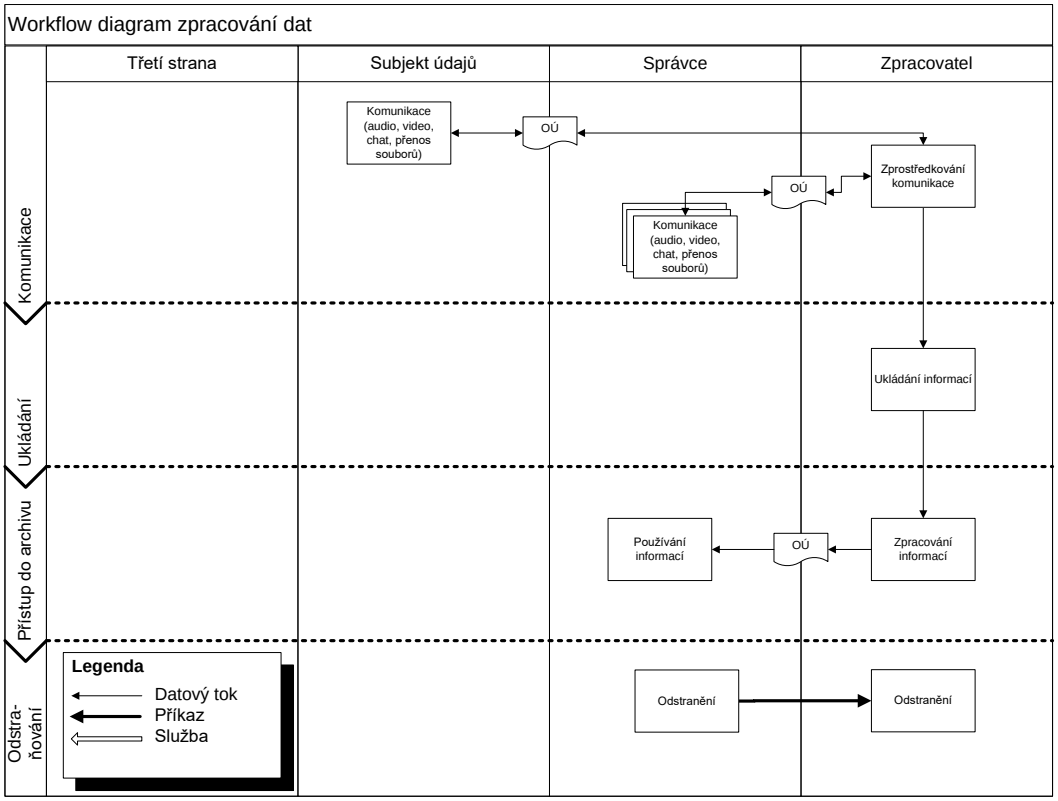
- Uživatelské rozhraní mezi pracovní stanicí a uživatelem ve formě klienta služby nebo prohlížeče (pro uživatele, kteří nemají instalovaného plnohodnotného klienta služby).
- Technické rozhraní ve formě rozhraní služby Office 365 Skype for Business dostupného protokolem HTTPS (HTTP/SIP přes TLS) a video/audio připojení (SRTP protokol).

Podmínkou je autentizace pracovníka správce (uživatele) ke službě Office 365 Skype for Business.

Workflow diagram zpracování dat

Metody zpracování dat jsou graficky zobrazeny na následujícím obrázku:

Obr. 3
Workflow diagram pro scénář 3



8.3.1.3 POPIS OPERAČNÍCH POSTUPŮ

Podle [33] je vhodné v rámci DPIA popsat plánované operační postupy správy a používání informačního systému, které mohu mít vliv na bezpečnost osobních údajů, zejména:

- koncept správy interních uživatelů (pracovníků správce) a jejich oprávnění,
- koncept správy externích pracovníků (osob, kterým bylo umožněno nahlédnout do příslušného dokumentu) a jejich oprávnění,
- koncept zajištění výkonu práv subjektu údajů, tedy jakým způsobem bude postupováno v jednotlivých případech, kdy subjekt údajů uplatné své právo[14],
- koncept provozu systému (služby), přičemž zde musí být uvedeno, že část systému je provozována externě, konkrétně v cloudové službě typu SaaS Office 365 Skype for Business,
- koncept zajištění podpory informačního systému, přičemž zde musí být zejména uvedeny subjekty, které se budou podílet na podpoře informačního systému včetně informací, zdali budou mít přístup k osobním údajům a případně odkud,
- koncept vytváření záznamů o činnosti pracovníků správce (zaměstnanců správce, pracovníků smluvních partnerů) a pracovníků podpory a vlastního systému (logování) včetně plánů na jejich další uchování,
- plány zálohování a obnovy (které mohou být vzhledem k plánovanému využití cloudové SaaS služby poměrně jednoduché),

[14] V prostředí Skype for Business nabízí poskytovatel služby podporu činností spojených s uplatněním práv subjektů v podobě standardních nástrojů typu vyhledávání, eDiscovery a řízení přístupu (například pro případ zablokování přístupu).

- ochrana a správa metadat,
- plány na uchování a odstranění dat a likvidaci médií,
- koncept zrušení informačního systému (ukončení smlouvy a případně postup vrácením osobních údajů správci).

Pozn: Vzhledem ke skutečnost, že uvedené oblasti nesouvisí přímo s analyzovanou službou a přitom jsou úzce spojené s konkrétní organizací, je vysoce pravděpodobné, že se budou v závislosti na organizaci správce lišit. V rámci této vzorové DPIA tedy není vypracován plnohodnotný vzor, ale pouze identifikovány doporučené oblasti pro další rozpracování.

8.3.1.4 POPIS INTERAKCE SE SUBJEKTEM ÚDAJŮ

Interakce s pacientem (subjektem údajů) se bude skládat z

- informování subjektu údajů,
- poskytování údajů subjektem údajů (např. v rámci vyšetření nebo konzultací),
- výkonu práv subjektu údajů (přístup k osobním údajům, oprava, výmaz, omezení zpracování a vznesení námitky).

Subjekt údajů bude informován o:

Tab. 16 Oblasti informování subjektu pro scénář 3

Požadavek GDPR	Komentář
Totožnost a kontaktní údaje správce a jeho případného zástupce	
Kontaktní údaje případného pověřence pro ochranu osobních údajů	Tento bod se uplatní dle rozsahu zpracování (jednotlivý lékař nemusí, nemocnice musí)
Účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování	Zpracování osobních údajů bude probíhat výhradně za účelem poskytování lékařské péče formou konzultací a/nebo konsilií. Právním základem (titulem) pro zpracování je: Preventivní nebo pracovní lékařství, posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní péče či léčby. Souhlas udělený subjektem údajů[15] (pro případy, které nespadají pod výše uvedený titul, zejména pod GDPR, článek 9, odstavec 2, bod h).
Oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);	Pravděpodobně se neuplatní
Případné příjemce nebo kategorie příjemců osobních údajů	Kromě subjektu údajů a pracovníků správce (vč. jeho smluvních partnerů) k údajům mohou přistupovat pouze osoby, které mají tento přístup povolen speciálním zákonem.

[15] V uvedeném případě musí správce zajistit zajištění souhlasu s jeho další správu.

Požadavek GDPR	Komentář
Případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny	Osobní údaje v případě využití Office 365 jsou předávány do zahraničí na základě článku 46 odst. 2 písm. c) GDPR, tedy na základě Standardních smluvních doložek přijatých Komisí podle čl. 93 odst. 2. Údaje o vhodných zárukách jsou uvedeny v rámci veřejně přístupných PSO, resp. Přílohy č. 2 PSO – Standardních smluvních doložkách.
Doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby	
Existence práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů	PSO stanoví v kap. „Použití zákaznických dat“, že správce osobních údajů (zákazník) si zachová všechna práva týkající se zákaznických dat. Z pohledu zpracovatele osobních údajů stanoví PSO v kap. „Přístup k zákaznickým datům“: (1) poskytovat zákazníkovi možnost opravit, odstranit nebo zablokovat zákaznická data, nebo (2) provádět takové opravy, odstranění nebo blokování jménem zákazníka. Správce osobních údajů má za tímto účelem k dispozici nástroje služby Office 365 jako jsou vyhledávání obsahu, eDiscovery (viz [34]), a auditní logy pro změny nebo výmazy obsahu.
Pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním	
Existence práva podat stížnost u dozorového úřadu	
Skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů	Pravděpodobně se neuplatní
Skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů	Pravděpodobně se neuplatní

Výkon práv subjektu údajů bude možné vykonávat žádostí u pracovníka správce nebo komunikací s dozorovým úřadem.

8.3.1.5 POŽADAVKY NA SOUKROMÍ A ZABEZPEČENÍ

Explicitní požadavky na soukromí a zabezpečení jsou dané

- zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (aktuálně) a
- nařízením 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 (od 25. 5. 2018).

Další požadavky na zabezpečení vyplývají z analýzy rizik.

8.3.2 ANALÝZA RIZIK

V této kapitole je vypracována vzorová analýza rizik v rámci DPIA, tedy posouzení rizik pro práva a svobody subjektů. Při této analýze rizik je postupováno podle metodiky vycházející z požadavků VoKB, ale upravené v oblasti dopadů tak, aby zohledňovala dopad na subjekt údajů (pacienta) – viz příloha č. 1.

8.3.2.1 KRITÉRIA PRO AKCEPTACI RIZIK

Kritéria pro aceptaci rizik jsou uvedena v příloze 1 (Metodika analýzy rizik), kapitole 3.2.
U jednotlivých rizik je uvedena osoba, která může příslušnou úroveň zbytkového rizika akceptovat a zda-li se jedná o vysoké riziko pro práva a svobody fyzických osob dle GDPR, které před zahájením zpracování vyžaduje konzultaci s dozorovým úřadem.

8.3.2.2 AKTIVA A JEJICH HODNOTY

Uložená nejvíce citlivá **datová aktiva** jsou z pohledu důvěrnosti, integrity a dostupnosti **ohodnocena** podle vodítek uvedených v příloze č. 1 hodnotami uvedenými v následující tabulce.

Tab. 17
Ohodnocení dat pro scénář 3

Aspekt	Úroveň	Zdůvodnění
Důvěrnost	Vysoká	Subjekt údajů bude vystaven vážným nepříjemnostem, které bude schopen překonat pouze se značnými obtížemi (zpronevěra finančních prostředků, blacklisting ze strany bank, škody na majetku, ztráta zaměstnání, předvolání k soudu, zhoršení zdravotního stavu, atd.). Zde předpokládán scénář přes dopad na soukromý život – konkrétně odmítnutí zaměstnání.
Integrita	Vysoká	Subjekt údajů bude vystaven vážným nepříjemnostem, které bude schopen překonat pouze se značnými obtížemi (zpronevěra finančních prostředků, blacklisting ze strany bank, škody na majetku, ztráta zaměstnání, předvolání k soudu, zhoršení zdravotního stavu, atd.). Zde předpokládán scénář modifikace uložených záznamů, což může vést ke špatné volně postupu léčby, a tedy následně ke zdravotním komplikacím.
Dostupnost	Nízká	Subjekt údajů buď nebude ovlivněn vůbec anebo bude vystaven drobným problémům, které bude schopen bez větších obtíží překonat (čas strávený opětovným zadání informací, nepříjemností, nepohodlí, podrážděnost, atd.). Zde předpokládám scénář výpadku služeb, kdy si pacient nebo lékař bude muset domluvit jiný termín komunikace.

Aspekt	Úroveň	Zdůvodnění
Ztráta	Střední	Subjekt údajů bude vystaven značným nepříjemnostem, které bude schopen za cenu jistých potíží překonat (zvýšení nákladů, odepření služby, strach, nepochopení, stress, malá fyzická újma, atd.). Zde předpokládán scénář ztráty záznamů v archivu, kdy bude nutné komunikaci opakovat.

Nepřímé újmy (např. subjekt utrpí psychickou újmu a následně bude muset podstoupit psychiatrickou léčbu) nemůže správce a ani zpracovatel předjímat a proto tato rizika nejsou zahrnuta.

V následující tabulce je uveden seznam všech identifikovaných aktiv s uvedením jejich popisu spolu s jejich typem podle přílohy č. 1.

Tab. 18
Seznam aktiv pro scénář 3

Typ aktiva	Aktivum	Popis
Datová aktiva	Přenášené hovory a uložené záznamy rozhovorů	Nestrukturovaná data obsahující kontaktní údaje a údaje o zdravotním stavu pacienta (soubory)
	Přenášené soubory a uložené přenášené soubory	
Služby	Služba Skype for Business	Komunikace a přenos souborů
	Komunikace s externími subjekty	Komunikace a přenos souborů s uživateli, kteří nejsou součástí služeb Skype fo Business poskytovaných správci
	Služba Azure AD	Rozhraní pro správu identit, autentizačních údajů a oprávnění

Vlastní ohodnocení identifikovaných aktiv vychází z výše uvedeného ohodnocení dat. V dalších částech analýzy se pro zjednodušení pracuje s Přenášenými hovory a uloženými záznamy rozhovorů a s Přenášenými soubory a uloženými přenášenými soubory dohromady jako s Datovými aktivy.

Tab. 19
Ohodnocení aktiv pro scénář 3

Aktivum	Důvěrnost	Integrita	Dostupnost	Ztráta
Datová aktiva	Vysoký	Vysoký	Nízký	Střední
Služba Skype for Business	Vysoký	Vysoký	Nízký	-
Komunikace s externími subjekty	Vysoký	Vysoký	Nízký	-
Služba Azure AD	Střední	Vysoký	Nízký	-

8.3.2.3 HROZBY A ZRANITELNOSTI

Seznam uvažovaných hrozeb je uveden v příloze č. 1, kapitola 2.2.1.

V případě **ohodnocení úrovní hrozeb** a **zranitelností** jsou hodnoty úrovní uvedeny přímo v tabulkách analýzy rizik (příslušné hodnoty se liší v závislosti na scénáři a aktivu, a proto není možné definovat jednu celkovou úroveň).

V této analýze uvedené hodnoty budou potom v případě konkrétní analýzy rizik IS správce nahrazeny hodnotami vycházejícími z charakteristik prostředí konkrétního správce.

8.3.2.4 OHODNOCENÍ RIZIK

Na uvedená aktiva byly namapovány relevantní hrozby uvedené v příloze č. 1, pro které byla určena jejich úroveň a následně i úroveň zranitelnosti, to vše za předpokladu neexistence bezpečnostních standardních opatření (jedná se tedy o teoretickou maximální hodnotu rizika uváděnou zejména za účelem porovnání s výslednou úrovní zbytkového rizika po implementaci opatření). Na základě toho byla určena **inherentní rizika** uvedená v tabulce Tab. 20 (sloupec „Inher. riziko“).

Následně byla rizika s úrovní vyšší než nízká (v tabulce případně označena zeleně) snížena opatřeními nabízenými poskytovatelem cloudových služeb a byla určena **zbytková rizika** uvedená ve stejné tabulce Tab. 20 (sloupec „Zbytkové riziko“).

Tab. 20 Rizika pro scénář 3

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbyt. riziko
Datová aktiva					
	Datová aktiva	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky správce	7	7
	Datová aktiva	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky poskytovatele	7	4
	Datová aktiva	Nesprávné řízení bezpečnosti	Nesprávné vyhodnocení SLA	6	6
	Datová aktiva	Nesprávné řízení bezpečnosti	Ztráta kontroly v důsledku akce poskytovatele	6	4
Služby					
	Služba Skype for Business	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	8	5
	Služba Skype for Business	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	9	5
	Služba Skype for Business	Zneužití systémových zdrojů	Obecná zranitelnost u správce	6	6
	Služba Skype for Business	Zavedení škodlivého software	Obecná zranitelnost ze strany správce	8	5
	Služba Skype for Business	Popření	Obecná zranitelnost	7	4
	Služba Skype for Business	Napadení komunikace	Obecná zranitelnost	7	5
	Služba Skype for Business	Přerušení komunikace	Obecná zranitelnost	5	4
	Služba Skype for Business	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	9	4
	Služba Skype for Business	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele	7	3
	Služba Skype for Business	Selhání software	Obecná zranitelnost u poskytovatele	7	3
	Služba Skype for Business	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele	5	1
	Služba Skype for Business	Selhání údržby	Obecná zranitelnost u poskytovatele	7	3
	Služba Skype for Business	Chyba uživatele	Obecná zranitelnost u správce	7	7

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbyt. riziko
	Služba Skype for Business	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	7	4
	Služba Skype for Business	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)	4	2
	Služba Skype for Business	Úmyslné poškození externími pracovníky	Obecná zranitelnost	4	1
	Služba Skype for Business	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	7	3
	Služba komunikace s externími IS	Zavedení škodlivého software	Zranitelnost u příchozí komunikace	8	4
	Služba komunikace s externími IS	Popření	Obecná zranitelnost	7	4
	Služba komunikace s externími IS	Napadení komunikace	Zranitelnost u příchozí komunikace	8	8
	Služba komunikace s externími IS	Napadení komunikace	Zranitelnost u odchozí komunikace	8	8
	Služba komunikace s externími IS	Přerušení komunikace	Obecná zranitelnost	5	4
	Služba komunikace s externími IS	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	9	4
	Služba komunikace s externími IS	Chyba uživatele	Zranitelnost u odchozí komunikace	8	8
	Služba Azure AD	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	8	4
	Služba Azure AD	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	9	4
	Služba Azure AD	Popření	Obecná zranitelnost	7	4
	Služba Azure AD	Napadení komunikace	Obecná zranitelnost	7	4
	Služba Azure AD	Přerušení komunikace	Obecná zranitelnost	5	4
	Služba Azure AD	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	9	4

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Inher. riziko	Zbyt. riziko
	Služba Azure AD	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele	7	3
	Služba Azure AD	Selhání software	Obecná zranitelnost u poskytovatele	7	3
	Služba Azure AD	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele	5	1
	Služba Azure AD	Selhání údržby	Obecná zranitelnost u poskytovatele	7	3
	Služba Azure AD	Chyba uživatele	Obecná zranitelnost u správce	7	6
	Služba Azure AD	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	6	2
	Služba Azure AD	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)	4	2
	Služba Azure AD	Úmyslné poškození externími pracovníky	Obecná zranitelnost	4	1
	Služba Azure AD	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	7	3

Detailní seznam inherentních a zbytkových rizik je uveden v příloze č. 4.

Úroveň některých rizik snížena nebyla, neboť se jedná o rizika, která musí být snížena opatřeními na úrovni správce (příslušné oblasti jsou zcela mimo vliv poskytovatele cloudových služeb). Jedná se zejména o tyto kombinace hrozeb a zranitelností:

- Zneužití práv (neoprávněná akce obsluhy) – Zneužití pracovníky správce,
- Nesprávné řízení bezpečnosti – Nesprávné vyhodnocení SLA,
- Zneužití systémových zdrojů - Obecná zranitelnost u správce,
- Chyba uživatele – Obecná zranitelnost u správce a Zranitelnost u odchozí komunikace,
- Napadení komunikace – Zranitelnost u příchozí komunikace (tato hrozba je mimo kontrolu správce) a
- Napadení komunikace – Zranitelnost u odchozí komunikace (tato hrozba je mimo kontrolu správce).

S výjimkou rizik, která musí být snížena opatřeními na úrovni správce a rizik na straně externích subjektů, **byla implementací opatření ostatní rizika snížena až na úroveň 5**, což je ve spodní části střední úrovně rizik (jedná se tedy o rizika, která **mohou být akceptovaná**, ale měla by být nadále sledovaná).

Pro snížení rizik byla použita opatření uvedená v kapitole 8.3.3 (sloupec AR).

Mapování opatření na rizika, která snižují, je uvedeno v příloze č. 4.

Rizika správce

V rámci analýzy rizik v rámci DPIA, která bude prováděna pro celý informační systém a nikoliv pouze pro služby Skype for Business, je nutné analyzovat nejenom rizika spojená se službami Office 365, ale i rizika spojená s zařízeními plně ve správě správce, na jejichž úroveň nemá společnost Microsoft v roli poskytovatele služeb Skype for Business žádný vliv.

V rámci DPIA tedy bude nutné navíc analyzovat následující rizika (popsaná kombinací akivum – hrozba - zranitelnost):

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

- Krádež externími pracovníky (včetně vybavení nebo dat) – Obecná zranitelnost (Nedostatek opatření)
- Úmyslné poškození interními pracovníky – Obecná zranitelnost (Nedostatek opatření)
- Úmyslné poškození externími pracovníky – Obecná zranitelnost (Nedostatek opatření)

- Aktivum: Komunikační linky
  - Přerušení komunikace – Nedostatečná SLA linky nebo nedostatek záložních linek

Pozn: Vzhledem ke skutečnosti, že uvedené oblasti nesouvisí přímo s analyzovanou službou a přitom jsou úzce spojené s konkrétní organizací, je vysoce pravděpodobné, že se budou v závislosti na organizaci správce lišit. V rámci této vzorové DPIA tedy není vypracován plnohodnotný vzor, ale pouze identifikována rizika, která musí být dále ohodnocena.

8.3.2.5 ANALÝZA SHODY

Tato DPIA je vytvářená z pohledu subjektu údajů, kdy jsou analyzovány dopady porušení zabezpečení osobních údajů na konkrétní subjekt údajů (pacienta), je tato kapitola omezena na splnění konkrétních požadavků stávající a budoucí legislativy zaměřených na zabezpečení informačního systému. Ostatní požadavky, které přímo nesouvisející s vlastním zabezpečením dat, jsou analyzovány v samostatné kapitole 7.

Požadavky GDPR

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
Článek 32, odst. 1	S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:		
Článek 32, odst. 1, písm. a)	a) pseudonymizace a šifrování osobních údajů;	II-10-1 II-10-2 II-12	10.13 10.15
Článek 32, odst. 1, písm. b)	b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;	I-1-0 I-2-0 I-3-0 I-4-0 I-5-0 I-6-0 I-7-0 I-8-0 I-9-0 I-10-0 I-11-0 I-12-0 I-13-0 II-1-0 II-2-0 II-3-0 II-4-0 II-5-0 II-6-0 II-7-0 II-8-0	všechna z 9 a 10

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
		II-9-0 II-10-1 II-10-2 II-11-0	
Článek 32, odst. 1, písm. c)	c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;	I-12-0 I-13-0 II-11-0	9.12 9.13 10.14
Článek 32, odst. 1, písm. d)	d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.	I-11-0 II-9-0	9.11 10.12

Požadavky ZoOOÚ

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
§ 13, odst. 1	Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.	I-1-0 I-2-0 I-3-0 I-4-0 I-5-0 I-6-0 I-7-0 I-8-0 I-9-0 I-10-0 I-11-0 I-12-0 I-13-0 II-1-0 II-2-0 II-3-0 II-4-0 II-5-0 II-6-0 II-7-0 II-8-0 II-9-0 II-10-1 II-10-2 II-11-0	všechna z 9 a 10
§ 13, odst. 2	Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.	I-3-0	9.3
§ 13, odst. 4	V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také		
	a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,	I-9-0 II-3-0 II-4-0	9.9 10.6 10.7

ID požadavku	Text požadavku	Opatření ID	Opatření kap.
	b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,	I-9-0 II-3-0 II-4-0	9.9 10.6 10.7
	c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a	II-6-0 II-8-0	10.9 10.11
	d) zabránit neoprávněnému přístupu k datovým nosičům.	I-9-0 II-1-0 II-3-0 II-4-0 II-10-1	9.9 10.4 10.6 10.7 10.13

8.3.3 IDENTIFIKOVANÁ OPATŘENÍ

V rámci analýzy rizik a identifkace opatření pro pokrytí legislativních požadavků byla identifikována následující bezpečnostní opatření:

Tab. 21
Opatření scénáře 3

ID	Kapitola	Název opatření	AR	Shoda
I-1-0	9.1	Systém řízení bezpečnosti informací	ano	ano
I-2-0	9.2	Řízení rizik	ano	ano
I-3-0	9.3	Bezpečnostní politika	ano	ano
I-4-0	9.4	Organizační bezpečnost	ano	ano
I-5-0	9.5	Stanovení bezpečnostních požadavků pro dodavatele	ano	ano
I-6-0	9.6	Řízení aktiv	ano	ano
I-7-0	9.7	Bezpečnost lidských zdrojů	ano	ano
I-8-0	9.8	Řízení provozu a komunikací	ano	ano
I-9-0	9.9	Řízení přístupu osob	ano	ano
I-10-0	9.10	Akvizice, vývoj a údržba	ano	ano
I-11-0	9.11	Kontrola a audit	ano	ano
I-12-0	9.12	Zvládání bezpečnostních událostí a bezpečnostních incidentů	ano	ano
I-13-0	9.13	Řízení kontinuity činností	ano	ano
II-1-0	10.4	Fyzická bezpečnost	ano	ano
II-2-0	10.5	Nástroj pro ochranu integrity komunikačních sítí	ano	ano
II-3-0	10.6	Nástroj pro ověřování identity uživatelů	ano	ano
II-4-0	10.7	Nástroj pro řízení přístupových oprávnění	ano	ano
II-5-0	10.8	Nástroj pro ochranu před škodlivým kódem	ano	ano
II-6-0	10.9	Nástroj pro zaznamenávání činnosti	ano	ano
II-7-0	10.10	Nástroj pro detekci kybernetických bezpečnostních událostí	ano	ano
II-8-0	10.11	Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	ano	ano
II-9-0	10.12	Aplikační bezpečnost	ano	ano
II-10-1	10.13	Kryptografické prostředky ochrana dat (v klidu)	ano	ano
II-10-2	10.13	Kryptografické prostředky ochrana dat (při přenosu)	ano	ano
II-11	10.14	Nástroj pro zajišťování úrovně dostupnosti informací	ano	ano
II-12	10.15	Pseudonymizace	ne	ne

Popis jednotlivých opatření je uveden v kapitolách č. 9 a 10.

9 KATALOG ORGANIZAČNÍCH OPATŘENÍ

Tato kapitola obsahuje seznam organizačních opatření nabízených cloudovými službami Microsoft Online Services, které přispívají nebo mohou přispět k zajištění důvěrnosti, integrity a dostupnosti dat, resp. služeb umístěných, resp. poskytovaných v cloudových službách.

Vzhledem k existenci ZoKB/VoKB, jejichž požadavky budou minimálně některé systémy zpracovající osobní údaje muset také plnit (například v roli provozovatelů základních služeb podle připravované novely ZoKB), byla organizační opatření rozdělena do skupin dle VoKB.

Bezpečnostní dokumentace

Popis jednotlivých bezpečnostních opatření (technických i organizačních v prostředí Microsoft Online Services) je uveden v bezpečnostní dokumentaci.

Pro zákazníky je základním zdrojem veřejných informací Microsoft Trust Center obsahující rozcestník pro všechny služby (http://www.microsoft.com/en-us/trustcenter). Vlastní bezpečnostní dokumentace je uložena na Microsoft Service Trust Portálu (STP) https://trustportal.office.com, který je přístupný administrátorům organizace po vytvoření Microsoft Office 365 nebo Microsoft Azure subskripce. Tito administrátoři mohou delegovat přístup do STP portálu pro další uživatele.

Ve studiích [1] a [2] možno nalézt podrobný popis bezpečnostní dokumentace Microsoft Online Services a Microsoft Office 365, na kterou je v této kapitole odkazováno.

9.1 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

V prostředí Microsoft Online Services je u klíčových služeb zaveden systém řízení bezpečnosti informací, certifikovaný v souladu s normou ISO/IEC 27001:2013, přičemž v rámci analyzovaného modelu informačního systému jsou relevantní následující procesy/služby:

- Microsoft's Cloud Infrastructure and Operations a
- Microsoft Azure.

Skutečnost, že výše uvedené procesy/služby jsou certifikované podle ISO/IEC 27001:2013 nemá přímý vliv na systém řízení bezpečnosti informací správce, jedná se však o formu ujištění, že služby a procesy související s outsourcingem, splňují normou stanovené bezpečnostní požadavky.

Více viz dokumenty popisující systém řízení bezpečnosti informací – [3], [86] a [87].

9.2 ŘÍZENÍ RIZIK

Vzhledem k celosvětové působnosti společnosti Microsoft, a tedy i služeb Microsoft Online Services, je kontrola zavedených opatření prováděna vůči požadavkům různých norem a standardů, přičemž záznamy těchto kontrol jsou zákazníkům dostupné ve formě auditních zpráv (viz [92], [93], [94], [95], [96] a [97]).

V rámci analyzovaného modelu informačního systému zahrnujícího služby Microsoft Office 365 je možné rozsah a stav zavedených bezpečnostních opatření zjistit z následujících dokumentů:

- Bezpečnostní politika „Microsoft Security Policy“
- Prohlášení o aplikovatelnosti pro jednotlivé služby
- Zprávy z auditu podle normy ISO/IEC 27001

Kromě toho platí, že společnost Microsoft provádí hodnocení a řízení rizik dle své metodiky, jejíž jádro je z velké části založeno na normách ISO/IEC 27001, ISO/IEC 27005 a je v souladu se standardem NIST 800-30. Soulad této metodiky s požadavky vyhlášky č. 316/2014 Sb., o kybernetické bezpečnosti, byl hodnocen nezávislým auditorem – viz [98].

9.3 BEZPEČNOSTNÍ POLITIKA

V prostředí Microsoft Online Services je implementováno množství bezpečnostních politik (a návazných bezpečnostních standardů), přičemž většina z nich je z bezpečnostních důvodů dostupná pouze pracovníkům společnosti Microsoft.

Pro zákazníky využívající služby Microsoft Office 365 jsou k dispozici dokumenty popisující zavedená opatření a jejich úroveň s podrobností nabízející základní přehled o opatřeních, ale zároveň nezvyšující rizika služeb Microsoft Online Services. Zejména se jedná o následující dokumenty:

- Bezpečnostní politika „Microsoft Security Policy“ (viz [3])
- Dokument „Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014“ (viz [90])
- Prohlášení o aplikovatelnosti pro jednotlivé služby (viz [88] a [89])
- Zprávy z auditu podle normy ISO/IEC 27001 (viz [92] a [93])

9.4 ORGANIZAČNÍ BEZPEČNOST

V prostředí Microsoft Online Services (konkrétně Office 365) je definována odpovědnost jednotlivých rolí v oblasti bezpečnosti informací i odpovědnost za bezpečnost informací celkově a jsou stanoveny požadavky na oddělení jednotlivých rolí. Kromě toho jsou zavedené týmy odpovědné za řešení bezpečnosti v konkrétních oblastech. Bližší podrobnosti je možné nalézt v [3], [90], [88] a [89].

Uvedené role však nijak nesouvisí s rolemi zavedenými správcem.

9.5 STANOVENÍ BEZPEČNOSTNÍCH POŽADAVKŮ PRO DODAVATELE

V případě služeb Microsoft Online Services (konkrétně Microsoft Office 365) jsou součástí licenční smlouvy také Podmínky pro služby online (viz. [4]) a Smlouva o úrovni služeb (viz. [5]), jejíž přílohou je standardní smluvní doložka ve smyslu čl. 26 odst. 2 směrnice 95/46/ES pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích.

Dokument obsahuje všeobecné obchodní podmínky pro služby online, přičemž mj. obsahuje

- podmínky ochrany osobních údajů
  - závazek užití dat pouze pro poskytování služeb,
  - závazek neposkytnutí dat třetím stranám kromě vyjmenovaných situací a procesů,
  - závazek napomáhat při ochraně bezpečnosti informací zákazníka,
  - závazek oznámení incidentu zabezpečení,
  - vymezení místa zpracování dat,
  - pravidla použití dodavatelů,
  - kontakt společnosti Microsoft v oblasti ochrany osobních údajů,
  - umístění uchování neaktivních zákaznických dat,
  - opatření pro zajištění soukromí – vrácení / smazání dat, pracovníci, subdodavatelé,
  - specifické podmínky pro Evropu,

- základní popis opatření, kterými společnost Microsoft zajišťuje ochranu dat zákazníků v oblastech
  - organizace zabezpečení informací,
  - správa prostředků,
  - zabezpečení lidských zdrojů,
  - fyzické zabezpečení a bezpečnost životního prostředí,
  - sdělení a správa operací,
  - řízení přístupu,
  - správa incidentů zabezpečení informací a
  - správa kontinuity podnikání,
- závazek společnosti provádět audity (např. podle ISO/IEC 27001, SSAE 16 / ISAE 3402, AT 101), a to pro každou službu minimálně jednou ročně, výsledky zpráv poskytnout definovaným způsobem zákazníkovi (na základě dohody o mlčenlivosti) a dohoda, že zákazník uplatňuje své právo auditu uvedeným způsobem s možností změny způsobu výkonu tohoto práva,
- standardní smluvní doložku vytvořenou v souladu s rozhodnutím Evropské komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice EU o ochraně osobních údajů[16].

Soulad metodik a postupů hodnocení rizik a zvládání rizik s požadavky Vyhlášky na straně Microsoft Online Services je možné doložit vyjádřením nezávislého auditora (viz [98]).

Provádění kontrol bezpečnostních opatření zavedených na straně Microsoft Online Services je možné doložit certifikací podle ISO/IEC 27001 spolu s následujícími podklady:

- Bezpečnostní politika „Microsoft Security Policy“ (viz [3])
- Prohlášení o aplikovatelnosti pro jednotlivé služby (viz [88] a [89])
- Zprávy z auditu podle normy ISO/IEC 27001 pro jednotlivé služby (viz [92] a [93])

Dalším způsobem kontroly účinnosti některých bezpečnostních opatření mohou být i auditní zprávy SOC 1 Type II a SOC 2 Type II (viz [94], [95], [96] a[97]).

Zákazníci Microsoft online services mají (jakožto povinné osoby) přístup k těmto podkladovým dokumentům včetně certifikace ISO/IEC 27001 pro účely vlastního řízení rizik prostřednictvím tzv. Service Trust Portálu[17].

Kromě výše uvedených opatření v oblasti ochrany osobních údajů a kontrol bezpečnostních opatření společnost Microsoft implementuje následující organizační specifická opatření:

1) Za účelem zamezení nejasného rozdělení odpovědností za implementaci bezpečnostních opatření společnost Microsoft ve všeobecných obchodních podmínkách „Volume Licensing: Podmínky pro služby online“ informuje správce, za které oblasti ručí Microsoft, kde si Microsoft nechává právo vlastního rozhodování, a jaké oblasti musí správce pokrýt vlastními silami. Zejména jsou tyto informace uvedeny v části „Podmínky ochrany osobních údajů a zabezpečení“, kde jsou uvedeny jak závazky společnosti, tak i případná zřeknutí se odpovědnosti, a v části "Zabezpečení", kde uveden zkrácený seznam opatření na straně Microsoftu včetně závazku tato opatření dodržovat. Kromě toho společnost Microsoft vytvořila informativní dokumenty „Embracing Cloud in Health: a European Risk Assessment Framework – A guide to privacy and security considerations for the adoption

[16] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf
[17] Microsoft Service Trust Portal: https://trustportal.office.com

of cloud services in the health sector“ (viz [99]) a „Shared Responsibilities For Cloud Computing“ [100] , ve kterých popisuje rozdělení odpovědnosti definovaných GDPR mezi sebe a správce.

2) Za účelem vyjasnění úrovně služeb společnost Microsoft ve všeobecných obchodních podmínkách „Volume Licensing: Smlouva o úrovni služeb pro Služby online společnosti Microsoft“ uvádí SLA (z pohledu dostupnosti jednotlivých služeb) a algoritmy finanční náhrady zákazníkovi v případě nedodržení úrovně SLA (ve formě kreditů služby).

3) Za účelem ověření účinnosti bezpečnostních opatření společnost Microsoft

   - pro obecné ověření účinnosti organizačních bezpečnostních opatření poskytuje auditní zprávy,
   - pro aktivní identifikaci zranitelností platformy Azure vypsala odměny za objevení a nahlášení zranitelností (bug bounty program, (https://technet.microsoft.com/en-us/security/dn425036).

4) V oblasti poskytování nezbytných informací pro provádění hodnocení rizik na straně správce společnost Microsoft na STP portálu poskytuje dokumentaci popisující implementovaná bezpečnostní opatření.

5) Za účelem zamezení neoprávněného poskytnutí dat mimo jurisdikci EU společnost Microsoft umožňuje správci zvolit ukládání a zpracování údajů výhradně v zemích EHP/EU. Výjimky z tohoto pravidla jsou popsány v Trust Center https://o365datacentermap.azurewebsites.net/, přičemž v tomto případě se zpracování provádí na základě standardní smluvní doložky, která je součástí všeobecných obchodních podmínek.

6) Za účelem zvýšení transparentnosti z pohledu certifikací společnost Microsoft ve všeobecných obchodních podmínkách „Volume Licensing: Podmínky pro služby online“ uvádí standardy a rámce řízení, kterými se řídí, s vymezením, že tento standard nebo rámec odstraní v případě, kdy se v odvětví již nepoužívá a byl nahrazen jiným standardem nebo rámcem.

7) V oblasti využívání služeb subdodavatelů společnost Microsoft přebírá zodpovědnost za subdodavatele a vede jejich seznam na webu (https://aka.ms/subcontractors). Dále se zavazuje minimálně 6 měsíců před poskytnutím oprávnění k přístupu novému dodavateli aktualizovat tento web a zákazníka o této změně informovat.

8) V oblasti neschopnosti dostát současným či budoucím legislativním požadavkům společnost Microsoft nabízí k dispozici věcné podklady a metodické materiály, které umožní zákazníkům být v souladu se současnými plošnými legislativními požadavky (minimálně v rozsahu požadavků uváděných v této studii – viz kapitola 7), samozřejmě za podmínky sdílené odpovědnosti za bezpečnost mezi společností Microsoft a správcem. Kromě toho společnost Microsoft ve svých všeobecných obchodních podmínkách deklaruje závazek, že dodrží veškeré zákony a předpisy, které se vztahují k provozování služeb online a na poskytovatele služeb informačních technologií, včetně zákonů týkajících se oznámení narušení bezpečnosti.

Ve věci nařízení GDPR společnost Microsoft v červnu 2016 vydala prohlášení, že v tuto chvíli ještě nemá zavedena všechna potřebná organizační opatření, ale garantuje zákazníkům svoji budoucí připravenost[18].

9) V oblasti neúplnosti nebo netransparentnosti obchodních podmínek společnost Microsoft poskytuje velmi obsažné všeobecné obchodní podmínky „Volume Licensing: Podmínky pro služby online“, které pokrývají všechny relevantní oblasti, zejména závazky v oblasti zabezpečení a ochrany soukromí.

10) Z pohledu hodnocení stability poskytovatele platí, že společnost Microsoft, která je nadnárodní a stabilní společností, deklaruje cloudové služby jako svoji strategickou prioritu, a tyto služby poskytuje již více než 20 milionům organizací nebo firem globálně. Cloudové služby jsou v portfoliu produktů společnosti Microsoft nejrychleji rostoucím segmentem.

11) Za účelem snížení možnosti nedostupnosti či výpadku služby společnost Microsoft v příloze pro „Podmínky pro služby online“ uvádí transparentní SLA. Společnost dále poskytuje portál s informacemi o aktuálním stavu dostupnosti cloudových služeb celosvětově, viz https://portal.office.com/servicestatus , a zavedla strukturovaný přístup k dostupnosti dat a služeb poskytovaných z datových center – na bázi tzv. Availability sets/Fault domains, a LRS/ZRS/GRS redundantní úložiště (viz kap. 10.14).

12) Za účelem identifikace oblastí, kde může docházet ke vzniku nepokrytých zbytkových rizik, společnost Microsoft vytvořila informativní dokumenty

- „Embracing Cloud in Health: a European Risk Assessment Framework – A guide to privacy and security considerations for the adoption of cloud services in the health sector“ (viz [99]) a
- „Shared Responsibilities For Cloud Computing“ (viz [100]),

ve kterých popisuje rozdělení odpovědnosti definovaných GDPR mezi sebe a správce a zdůrazňuje oblasti, na které se má správce zaměřit.

9.6 ŘÍZENÍ AKTIV

Z pohledu zpracovatele osobních údajů jsou v této oblasti zejména zajímavé mechanizmy ochrany údajů z oblasti šifrování dat.

Mechanizmy šifrování dat nativně nabízené prostředím Microsoft Online Services (konkrétně Microsoft Office 365) jsou uvedeny v kapitole 10.13.

Prostředí Microsoft Office 365 nenabízí nástroje pro zajištění pseudonymizace[19].

[18] Prohlášení společnosti Microsoft zákazníkům ve věci nařízení GDPR (červen 2016):
Microsoft's cloud business is grounded in four commitments. The security of data is our priority. We will ensure people's data is private and under their control. We will figure out the laws in each country and make sure data is managed accordingly. And we will be transparent so people know what we are doing.
The EU General Data Protection Regulation (GDPR) is a welcome step forward for the EU and is aligned with our cloud commitments. We are reviewing the GDPR and the manner in which we will ensure compliance of our enterprise Online Services when it goes into effect in May 2018. We'll share more specific details as our plans are finalized and will stand behind our contractual commitment to "comply with all laws and regulations applicable to [our] provision of the Online Services.

[19] Zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

9.7 BEZPEČNOST LIDSKÝCH ZDROJŮ

V prostředí Microsoft Online Services (konkrétně Microsoft Office 365) jsou bezpečnostní opatření v oblasti bezpečnosti lidských zdrojů zavedena a kontrolována, a to minimálně v oblastech

- kontroly spolehlivosti pracovníků[20],
- zvyšování bezpečnostního povědomí,
- disciplinárního řízení,
- zachování mlčenlivosti,
- vracení aktiv pracovníkem v případě ukončení pracovního vztahu.

Bližší podrobnosti je možné nalézt v dokumentech [90], [88] a [89].

9.8 ŘÍZENÍ PROVOZU A KOMUNIKACÍ

V prostředí Microsoft Online Services (konkrétně Microsoft Office 365) jsou bezpečnostní opatření v oblasti řízení provozu a komunikací zavedena a kontrolována, a to minimálně v oblastech

- provozní pravidla a postupy,
- zálohování a obnovy,
- škodlivého software,
- definované základní konfigurace bezpečnostní funkcionality,
- řízení změn,
- instalace software,
- záznamů událostí,
- řízení kapacity a výkonu,
- řízení zranitelností,
- přístupu k dokumentaci a
- ochrany koncových bodů.

Bližší podrobnosti je možné nalézt v dokumentech [3], [90], [88] a [89].

[20] Společnost Microsoft provádí kontrolu spolehlivosti zaměstnanců a dodavatelů pracujících u zákazníků nebo majících možnost přístupu k osobním údajům zákazníků, a to minimálně na základě informací o zaměstnancově nebo dodavatelově minulosti, přičemž u vybraných rolí je prováděna důkladnější kontrola spolehlivost zahrnující mj. i bezpečnostní prověrku. Při kontrole spolehlivosti je zejména prověřována kriminální historie nebo kontrola správnosti a úplnosti předložených dokladů nebo sdělených informací. Do ukončení kontroly spolehlivosti není zaměstnanci nebo dodavateli povolen přístup.
Více viz dokument [90], opatření z cíle A.7.1.

9.9 ŘÍZENÍ PŘÍSTUPU A BEZPEČNÉ CHOVÁNÍ UŽIVATELŮ

V prostředí Microsoft Online Services (konkrétně Microsoft Office 365) jsou bezpečnostní opatření v oblasti řízení přístupu a bezpečného chování uživatelů zavedena a kontrolována, a to minimálně v oblastech

- politiky řízení přístupu,
- schválení a kontroly přístupu (interní proces LockBox),
- minimálního oprávnění,
- externích přístupů,
- autentizace,
- standardních uživatelských účtů,
- používaní privilegovaných programů,
- odebírání přístupu.

Bližší podrobnosti je možné nalézt v dokumentech [3], [90], [88] a [89].

9.10 AKVIZICE, VÝVOJ A ÚDRŽBA

V prostředí Microsoft Online Services (konkrétně Microsoft Office 365) jsou bezpečnostní opatření v oblasti akvizice, vývoje a údržby zavedena a kontrolována, a to minimálně v oblastech

- definování a sledování plnění požadavků na bezpečnost,
- použití strategie ochrany do hloubky,
- bezpečného vývoje software,
- kontroly integrity dat a
- kontroly bezpečnostních funkcí.

Bližší podrobnosti je možné nalézt v dokumentech [3], [90], [88] a [89].

9.11 KONTROLA A AUDIT KRITICKÉ INFORMAČNÍ INFRASTRUKTURY A VÝZNAMNÝCH INFORMAČNÍCH SYSTÉMŮ

V prostředí Microsoft Online Services (konkrétně Microsoft Office 365) jsou bezpečnostní opatření kontrolována a auditována.

Provádění jednotlivých kontrol a auditů včetně jejich zaměření a případných nálezů společnost Microsoft dokládá zprávami z auditu, které jsou jejím zákazníkům k dispozici. Vybrané zprávy z auditu jsou uvedeny v [92], [93], [94], [95], [96] a [97].

9.12 ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

V prostředí Microsoft Online Services (konkrétně Office 365) jsou bezpečnostní opatření v oblasti zvládání kybernetických bezpečnostních událostí a incidentů zavedena a kontrolována s tím, že se společnost Microsoft zavazuje zákazníkovi ohlásit vznik bezpečnostního incidentu, spočívajícího v nezákonném přístupu k datům zákazníka, jehož výsledkem je ztráta, zveřejnění nebo změna zákaznických dat.

Bližší podrobnosti je možné nalézt v dokumentech [3], [4], [90], [88] a [89].

9.13 ŘÍZENÍ KONTINUITY ČINNOSTÍ

V prostředí Microsoft Online Services (konkrétně Microsoft Office 365) jsou bezpečnostní opatření v oblasti řízení kontinuity činností zavedena a kontrolována tak, aby zajistila úroveň služeb definovanou v dokumentu „Smlouva o úrovni služeb pro Služby online společnosti Microsoft“ (viz [5]) – typicky dostupnost 99,9%.

Bližší podrobnosti o nasazených opatřeních je možné nalézt v dokumentech [3], [90], [88] a [89].

10 KATALOG TECHNICKÝCH OPATŘENÍ

Tato kapitola obsahuje seznam technických opatření nabízených cloudovými službami Microsoft Online Services, které přispívají nebo mohou přispět k zajištění důvěrnosti, integrity a dostupnosti dat, resp. služeb umístěných, resp. poskytovaných v cloudových službách.

Vzhledem k existenci ZoKB/VoKB, jejichž požadavky budou minimálně některé systémy zpracovající osobní údaje muset také plnit, byla technická opatření rozdělena do skupin dle VoKB.

10.1 OPATŘENÍ PRO ZAJIŠTĚNÍ DŮVĚRNOSTI

Pro tabulku Tab. 22 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 22 Opatření pro zajištění důvěrnosti

Komponenta systému	**Úroveň vysoká**	**Úroveň kritická**
Předepsaná úroveň ochrany	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací vnější komunikační sítí jsou chráněny pomocí kryptografických prostředků.	Pro ochranu důvěrnosti je požadována evidence osob, které k aktivům přistoupily, a metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.
Příklady informací	**Informace, které nepožívají ochrany dle speciálního zákona** **Obecné osobní údaje**	**Citlivé (osobní) údaje** **Obecné osobní údaje, u kterých bylo správcem vyhodnoceno vyší riziko pro subjektu údajů nebo se vyskytují ve větším množství**
Scénář 1 - Sharepoint Online	Office 365 Security & Compliance Center a audit na úrovni Sharepoint Online, viz 10.9 TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.5 a 10.13. Azure Right Management Service, viz 10.13	Customer LockBox, viz 10.7. Azure Log Analytics pro pokročilé vyhodnocování logů, viz 10.9. Office 365 Per-File Encryption, viz 10.13 nebo Office 365 Advanced Encryption s Azure Key Vault, viz 10.13. Více faktorová autentizace, viz 10.6.
Scénář 2 - Exchange Online/ Outlook	Office 365 Security & Compliance Center a audit na úrovni Exchange Online, viz 10.9 TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.5 a 10.13. Office 365 Message Encryption, viz 10.13 nebo Azure Right Management Service, viz 10.13 nebo End-to-End šifrování mailů pomocí S/MIME, viz 10.13.	Customer LockBox, viz 10.7. Azure Log Analytics pro pokročilé vyhodnocování logů, viz 10.9. Office 365 Advanced Encryption s Azure Key Vault, viz 10.13. Více faktorová autentizace, viz 10.6.

Komponenta systému	Úroveň vysoká	Úroveň kritická
Skype for Business Online	Office 365 Security & Compliance Center a audit na úrovni Sharepoint Online, viz 10.9 TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.5 a 10.13. Azure Right Management Service, viz 10.13.	Customer LockBox, viz 10.7. Azure Operations Management Suite pro pokročilé vyhodnocování logů, viz 10.9. Office 365 Per-File Encryption, viz 10.11 nebo Office 365 Advanced Encryption s Azure Key Vault, viz 10.13. Více faktorová autentizace, viz 10.6.

10.2 OPATŘENÍ PRO ZAJIŠTĚNÍ INTEGRITY

Pro tabulku Tab. 23 platí, že opatření, která jsou uvedena na nižších úrovních, se uplatní i na úrovně vyšší.

Tab. 23
Opatření pro zajištění integrity

Komponenta systému	Úroveň vysoká	Úroveň kritická
Předepsaná úroveň ochrany	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených vnějšími komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (např. pomocí technologie digitálního podpisu).
Příklady informací	**Informace, které nepožívají ochrany dle speciláního zákona** **Obecné osobní údaje**	**Citlivé (osobní) údaje** **Obecné osobní údaje, u kterých bylo správcem vyhodnoceno vyší riziko pro subjektu údajů nebo se vyskytují ve větším množství**

Komponenta systému	Úroveň vysoká	Úroveň kritická
Scénář 1 - Sharepoint Online	Office 365 Security & Compliance Center a audit na úrovni Sharepoint Online, viz 10.9 TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.5 a 10.13.	Customer LockBox, viz 10.7. Azure Operations Management Suite pro pokročilé vyhodnocování logů, viz 10.9. Office 365 Per-File Encryption, viz 10.11 nebo Office 365 Advanced Encryption s Azure Key Vault, viz 10.11. Více faktorová autentizace, viz 10.6. Zajištění integrity dat je nutné řešit na aplikační úrovni – například podepisování dokumentů digitálním podpisem (Microsoft Office, Acrobat Reader).
Scénář 2 - Exchange Online/ Outlook	Office 365 Security & Compliance Center a audit na úrovni Exchange Online, viz 10.9 TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.5 a 10.13. Office 365 Message Encryption, viz 10.13 nebo Azure RMS pro Exchange Online, viz 10.13 nebo Podpis mailů pomocí S/MIME, viz 10.13.	Customer LockBox, viz 10.7. Azure Operations Management Suite pro pokročilé vyhodnocování logů, viz 10.9. Office 365 Advanced Encryption s Azure Key Vault, viz 10.11. Více faktorová autentizace, viz 10.6.
Skype for Business Online	Office 365 Security & Compliance Center a audit na úrovni Sharepoint Online, viz 10.9 TLS pro aplikační protokoly (HTTP, SMTP a další), viz 10.5 a 10.13. Azure RMS pro Exchange Online, viz 10.13.	Customer LockBox, viz 10.7. Azure Operations Management Suite pro pokročilé vyhodnocování logů, viz 10.9. Office 365 Per-File Encryption, viz 10.11 nebo Office 365 Advanced Encryption s Azure Key Vault, viz 10.11. Více faktorová autentizace, viz 10.6. Zajištění integrity dat je nutné řešit na aplikační úrovni – například podepisování dokumentů digitálním podpisem (Microsoft Office, Acrobat Reader).

10.3 OPATŘENÍ PRO ZAJIŠTĚNÍ DOSTUPNOSTI

Opatření pro zajištění dostupnosti odpovídají požadavkům VoKB, příloha 1, úroveň vysoká.

Tato opatření jsou popsaná v kapitole 10.14.

10.4 FYZICKÁ BEZPEČNOST

V oblasti fyzické bezpečnosti je prostředí Office 365 chráněno následovně:

Bezpečnostní politika společnosti Microsoft (Microsoft Security Policy, viz [3]) definuje požadavky na fyzickou bezpečnost a bezpečnost prostředí, které zahrnují:

- definování pravidel pro zabránění neoprávněnému fyzickému přístupu nebo poškození a rušení informací,
- zabránění a kontrola neoprávněného fyzického přístupu k produkčním informačním systémům a zařízením,
- zabránění a kontrola neoprávněného fyzického přístupu k citlivým informačním systémům a zařízením,
- ochrana informačních systémů proti neplánovaným výpadkům, jako jsou výpadky proudu, selhání vybavení a ohrožení životního prostředí.

Dokumenty popisující fyzickou bezpečnost prostředí Microsoft Online Services jsou přehledně uvedeny v dokumentu Protecting Data in Microsoft Online Services (viz [32]) v kapitole 9.2.

10.5 NÁSTROJ PRO OCHRANU INTEGRITY KOMUNIKAČNÍCH SÍTÍ

Microsoft Office 365 poskytuje možnosti ochrany komunikačních sítí, viz [4]:

- Protože Office 365 využívá technologie Microsoft Azure, automaticky využívá možností zabezpečení, která poskytují technologie Azure (viz dále v této kapitole).
- Office 365 je poskytován jako SaaS a proto není možné definovat architekturu služeb, serverů, síti ani jejich bezpečnostní parametry. Tato oblast bezpečnosti je zajišťována společností Microsoft.
- Vzdálená správa služeb Office 365 je prováděna prostřednictvím webového rozhraní Office 365 portálu. Přístup k tomuto portálu je zabezpečen autentizací, kdy je možné:
  - Využít federované autentizace proti internímu Active Directory nebo jiné kompatibilní adresářové službě
  - Využít dvou faktorovou autentizaci v rámci Azure Active Directory nebo pomocí federované autentizace.
  - Integrita a důvěrnost přenášených dat je zajištěna použitím protokolu TLS.
- Pro přístup ke službám Office 365 se používají různé síťové protokoly, jako například HTTPS, POP3, IMAP, SMTP a další. Tyto protokoly jsou zabezpečeny pomocí protokolu TLS.

- Pro některé případy je možné využít zabezpečení přenášených dat na aplikační úrovni:
  - Azure Rights Management (Azure RMS) pro zabezpečení obsahu jednotlivých dokumentů nebo mailů.
  - Secure/Multipurpose Internet Mail Extensions (S/MIME) pro šifrování a digitální podepisování mailů.
  - Office 365 Message Encryption, využívá Azure RMS, řeší zabezpečení mailů zasílaných externím uživatelům a partnerům.
  - SMTP TLS pro partnery umožňuje při použití certifikátů konfigurovat mezi definovanými poštovními servery šifrování na úrovni protokolu SMTP.

Microsoft Azure poskytuje možnosti ochrany na úrovni datového centra Azure v několika úrovních, viz [4] a [7] (uvádíme pouze informace relefoantní pro Office 365, úplný popis lze nalézt v [32], kapitola 10.2.4):

- zablokování neautorizované komunikace do a uvnitř datového centra s použitím:
  - izolace prosazované na několika úrovních
    - komunikace mezi virtuálními servery vždy prochází přes paketový filtr (firewall),
    - virtuální server není schopen komunikovat na úrovni 2. vrstvy ISO/OSI modelu a tudíž nemůže odposlouchávat síťovou komunikaci, která není určena přímo jemu,
    - virtuální server nemůže odeslat DHCP odpověď, pouze DHCP požadavek. Pouze Network Manager – komponenta Azure infrastruktury smí odesílat DHCP odpovědi,
    - virtuální servery nemohou komunikovat s klíčovými virtuálními servery Azure infrastruktury,
    - segmentace sítě je zajištěna pomocí Azure virtuálních sítí (Azure Virtual Network – VNET), virtuální síť může obsahovat jeden nebo více IP v4 subnetů. V rámci nasazení (deployment) je možné vytvořit množství VNET. Pomocí Network Security Group (firewallů) lze nastavit potřebnou komunikaci (definovat ACLs). Network Security Group může být přiřazena virtuální síti nebo jednotlivému síťovému adaptéru virtuálního serveru. Virtuální servery mohou být připojeny do jedné VNET. Na úrovni virtuálního síťového adaptéru lze řídit síťovou komunikaci pomocí interního firewallu virtuálního serveru nebo pomocí Network Security Group (firewallů),
  - překladu IP adres – NAT, komponenta Endpoint,
  - fyzického oddělení backend serverů od Internetu
  - použití privátních IP adres
    - po instalaci je virtuálnímu serveru v Microsoft Azure přidělena privátní IP adresa, která není z principu z Internetu dostupná,
    - pro zajištění přístupu z Internetu k virtuálnímu serveru je nutné vytvořit a konfigurovat Endpoint, který má přiřazenou veřejnou IP adresu a na kterém se nastavuje povolená komunikace (ACLs),

- šifrování síťové komunikace je zajištěno v následujících případech:
  - komunikace mezi datovými centry,
  - komunikace mezi lokalitou zákazníka a datovým centrem Azure. Tuto komunikaci lze zašifrovat pomocí:
    - End to End s použitím protokolu TLS (například HTTPS),
    - pronajatý okruh mezi lokalitou zákazníka a datovým centrem Azure pomocí služby Express Route, které ale nešifruje data přenášená přes WAN – šifrování komunikace je nutné zajistit vlastními silami na úrovni aplikačních prtokolů,
- zabezpečení vzdáleného přístupu a vzdálené správy
  - přístup k portálu správy je zašifrován pomocí protokolu TLS 1.2,
  - další zabezpečení vzdáleného přístupu je možné pomocí:
    - využití připojení přes pronajatý okruh (služba Express Route),
    - omezení přístupu z Internetu pro vyjmenované IP adresy,

10.6 NÁSTROJ PRO OVĚŘOVÁNÍ IDENTITY UŽIVATELŮ

Oblast nástroje pro autentizaci uživatelů je v prostředí Office 365 realizována následovně:

Microsoft provozuje multi-tenant cloudovou adresářovou službu a službu správy identit – Azure Active Directory, viz [40]. Azure AD podporuje autentizaci

- jménem a heslem,
- více-faktorovou autentizaci,
  - autentizace jménem a heslem je ještě doplněna o autentizaci pomocí zařízení,
  - telefonickým hovorem,
  - textovou zprávou,
  - mobilní aplikací – notifikací,
  - mobilní aplikací – ověřovacím kódem,
  - OATH tokenem.
- Základní verze více-faktorové autentizace je součástí služby Office 365, rozšířená je dostupná v rámci doplňkové služby Azure Multi-Factor Authentication.

Azure AD více faktorovou autentizaci lze použít v případech:

- autentizace administrátora (Azure subscription) k Microsoft Azure,
- autentizace uživatelů ke službám využívajícím Azure AD (včetně on-premise služeb).

Azure AD umožňuje definovat politiku hesel na úrovni předplatného nebo domény, viz [41]. Výchozí nastavení politiky hesel je následující:

- délka hesla 8–16 znaků,
- maximální doba platnosti hesla 90 dní, hodnotu lze měnit,
- oznámení o ukončení platnosti hesla 14 dní před ukončením, hodnotu lze měnit
- ukončení platnosti hesla je zakázané (heslo nevyprší), hodnotu lze měnit,
- minimální doba platnosti hesla – poslední heslo nelze znovu použít,
- historie hesel bez omezení,
- zamykání účtu; po deseti neplatných pokusech o přihlášení musí uživatel opsat zobrazený text (CAPTCHA), což zajišťuje ochranu před automatizovaným útokem.

Azure AD obsahuje funkci správy privilegovaných identit (Privileged Identity Management, viz [39]), která umožňuje spravovat řídit a monitorovat privilegované identity / organizační role:

- Global Administrator,
- Billing Administrator,
- Service Administrator,
- User Administrator,
- Password Administrator.

Správa privilegovaných identit obsahuje funkce:

- zjištění, kteří uživatelé AD jsou administrátory Azure,
- povolení on-demand „just in time“ administrátorského přístupu,
- reporty o historii přístupu administrátora a o změnách rolí,
- notifikace o přístupu k administrátorské roli.

Azure AD podporuje integraci s interními adresářovými službami (On-Premise Directory), viz [25], pomocí:

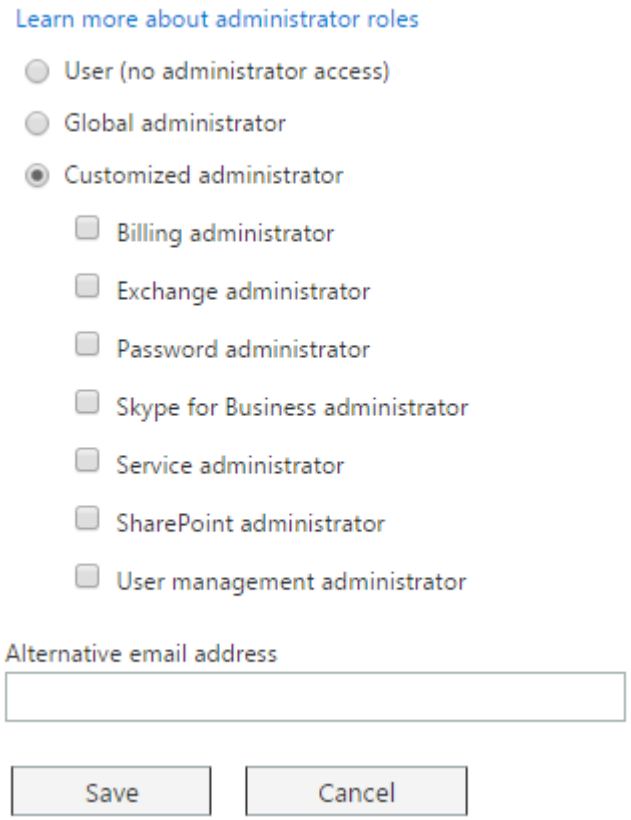
- synchronizace identit
  - identity jsou synchronizované, hesla mohou být různá s různou politikou a musí být udržována separátně,
- synchronizace identit a hesel (synchronizuje se hash hesla)
  - identity i hesla jsou synchronizovaná, uživatelé používají jedno heslo ke cloudovým i on-premise systémům. Změna hesla je propagována napříč synchronizovanými adresářovými službami,
- federace identit
  - informace o identitě je synchronizována s Azure AD, vlastní autentizace ale zajišťuje on-premise adresářová služba (například Active Directory).

10.7 NÁSTROJ PRO ŘÍZENÍ PŘÍSTUPOVÝCH OPRÁVNĚNÍ

Oblast nástroje pro řízení přístupových oprávnění je v prostředí Office 365 realizována následovně:

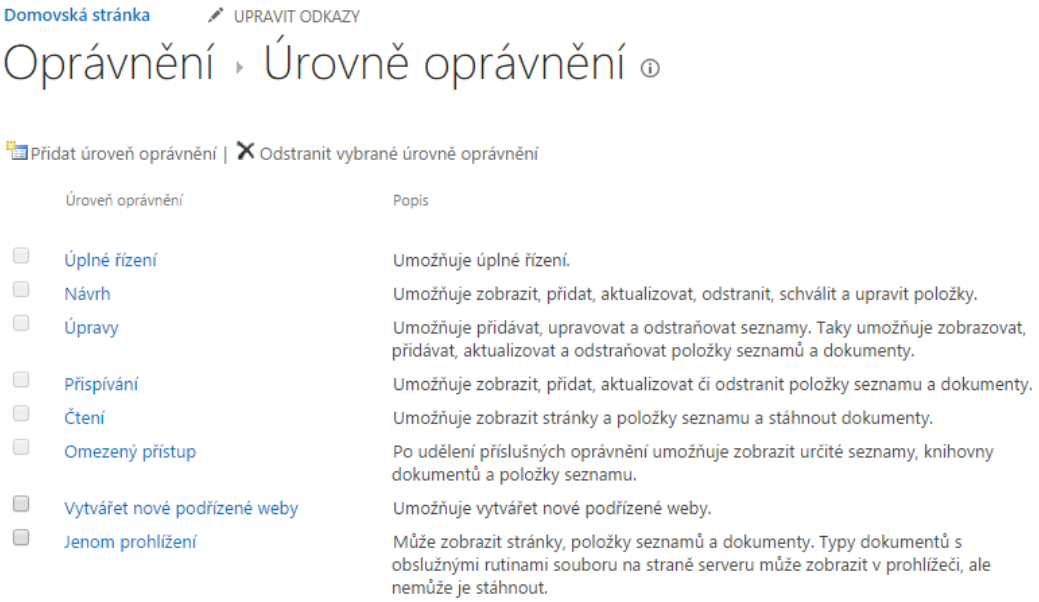
Office 365 obsahuje vlastní administrátorské role. Tyto role mohou být přiřazeny na úrovni portálu správy Office 365.

Obr. 4
Administrátorské role Office 365



Jednotlivé části Office 365, jako Exchange, Sharepoint a další mají vlastní portály správy (dostupné z portálu Office 365), kde je možné přiřazovat specifické administrátorské i uživatelské role a v rámci těchto částí.

Obr. 5
Přístupová oprávnění webu Sharepoint



- Externí uživatelé
  - Exchange Online umožňuje sdílení kalendářů s externími uživateli (viz [77]).
    - Sdílení kalendářů s externími uživateli může nakonfigurovat pouze správce příslušné Exchange Online organizace.
    - Sdílení lze nakonfigurovat na úrovni organizačních vztahů (jiná organizace Office 365 nebo on-premise organizace), nebo na úrovni politik pro sdílení (ostatní uživatelé internetu nebo uživatelé on-premises Exchange).
    - V rámci sdílení kalendářů lze určit úroveň přístupu k míře sdílených detailů:
      - Bez přístupu k záznamu.
      - Přístup k informaci o dostupnosti (volno, obsazeno).
      - Přístup k informaci o dostupnosti (volno, obsazeno) včetně konkrétního času, předmětu a lokality kalendářového záznamu.
  - Sharepoint Online umožňuje sdílet data s externími uživateli:
    - Sdílení dat s externími uživateli může nakonfigurovat pouze správce příslušné Sharepoint Site nebo uživatel s plnými oprávněními ke sdílenému Sharepoint Site nebo dokumentu.
    - Externí uživatelé se musí být autentizovat pomocí svého účtu Microsoft Account (účet pro veřejné cloudové služby Microsoft) nebo účtu v Azure AD své organizace.
    - Sharepoint umožňuje sdílet data pomocí linku pro anonymní sdílení – každý kdo zná link k datům k nim získá přístup. Linku pro anonymní sdílení lze zrušit.
  - Skype 4 Bussiness umožňuje komunikaci s externími uživateli
    - Externí uživatelé přistupují prostřednictvím Skype4Business Web App
    - V rámci meetingu mají externí uživatelé přístup k souborům, které jsou s meetingem spojené

Customer LockBox

Customer Lockbox pro Office 365 je navržen tak, aby zákazníkům poskytl bezprecedentní kontrolu nad jejich daty ve službě. Customer Lockbox dává zákazníkům explicitní kontrolu ve velmi vzácných případech, kdy může inženýr společnosti Microsoft potřebovat přístup k obsahu zákazníka za účelem vyřešení problému zákazníka.

Služby Microsoft Office 365 jsou vyvinuty tak, že pro svůj běh nevyžadují přístup zaměstnanců společnosti Microsoft k zákaznickým datům. Ten může být potřeba pouze při řešení požadavků nebo problémů zákazníka. V těchto případech je přístup umožněn a kontrolován pomocí Customer Lockboxu, který zajistí, že Microsoft inženýr nedostane přístup k obsahu zákazníka bez výslovného souhlasu zákazníka. Když zákazník dostane žádost o přístup, může žádost zkoumat a buď schválit, nebo odmítnout. Dokud není žádost schválena, nebude přístup Microsoft inženýrovi umožněn.

Veškeré aktivity jsou logovány a dostupné v rámci Office 365 Management API služby, případně prostřednictvím standardních nástrojů (jako například PowerShell).

Více informací o Customer Lockboxu pro Office 365 je uvedeno v dokumentu [32].

10.8 NÁSTROJ PRO OCHRANU PŘED ŠKODLIVÝM KÓDEM

V oblasti Microsoft Office 365 je ochrana před škodlivým kódem realizována prostřednictvím Microsoft Antimalware, který zajišťuje automatickou ochranu pro:

- Exchange Online Protection (EOP), viz [9]
  - Antispamová a antimalwareová ochrana příchozích a odchozích mailů
  - Multi-engine ochrana
  - Ochrana v reálném čase
  - Přednostní aktualizace signatur a definic
- Exchange Online Advanced Threat Protection, viz [10]
  - Ochrana příloh proti neznámému škodlivému kódu
  - Ochrana proti zákeřným odkazům v reálném čase
  - Pokročilé reporty a sledování vektoru útoku
- Sharepoint Online
  - Antimalwareová ochrana pro soubory ukládané do Sharepoint Online
- Skype for Business
  - Soubory sdílené mezi uživateli v rámci hovorů a konferencí jsou ukládány do Exchange Online nebo Sharepoint Online, a je využita jejich antimalwareová ochrana..

10.9 NÁSTROJ PRO ZAZNAMENÁVÁNÍ ČINNOSTÍ INFORMAČNÍCH SYSTÉMŮ, JEJICH UŽIVATELŮ A ADMINISTRÁTORŮ

Office 365 auditing umožňuje sledovat činnost a auditovat změny na úrovni Office 365 pomocí reportů (Service Usage Reports, viz [21]) a Compliance reportů (dostupné v compliance centru Office 365). Jsou k dispozici Compliance reporty, které využívají auditní logování. Toto logování musí být nejprve administrátorem Office 365 povoleno. Auditní informace jsou uchovávány v Office 365 po dobu 90 dnů. Informace o událostech lze získávat pomocí reportů, exportu reportů a pomocí PowerShellu.

Auditní reporty jsou rozděleny do kategorií:

- Office 365 audit log report
- Azure AD reports
- Exchange audit report
- Data loss prevention
  - Shody se zásadami a pravidly ochrany před únikem informací
  - Falešně pozitivní výsledky a přepsání zásad ochrany před únikem informací

Reporty (service usage reporty) jsou rozděleny do kategorií:

- Mail
  - Active and inactive mailboxes
  - New and deleted mailboxes
  - New and deleted groups
  - Mailbox usage
  - Types of mailbox connections
- Použití
  - Browser used
  - Operating systém used
  - Licensing vs Active Usage
- Skype for Business
  - Active users
  - Peer-to-peer sessions
  - Conferences
  - Audio minutes and video minutes
  - Client devices
  - Client devices per user
  - User activities
  - PSTN usage
  - Users blocked
- SharePoint
  - Tenant storage metrics
  - Team sites deployed
  - Team site storage
- OneDrive for Business
  - OneDrive for Business sites deployed
  - OneDrive for Business storage

- Auditing
  - Mailbox access by no-owners
  - Role group changes
  - Mailbox content search and hold
  - Mailbox litigation holds
  - Azure AD reports
- Ochrana
  - Top senders and recipients
  - Top malware for mail
  - Malware detection
  - Spam detection
  - Sent and received mail
- Pravidla
  - Top rule matches for mail
  - Rule matches for mail
- DLP
  - Top DLP policy maches for mail
  - Top DLP rules matches for mail
  - DLP policy matches by severity for mail
  - DLP policy matches, overrides and false positive for mail

Office 365 Management Activity API je RESTful API, které poskytuje přístup ke všem záznamům o uživatelských a administrátorských aktivitách uvnitř Office 365, viz 10.11.

Auditní záznamy vznikají i v doplňkových cloudových službách, které slouží pro zajištění důvěrnosti a intergrity dat. Tyto služby jsou uvedeny v kapitolách 10.1 a 10.2.

Synchronizace času

Synchronizace času v prostředí Microsoft Online Services je zajištěna službami cloudové platformy. Synchronizace času probíhá při startu virtuálního serveru nebo cloudové služby. Pomocí změny konfigurace lze nastavit synchronizaci i interval synchronizace s jiným zdrojem přesného času.

10.10 NÁSTROJ PRO DETEKCI KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

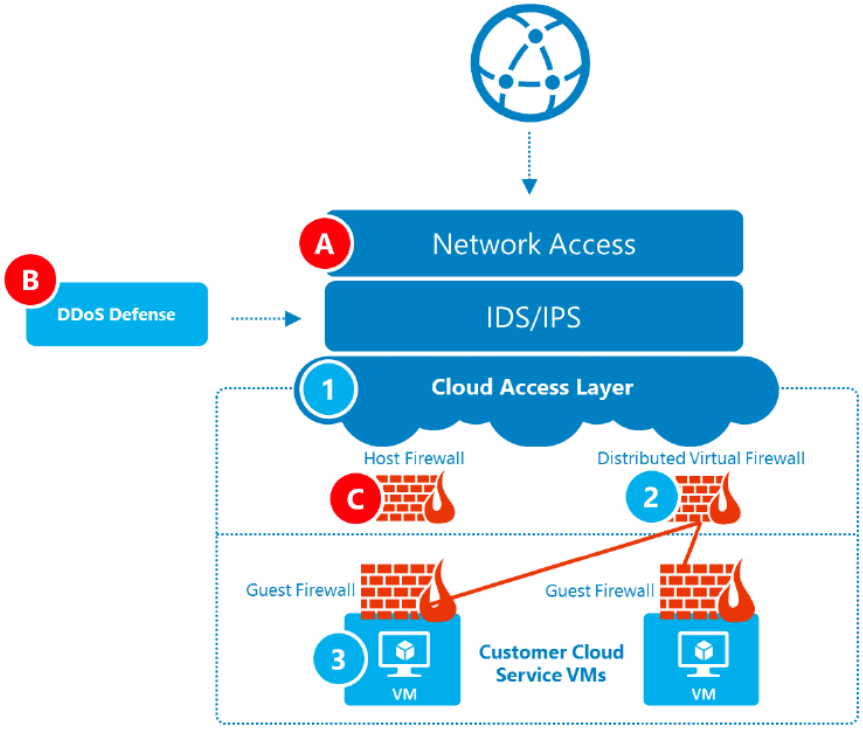
Oblast nástroje pro detekci kybernetických bezpečnostních událostí je v prostředí Office 365 realizována následovně:

Office 365 je provozován na platformě Microsoft Cloud Infrastructure and Operations (MCIO) která poskytuje služby pro detekci kybernetických bezpečnostních událostí a ochranu proti nim (viz [19]).

Obr. 6
Schéma datové sítě MCIO

Součástí ochrany je monitoring sítě a penetrační testování. Ochrana sítě je navržena jak pro ochranu proti vnějším útokům, tak i pro ochranu proti útokům od ostatních zákazníků Azure (ochrana mezi Azure tenanty). MCIO obsahuje distribuovaný DDoS obranný systém (viz [20]), který pomáhá Office 365 chránit. Tento systém používá standardní detekční a obranné mechanismy na úrovni síťového spojení.

Obr. 7
Úrovně ochrany infrastruktury MCIO



10.11 NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

Oblast nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí je prostředí Microsoft Online Services realizována následovně:

Office 365

Provozní stav a charakteristiky jednotlivých služeb Office 365 včetně platformy, na které jsou tyto služby provozovány, viz [12] je monitorován. Při provozu služeb jsou generovány logy událostí a auditní logy. Tyto logy jsou zašifrovaným kanálem přenášeny ke zpracování a následně zpracovávány (agregace a analýza) a vyhodnocovány interní službou na zpracování big dat – bezpečnostně analytický systém COSMOS, který využívá technologie Azure Machine Learning. Před vlastním zpracováním dat dochází k jejich anonymizaci.

Výstupem zpracování jsou reporty a notifikace, které slouží k zjištění možné podezřelé aktivity v produkčním prostředí. Odhalené zranitelnosti jsou následně v souladu s interní politikou řešeny, viz Obr. 8.

Obr. 8
Životní cyklus reakce na bezpečnostní incident, viz [22]

Office 365 Security & Compliance Center

Office 365 Security & Compliance Center umožňuje sledovat činnost a auditovat změny na úrovni Office 365 pomocí reportů Service Usage Reports a Compliance Reports. Auditní reporty Compliance Reports využívají auditní logování, které musí být nejprve administrátorem Office 365 povoleno. Auditní informace jsou uchovávány v Office 365 po dobu 90 dnů. Informace o událostech lze získávat pomocí reportů, exportu reportů a pomocí Powershellu.

Auditní reporty Compliance Reports jsou rozděleny do kategorií:

- Office 365 audit log report
- Azure AD reports
- Exchange audit report
- Data loss prevention
  - Shody se zásadami a pravidly ochrany před únikem informací
  - Falešně pozitivní výsledky a přepsání zásad ochrany před únikem informací

Reporty Service Usage Reports jsou rozděleny do kategorií:

- Mail
  - Active and inactive mailboxes
  - New and deleted mailboxes
  - New and deleted groups
  - Mailbox usage
  - Types of mailbox connections
- Použití
  - Browser used
  - Operating systém used
  - Licensing vs Active Usage
- Skype pro Firmy
  - Active users
  - Peer-to-peer sessions
  - Conferences
  - Audio minutes and video minutes
  - Client devices
  - Client devices per user
  - User activities
  - PSTN usage
  - Users blocked
- SharePoint
  - Tenant storage metrics
  - Team sites deployed
  - Team site storage
- OneDrive pro Firmy
  - OneDrive for Business sites deployed
  - OneDrive for Business storage
- Auditing
  - Mailbox access by no-owners
  - Role group changes
  - Mailbox content search and hold
  - Mailbox litigation holds
  - Azure AD reports
- Ochrana
  - Top senders and recipients
  - Top malware for mail
  - Malware detection
  - Spam detection
  - Sent and received mail

- Pravidla
  - Top rule matches for mail
  - Rule matches for mail
- DLP
  - Top DLP policy maches for mail
  - Top DLP rules matches for mail
  - DLP policy matches by severity for mail
  - DLP policy matches, overrides and false positive for mail

Office 365 Management Activity API je RESTful API, které poskytuje přístup ke všem záznamům o uživatelských a administrátorských aktivitách uvnitř Office 365, viz [12] a [13]. Výhody management API zahrnují:

- Přístup k více než 150 typům transakcí
- Aktivity logy z SharePoint Online, Exchange Online and Azure Active Directory a dalších Office 365 služeb
- Konzistentní schema napříč všemi logy
- Jednoduché zapnutí a vypnutí a aktivity logů

Prohledávání logů je umožněno pomocí nástroje Audit Log Search který pomocí grafického rozhraní nebo powershellu umožňuje prohledávat unifikované auditní logy, které obsahují informace o:

- Uživatelské činnosti v SharePoint Online a OneDrive for Business
- Uživatelské činnosti v Exchange Online
- Činnosti administrátorů v Sharepoint Online
- Činnosti administrátorů v Exchange Online
- Činnosti administrátorů v Azure AD

Dále jsou k dispozici možnosti auditování na aplikační úrovni jednotlivých komponent Office 365, viz [14]. Rozsah i auditované události jsou dokumentovány v dokumentu, viz [15]:

- Exchange Online, viz [16]
  - Mailbox auditing
    - Sledování přístupu k mailboxu a dalších aktivit, viz [17]
  - Administrator auditing
  - Non-owner mailbox access
  - Administrator role group
  - In-place eDiscovery & Hold
  - Litigation hold per mailbox
  - Export mailbox audit
  - Admin audit log
  - External admin audit log
    - Aktivita jiných než vlastních administrátorů (například zaměstnanců společnosti Microsoft)

- Pro SharePoint Online a OneDrive for Business jsou jednotlivé typy zaznamenávaných událostí uvedeny v dokumentu, viz [18]. K dispozici jsou následující auditní reporty:
  - Content modification
  - Content type and list modifications
  - Content viewing
  - Deletion
  - Run a custom report
  - Expiration and Disposition
  - Policy modifications
  - Auditing settings
  - Security settings

Azure Log Analytics

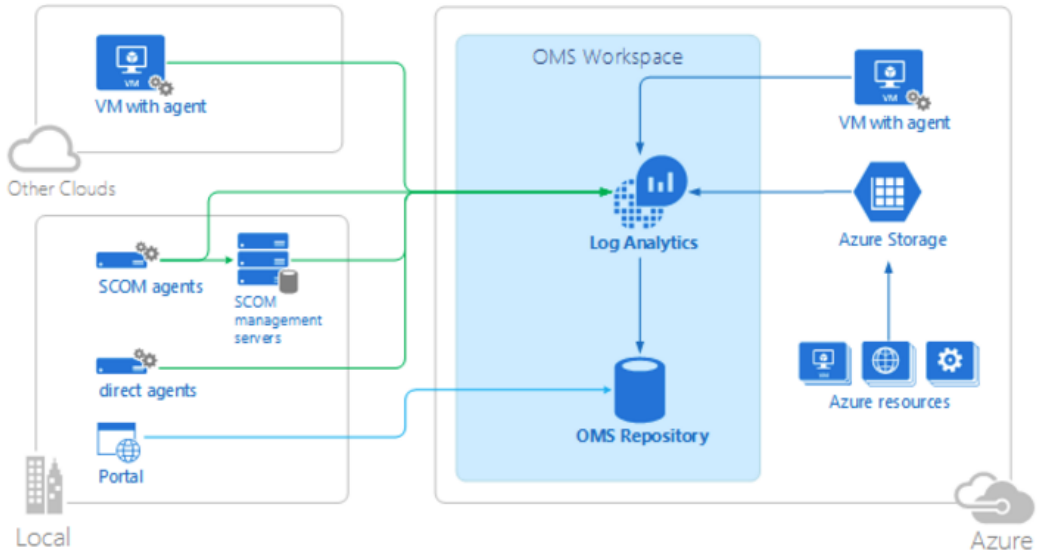
Microsoft Azure v rámci Operations Management Suite (OMS), obsahuje službu Log Analytics, která umožňuje sběr, kombinaci, korelaci a vizualizaci dat, která jsou generovaná v cloudovém i on-premise prostředí. Služba poskytuje upravitelný dashboard pro analýzu milionů událostí napříč prostředími v reálném čase, více informací viz [23].

Pro analýzu logů z Office 365 je k dispozici OMS Solution for Office 365[21] – při jeho aktivaci je napojena služba Log Analytics na Office 365 tenant, přebírá jeho logy a zpracovává je, například:

- monitorovat aktivitu uživatelů,
- monitorovat aktivitu administrátorů,
- detekovat nežádoucí uživatelské aktivity.

Azure Log Analytics umožňuje sběr i zdalších systémů včetně On-Premise IT organizace, které mohou doplnit informace získané z Office 365 do uceleného pohledu.

Obr. 9
Schéma Log Analytics



[21] Zatím jako public preview (v provozu od 5/2016, stav z 1.4.2017).

Synchronizace času

Synchronizace času v prostředí Microsoft Online Services je zajištěna službami cloudové platformy. Synchronizace času probíhá při startu virtuálního serveru nebo cloudové služby. Pomocí změny konfigurace lze nastavit synchronizaci i interval synchronizace s jiným zdrojem přesného času.

10.12 APLIKAČNÍ BEZPEČNOST

Oblast aplikační bezpečnosti je v prostředí Microsoft Online Services realizována následovně:

Vývoj software

Společnost Microsoft řídí veškerý vývoj software prostřednictvím procesu Bezpečný vývojový životní cyklus (Security Development Lifecycle), který je navržen tak, aby pomáhal snižovat závažnost i počet zranitelností kódu při neustále se měnících požadavcích. Těmito pravidly se řídí nejen vývoj aplikací, ale také vývoj cloudového operačního systému, který pro svůj provoz využívá cloudová infrastruktura.

V rámci vývoje dochází k testování software v oblastech:

- dynamická analýza
  - ověření funkčnosti a monitorování chování aplikace
    - porušení paměti,
    - použití privilegií,
    - kontrola kritických bezpečnostních aspektů,
- fuzzy testování
  - vyvolání selhání záměrným použitím poškozených nebo náhodných dat,
- posouzení plochy útoku
  - posouzení plochy útoku a modelu hrozeb po dokončení kódu,
  - přezkoumání nových vektorů útoků (v reakci na provedené změny) a jejich minimalizace.

Office 365 a Microsoft Azure

Průběžné zvyšování bezpečnostní konfigurace prostředí je zajišťováno konceptem Red Team & Blue Team (červený tým útočí a modrý tým útoku brání), viz [22], jedná se o pokročilou formu penetračního testování.

Ochrana aplikací a informací v prostředí Microsoft Online Services je zajištěna následovně:

- Autentizace administrátorů k Microsoft Azure a Office 365 je zajištěna pomocí Azure AD.
- Autentizace uživatelů k Office 365 je zajištěna pomocí Azure AD samostatně anebo federací s jinou autoritativní adresářovou službou, viz dokument [25].
- Autentizace k Office 365 a Microsoft Azure může být více faktorová. Toto nastavení lze vynutit na úrovni jednotlivých uživatelů.
- Řízení přístupu je zajištěno pomocí řízení přístupu pomocí rolí (RBAC).
- Audit přístupu k informacím včetně zaznamenávání typu provedené operace je realizováno pomocí auditních logů, diagnostického logování a sad reportů, viz kapitola 10.11.

- Ochrana informací při přenosu vnějšímu sítěmi je zajištěna
  - Pomocí protokolu HTTPS s využitím protokolu TLS 1.2.
  - Pomocí Site-to-Site VPN, která využívá protokol IPSec, konfigurační parametry, včetně algoritmů jsou uvedeny v dokumentu [26]
- Ochrana integrity elektronickým podpisem je k dispozici pro
  - Veškeré dokumenty vytvořené v Microsoft Office. Tyto dokumenty lze podepisovat klientským certifikátem na klientské zařízení, privátní klíč klientské zařízení neopouští. Tato funkcionalita je vestavěná do Microsoft Office
  - Podepisování elektronické pošty. Elektronickou poštu lze podepisovat klientským certifikátem na klientském zařízení, privátní klíč klientské zařízení neopouští. Tato funkcionalita je vestavěná do Microsoft Outlook a dalšího klientského software spolupracujícího s poštovním serverem Exchange
  - Jakékoliv dokumenty a elektronickou poštu prostřednictvím Azure Rights Management, viz [28].

Doba ukládání

Doba ukládání dat v prostředí Office 365 je řízena zásadami uchovávání, které je možné upravovat (viz [68], [69] a [78]).

10.13 KRYPTOGRAFICKÉ PROSTŘEDKY

Oblast kryptografických prostředků je v prostředí Microsoft Online Services realizována následovně:

Office 365

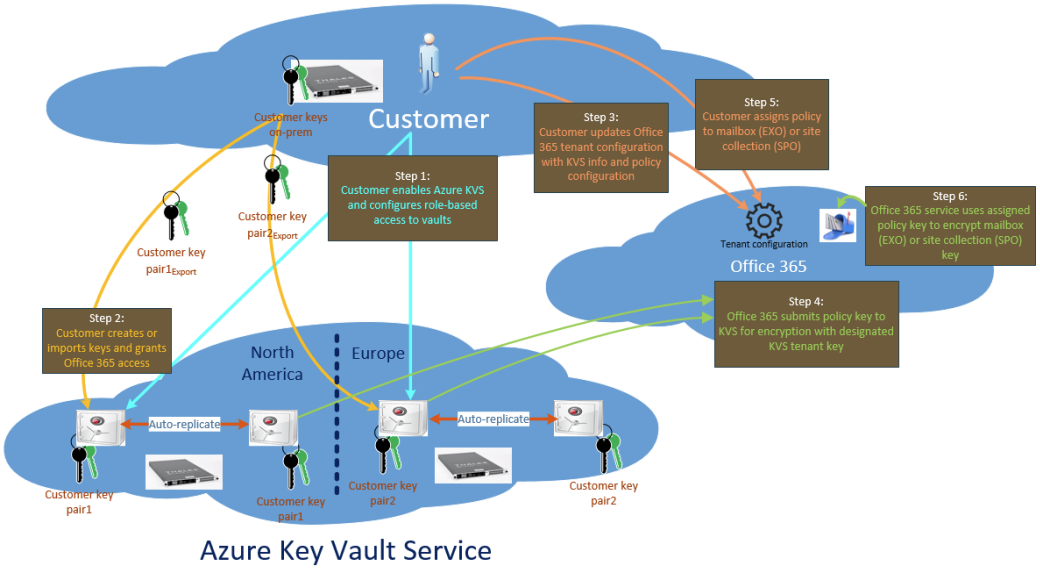
Pro ochranu data uložených v Office 365 jsou využity následující kryptografické prostředky pro šifrování uživatelských dat (viz [4]):

- Šifrování uložených dat na úrovni diskových svazků (Volume-level Encryption) ve službách ve službách Exchange Online, SharePoint Online (včetně OneDrive for Business) a Skype for Business:
  - Office 365 využívá technologii Microsoft BitLocker pro šifrování všech zákaznických dat uložených na úrovni diskových svazků pro eliminaci hrozeb souvisejících se ztrátou, krádeží nebo nesprávně vyřazenými fyzickými disky nebo počítači.
  - Microsoft BitLocker využívá kryptografický algoritmus se 128 nebo 256 bitovými klíči. Nové servery využívají pouze klíče s délkou 256 bitů, starší servery mohou využívat i klíče s délkou 128 bitů.
  - Microsoft BitLocker využívá dvě kategorie klíčů:
    - BitLocker Managed klíče, které jsou přiřazeny instalaci operačního systému serveru nebo šifrovanému disku. Tyto klíče jsou smazány a resetovány během reinstalace serveru nebo formátování disku.
    - BitLocker Recovery klíče, které jsou spravovány mimo BitLocker, ale jsou určeny pro šifrování disků. Tyto klíče jsou využity v případě, že je přeinstalován operační systém serveru, který obsahuje zašifrované disky. Dále jsou využívány službou Exchange Online Managed Availability Diagnostic v případě, kdy je nutné odemknout diskový svazek.
  - Klíč použitý pro zašifrování diskového svazku (Full Volume Encryption Key) pomocí BitLockeru je zašifrován pomocí hlavního klíče diskového svazku (Volume Master Key), které jsou uloženy v zabezpečeném sdíleném adresáři a přístupné pouze prověřeným a pověřeným osobám. Hlavní klíče jsou chráněny pomocí Passphrase, které jsou uloženy v Secure Store. Ten při přístupu k uložené Passphrase vyžaduje

vysokou úroveň oprávnění a schválení přístupu a přístupy jsou logovány. Schvalování přístupů zajišťuje jiná skupina než ta, která o přístup ke klíči žádá.

- Kryptografické algoritmy použité v BitLockeru byly validovány podle FIPS 140-2 (viz [38]) v rozsahu:
  - Cryptographic Module Specification
  - Cryptographic Module Ports and Interfaces
  - Finite State Model
  - Operational Environment
  - Design Assurance
  - Mitigation of Other Attacks
  - Self-Tests
- Office 365 Per-File Encryption zajišťuje ochranu uložených dat v produktech Skype for Business, OneDrive for Business a SharePoint Online.
  - Princip šifrování dat při ukládání spočítá v šifrování souborů před jejich uložením do Azure Storage. Při přístupu k souboru jsou data po načtení z úložiště před odesláním uživateli dešifrovány. Azure Storage nemá schopnost dešifrovat, identifikovat nebo rozpoznat uložený obsah.
  - Detailní popis způsobu ochrany dat včetně použitých šifrovacích algoritmů a způsobu správy klíčů je uveden v dokumentu [4]
- Office 365 Advanced Encryption zahrnuje šifrování na úrovni souborů (File-level Encryption) a zpráv (Message-level Encryption):
  - Office 365 Advanced Encryption umožňuje využít Azure Key Vault pro uložení klíčů, pro:

Obr. 10
Office 365 Advanced Encryption, viz [4]



- SharePoint Online včetně OneDrive for Business:
  - Všechny soubory v SharePoint Online jsou před uložením do Azure Storage zašifrovány pomocí AES s náhodně generovaným klíčem o délce 256 bitů. Před tím, než si uživatel soubor stáhne ze SharePoint Online je soubor získaný z Azure Storage dešifrován. Na úrovni infrastruktury Microsoft Azure nejsou k dispozici šifrovací klíče k uživatelským souborům služby SharePoint Online.
  - Uložené soubory jsou rozděleny do bloků, každý blok je zašifrován vlastním náhodným klíčem. Bloky jsou náhodně rozděleny mezi více Azure Storage Account.

        - Klíče jednotlivých bloků jsou zašifrovány hlavním klíčem souboru a jsou uloženy v SharePoint Content databázi společně s mapou uložení jednotlivých bloků souboru. Hlavní klíč souboru je uložen v odděleném SharePoint Secret Store a zašifrován pomocí Farm Key a zálohován do centrálního SharePoint Secret Store. Hlavní klíče jsou pravidelně jednou za 60 dní změněny a klíče bloků uložené v SharePoint Content databázi jsou při této příležitosti přešifrovány.
        - Hesla pro použitá pro Azure Storage Account jsou uložena v centrálním SharePoint Secret Store a delegovány do jednotlivých SharePoint farem podle potřeby. Jsou používána oddělená hesla Azure Storage Account pro zápis a pro čtení. Hesla pro Azure Strorage Account jsou pravidelně měněna po 60 dnech.
        - SharePoint Online tak odděluje vlastní soubory (Azure Storage), informace o místě uložení a šifrování souborů (SharePoint Content databáze) a informace potřebných pro získání a dešifrování souborů (Key Storage) do třech nezávislých komponent, které jsou fyzicky oddělené – bez přístupu ke všem třem komponentám není možné získat přístup k obsahu souborů.
    - Skype for Business:
        - Uživatelská data ve formě souborů a prezentací, které byly nahrány účastníky konference, zašifruje server Web Conferencing pomocí AES s klíčem 128 bitů. Zašifrované soubory jsou uloženy do sdíleného adresáře. Náhodně generovaný klíč s délkou 128 bitů je uložen v XML souboru obsahující data o konferenci. Tento XML soubor je zašifrován náhodně generovaným hlavním klíčem konference (Conference Master Key).
        - Uživatel si v klientské aplikaci může stáhnout soubory přiložené ke konferenci – stáhne si zašifrovaný soubor pomocí HTTPS a klientská aplikace si od Web Cenferencing serveru vyžádá šifrovací klíč pro jeho dešifrování. Klientská aplikace při přihlášení ke konferenci protokolem SIP over TLS získá od Web Conferencing serveru autentizační Cookie, kterou využívá pro autentizaci při stažení souborů přiložených ke konferenci.
    - Office 365 Message Encryption
        - Proprietární šifrování mailů s využitím technologie Microsoft Rights Management Service (RMS).
        - Při použití cloudové služby Azure RMS jsou pro šifrování mailů využity kryptografické algoritmy RSA s délkou klíčů 2048 bitů, AES s délkou klíčů 128 bitů a SHA-2.
        - Při použití on-premise Active Directory RMS mohou být použity dva režimy – Cryptographic Mode 1 – RSA s délkou klíčů 1024 bitů, AES s délkou klíčů 128 bitů a SHA-1 a Cryptographic Mode 2 – RSA s délkou klíčů 2048 bitů, AES s délkou klíčů 128 bitů a SHA-2.
- Šifrování mailů pomocí S/MIME:
    - Exchange Online podporuje End-to-End šifrování mailů ve formátu S/MIME a to včetně webového uživatelského rozhraní Outlook Web Access. Použité kryptografické algoritmy jsou závislé na konfiguraci mailového klienta a použitých certifikátech. Servery služby Exchange Online nemají k dispozici šifrovací klíče a nemohou získat obsah mailů.
- Pro šifrování uživatelských dat přenášených po Internetu se používá protokol TLS v rámci aplikačních protokolů HTTP, POP3, IMAP, SMTP, SIP a dalších:
    - Používány jsou pouze protokoly TLS 1.0, 1.1 a 1.2.
    - Preferovány jsou kombinace kryptografických algoritmů využívající výměnu klíčů pomocí algoritmu Diffie-Hellman založený na eliptických křivkách (ECDHE) s délkou klíčů 384 (preferovaná) nebo 256 bitů. Z důvodů kompatibility se staršími klienty jsou povoleny kombinace algoritmů využívající pro výměnu klíčů asymetrický algoritmus RSA.
    - Pro asymetrickou kryptografii je použit algoritmus RSA.

- Pro symetrickou kryptografii je použit algoritmus AES s délkou klíčů 256 (preferovaný) a 128 bitů v módu CBC. Z důvodu kompatibility se staršími klienty je použit i algoritmus 3DES s délkou klíče 168 bitů. Služba Exchange online z důvodu kompatibility se staršími mobilními zařízeními podporuje navíc ještě algoritmus RC4 s délkou klíče 128 bitů s nejnižší prioritou.
- Poporovány jsou hash funkce SHA-384 (preferovaný s AES-256), SHA-256 (preferovaný s AES-128) a SHA-1. Podpora pro SHA-1 by měla být ukončena k 1.1.2017 (viz [29]). Služba Exchange online z důvodu kompatibility se staršími mobilními zařízeními podporuje navíc ještě algoritmus MD5 společně s šifrovacím algoritmem RC4 s nejnižší prioritou.
- Certifikáty používané u serverových služeb Office 365 využívají asymetrický algoritmus RSA s délkou klíčů 2048 bitů a hash funkci SHA-256. Certifikáty obsahují odkazy na revokační informace CRL a OCSP. Použité certifikační autority mají stejné nebo vyšší parametry s výjimkou kořenové certifikační autority, která využívá hash funkci SHA-1 (což u kořenových certifikačních autorit nevadí – hash certifikátu není využíván pro jeho validaci).

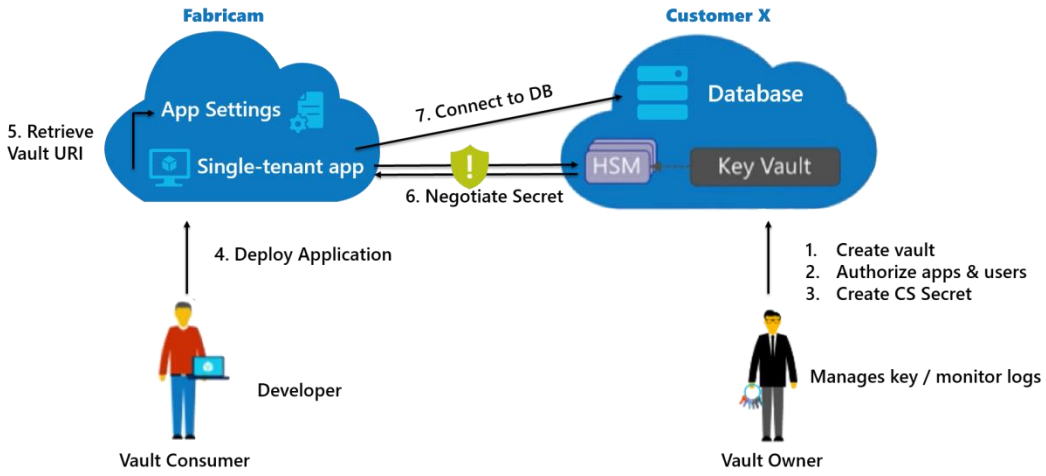
Azure Key Vault

Azure Key Vault je služba řešící problematiku bezpečného uložení symetrických i asymetrických klíčů pro cloudové služby provozované v rámci Microsoft Azure a Office 365:

- Azure Key Vault rozeznává dvě role:
  - **Azure Key Vault Owner:** vlastník klíčů, který vytváří úložiště klíčů, spravuje klíče a řídí přístupová oprávnění ke klíčům.
  - **Azure Key Vault Consumer:** uživatel klíčů který může provádět kryptografické operace s asymetrickými klíči a získat symetrické klíče v závislosti na přístupových oprávněních nastavených v Azure Key Vault.

Tyto dvě role umožňují oddělit správu/vlastnictví klíčů od jejich použití a umožňují zvýšit bezpečnost klíčů podle následujícího scénáře:

Obr. 11
Scénář využití Azure Key Vault

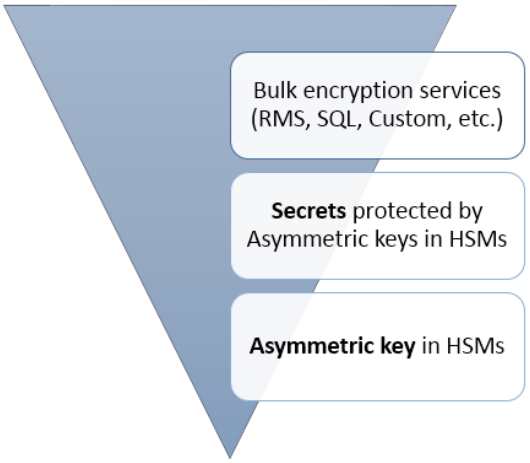


- V Azure Key Vault mohou být uloženy dva typy klíčů:
  - **Keys** asymetrické klíče pro algoritmus RSA s délkou 2048 bitů, které mohou být uloženy dvěma různými způsoby:
    - **HSM Protected Keys:** klíče jsou uloženy v hardwarovém Thales nShield HSM, který splňuje požadavky FIPS 140-2 Level 2 (viz [71]), a neumožňuje export soukromého klíče, pouze provést s ním operace.
    - **Software Protected Keys**: klíče jsou uloženy ve virtuálních serverech služby Azure Key Vault a jsou chráněny asymetrickými klíči uloženými v HSM. Tato varianta je levnější než HSM Protected Keys a je určena pro vývojové a testovací prostředí.

- **Secret**: bloky dat (BLOB) o velikosti maximálně 10 kB – obvykle symetrické šifrovací klíče, ale může jít i o jiné typy citlivých dat, například hesla nebo API tokeny – které, jsou uloženy ve virtuálních serverech služby Azure Key Vault a jsou chráněny asymetrickými klíči uloženými v HSM.

  Je třeba mít na zřeteli, že u tohoto typu klíčů získává role Azure Key Vault Consumer hodnotu klíče a musí být řešena jeho bezpečnost při využití v aplikaci (uložení v RAM, persistentní uložení v aplikaci a podobně).

Obr. 12
Typy klíčů v Microsoft Azure [55]

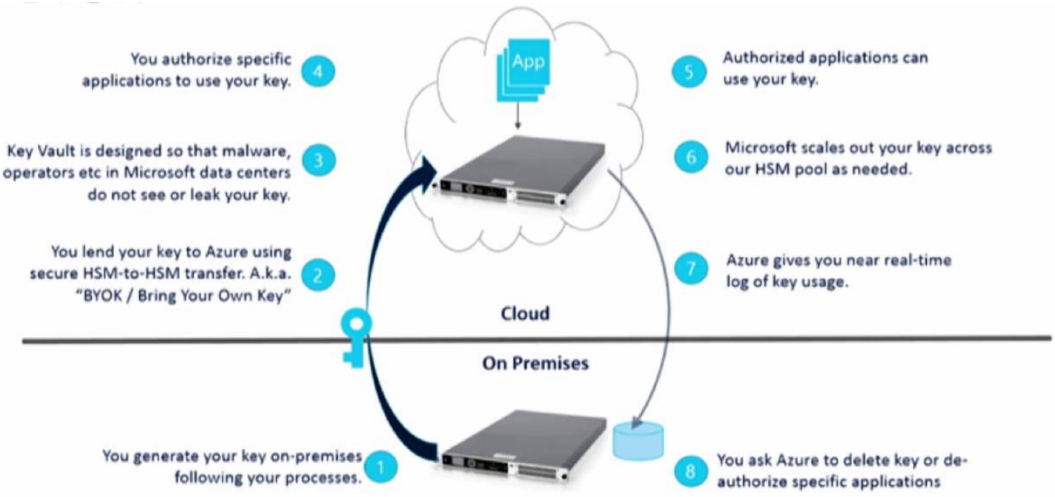


Azure Key Vault + BYOK

Využití Thales nShield HSM pro Azure Key Vault umožňuje realizovat scénář Bring your own Key (BYOK):

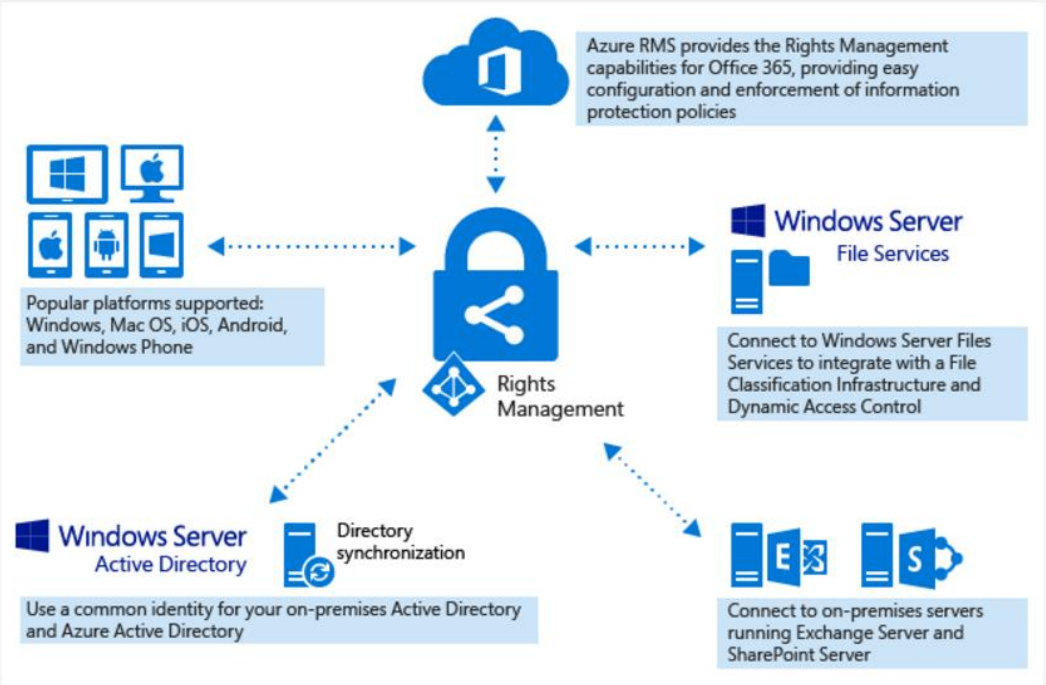
- Správce klíčů vygeneruje ve svém on-premise Thales nShield HSM pár klíčů pro RSA s délkou 2048 bitů.
- Správce klíčů pomocí Azure Key Vault BYOK Toolset exportuje soukromý klíč zašifrovaný pomocí veřejného klíče Microsoft Key Exchange Key do souboru. Soukromý klíč Microsoft Key Exchange Key je uložen v Azure Key Vault Thales nShield HSM.
- Správce klíčů nahraje soubor se zašifrovaným soukromým klíčem do Azure Key Vault. Zde je soubor nahrán do Thales nShield HSM a dešifrován soukromým klíčem Microsoft Key Exchange Key.

Obr. 13
Scénář BYOK s Azure Key Vault



Azure Rights Management Service (RMS)

Azure RMS je řešení pro ochranu informací zasílaných mailem, uložených na souborovém serveru nebo v cloudové službě a to i při přístupu k těmto informacím přes Internet z různých zařízení a při jejich sdílení s jinými uživateli či organizacemi. Trvalá ochrana informací, kterou Azure RMS poskytuje, nezabezpečuje jen data, ale pomáhá také splnit regulatorní požadavky.



Obr. 14
Schema Azure RMS pro Office 365, viz [28]

Azure RMS poskytuje následující funkcionality:

- Ochrana libovolného typu souboru
- Ochrana souboru bez ohledu na to, kde je uložen
- Ochrana příloh elektronické pošty (i pro mobilní zařízení). Pouze autorizovaný příjemce může vykonávat povolené aktivity s přiloženým, chráněným dokumentem. Zpráva jako taková šifrovaná není
- Auditování a monitorování chráněných souborů
- Podpora různých zařízení
  - Windows počítač, telefon a tablet
  - Mac počítač
  - iOS tablet a telefon
  - Android tablet a telefon
- Podpora spolupráci mezi organizacemi, pokud obě mají Office 365 nebo Azure předplatné
- Ochrana mailů v Exchange online integrací s DLP politikami
- Ochrana dokumentů v SharePoint Online integrací s chráněnými knihovnami
- Integrace s on-premise službami pomocí RMS konektoru
  - Exchange server
  - SharePoint server
  - Souborový server Windows se službou File Clasification Infrastructure
- Zjednodušení konfigurace požadované úrovně zabezpečení pomocí šablon
- API umožňující zabudovat podporu Azure RMS do aplikací třetích stran

- Kontrola vlastních dat
  - Použití vlastního tenant klíče v HSM modulu (BYOK) umožní ochránit data před poskytovatelem služby, viz [30]. Tato vlastnost není dostupná pro Exchange Online
  - Auditing a logování používání
    - Analýza používání RMS
    - Monitorování pokusů o zneužití
    - Forenzní analýza
  - Ochrana ztráty dat při ztrátě klíčů
  - Podpora federace identit mezi Azure AD a on-premise Active Directory a podpora jednotného přihlášení pomocí ADFS
  - Podpora exit scénáře bez ztráty chráněných dat, viz [31]

Azure RMS algoritmy a délky klíčů:

- Podpora kryptografických standardů a FIPS 140-2, viz [28]
- Ochrana dokumentů – AES s délkou klíče 128 bitů (AES s délkou klíče 256 bitů pro .p*file* a .ppdf soubory)
- Ochrana klíčů – RSA s délkou klíče 2048 bitů
- Podpis certifikátů – SHA-256

Jednotlivé generované klíče a způsoby jejich použití při ochraně informací v Azure RMS jsou popsány v dokumentu [28].

10.14 NÁSTROJ PRO ZAJIŠŤOVÁNÍ ÚROVNĚ DOSTUPNOSTI

Oblast nástroje pro zajišťování úrovně dostupnosti je v prostředí Office 365 realizována následovně:

Architektura služeb

Architektura jednotlivých služeb provozovaných v Microsoft Online Services je již od počátku navrhována jako vysoce dostupná. Takto navržená architektura zahrnuje:

- redundance
  - redundance disků a serverů v datovém centru,
  - redundance na úrovni budov datových center a napájení,
  - redundance na úrovni služeb jejich distribucí napříč datovými centry,
  - redundance dat jejich nepřetržitou replikací a udržováním násobného počtu replik,
- přizpůsobivost, elasticita
  - rozkládání zátěže s dynamickou prioritou,
  - automatický i ruční přesun služeb na fungující zdroje v případě poruchy,
  - rutinní provádění obnov pro zajištění připravenosti na výskyt poruchy,
- distribuované služby
  - komponenty SaaS a PaaS využívají distribuovanou funkcionalitu, kdy výpadek jednoho uzlu nebo lokality neohrozí dostupnost služby,
  - replikací adresářových služeb je zajištěna možnost autentizace uživatelů i v případě lokálního výpadku,
  - distribuované služby zjednodušují správu, údržbu, nasazování, diagnostiku a případné obnovy nebo opravy,

- monitorování
  - probíhá neustálé monitorování všech poskytovaných služeb a jejich komponent,
  - probíhá analýza provozního stavu a veškeré odchylky jsou reportovány a tím je umožněn proaktivní zásah,
  - úroveň logování, auditování a trasování umožňuje izolovat a řešit problémy,
- snižování složitosti
  - používání standardních komponent, kde je to možné,
  - používání standardizovaných procesů,
  - architektura software používá volné vazby mezi komponentami, takže monitorování a nasazování komponent je jednodušší,
  - propracovaný change management zahrnuje ověření změn před jejich celosvětovým nasazením,
- support
  - 24/7 podpora pro zákazníky,
- průběžné zlepšování
  - každý incident je zhodnocen a výsledky jsou využity k zamezení opakování podobného incidentu a pro zlepšení služeb,
- komunikace se zákazníkem
  - konzistentní komunikace se zákazníkem je zajišťována několika způsoby.

Dostupnost služeb

Dostupnost služeb Microsoft Office 365 je garantována poskytovatelem, společností Microsoft a je definována v dokumentu Service Level Agreement for Microsoft Online Services, viz [48] jako 99,9%.

10.15 PSEUDONYMIZACE

Pro scénáře výše uvedené scénáře zpracování dokumentů, elektronické formy nestrukturovaných dat, elektronické pošty, záznamů audio nebo video hovorů, u kterých je třeba zachovat interoperabilitu a přenositelnost mimo hranice organizace zpracovatele i správce (typicky soubory typu .DOCX, .XLSX, PPTX, PDF, JPG atd.), není prakticky proveditelné obecně zavádět pseudonymizaci osobních údajů, které se mohou v těchto souborech vyskytovat. Pseudonymizací by společnost Microsoft zasahovala do integrity zákaznických dokumentů, což by bylo v rozporu s povahou služby. Společnost Microsoft se proto zaměřuje na několik úrovní zajištění ochrany a případně i integrity osobních údajů šifrováním osobních údajů, čímž je ochrana osobních údajů nestrukturovaných dat dostatečně zajištěna a zároveň je zachována funkcionalita dokumentů.

Ačkoliv prostředí Microsoft Office 365 nenabízí automatizované nástroje pro zajištění pseudonymizace, správce údajů (zákazník společnosti Microsoft) má možnost nastavit interní procesy či zajistit řešení na aplikační úrovni takovým způsobem, kdy budou moci být údaje ukládány do prostředí Office 365 pseudonymizované (například vést konkrétní identifikační údaje subjektu odděleně od ostatních informací a dokumentů týkajících se subjektu).

11 SEZNAM POUŽITÝCH ZKRATEK

Tab. 24
Seznam použitých zkratek

Zkratka	Význam
AD	Active Directory
BYOK	Bring Your Own Key
DPIA	Data Protection Impact Assessment
DR	Disaster recovery
GDPR	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
IaaS	Infrastructure as a Service Infrastruktura jako služba – model poskytování cloud služeb
IPS	Intrusion Prevention System
IRM	Information Rights Management
IS	Informační systém
MCIO	Microsoft's Cloud Infrastructure and Operations
MS	Microsoft s.r.o.
Multi-tenant prostředí	Prostředí, které je poskytováno množství subjektů a které zajišťuje, aby činnost jednoho subjektu neovlivňovala činnost ostatních subjektů
NAT	Network Address Translation
NIS	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
PaaS	Platform as a Service
PIA	Privacy Impact Assessment (viz DPIA)
PSO	Podmínky pro služby online
PZS	Poskytovatel základních služeb
RMS	Rights Management Service
RPO	Recovery Point Objective / Bod obnovy dat
RTO	Recovery Time Objective / Doba obnovy chodu
SaaS	Software as a Service Software jako služba – model poskytování cloud služeb
SIEM	Security Information and Event Management
SLA	Service Level Agreement
VoKB	Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti

Zkratka	Význam
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
ZoOOÚ	Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

12 LITERATURA

[1] Protecting Data in Microsoft Online Services (Studie zpracovaná na základě poptávky Microsoft s.r.o.), 24. 5. 2016, S.ICZ

[2] Analýza rizik a bezpečnostní opatření zdravotnických IS v cloudu (Studie zpracovaná na základě poptávky Microsoft s.r.o.), 16.12.2016, S.ICZ

[3] Microsoft Corporation: Microsoft Security Policy, 6. 1. 2016

[4] Microsoft Volume Licensing: Podmínky pro služby online, 1.2.2017, Microsoft

[5] Microsoft Volume Licensing: Smlouva o úrovni služeb pro služby online společnosti Microsoft, 1.1.2017, Microsoft

[6] Microsoft Corporation: Trusting the Cloud, White Paper, 22. 11. 2015

[7] Microsoft Corporation: Windows Azure Network Security, 28. 11. 2013

[8] Microsoft Corporation: Data Encryption Technologies in Office 365, 22.1.2016

[9] Microsoft Corporation: Exchange Online Protection, 2016 (https://products.office.com/en-us/exchange/microsoft-exchange-online-protection-email-filter-and-anti-spam-protection-email-security-email-spam)

[10] Microsoft Corporation: Exchange Online Advanced Threat Protection, 2016 (https://products.office.com/en-us/exchange/online-email-threat-protection)

[11] Microsoft Corporation: Microsoft Azure Security and Audit Log Management, 14. 11. 2014

[12] Microsoft Corporation: Auditing and Reporting in Office 365, 13.8.2015

[13] Office 365 Team, Announcing the new Office 365 Management Activity API for security and compliance monitoring, 21.4.2015 (https://blogs.office.com/2015/04/21/announcing-the-new-office-365-management-activity-api-for-security-and-compliance-monitoring/)

[14] Microsoft Technet: Auditing in Office 365, 13.1.2016 (https://technet.microsoft.com/en-us/library/dn790283.aspx)

[15] Microsoft Corporation: Search the audit log in the Office 365 Protection Center (https://support.office.com/en-us/article/Search-the-audit-log-in-the-Office-365-Protection-Center-0d4d0f35-390b-4518-800e-0c7ec95e946c?ui=en-US&rs=en-US&ad=US)

[16] Microsoft Technet: Exchange auditing reports, 21.9.2015 (https://technet.microsoft.com/library/jj150497(v=exchg.150).aspx)

[17] Microsoft Technet: Enable mailbox auditing in Office 365, 28.9.2015 (https://technet.microsoft.com/en-us/library/dn879651.aspx)

[18] Microsoft Corporation: View audit log reports (https://support.office.com/en-us/article/View-audit-log-reports-b37c5869-1b47-4a82-a30d-ea20070fe527?CorrelationId=b47f8144-3ef7-4fb6-99e7-1ad349bbe8f9&ui=en-US&rs=en-US&ad=US#__toc272842194)

[19] Microsoft Corporation, Cloud Infrastructure Operational Excellence & Reliability, 13. 3. 2015

[20] Microsoft Corporation: Defending Office 365 against Denial-of-Service attack, 2/2015

[21] Microsoft Corporation: Microsoft Azure security and audit log management, 10. 12. 2015 (https://azure.microsoft.com/cs-cz/documentation/articles/azure-security-audit-log-management/)

[22] Mark Russinovich, An Inside Look at Cloud Service Provider Security, 20. 4. 2015

[23] Microsoft Azure: What is Log Analytics? (https://azure.microsoft.com/en-us/services/log-analytics/)

[24] Microsoft Azure: Add Log Analytics solution from the Solutions Gallery, 8.8.2016 (Add Log Analytics solutions from the Solutions Gallery)

[25] Microsoft Corporation: Integrating your on-premises identities with Azure Active Directory, 25. 1. 2016 (https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect/)

[26] Microsoft Corporation, About VPN devices for Site-to-Site VPN Gateway connections, 14. 12. 2015 (https://azure.microsoft.com/cs-cz/documentation/articles/vpn-gateway-about-vpn-devices/)

[27] Microsoft Corporation, ExpressRoute technical overview, 16. 1. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/expressroute-introduction/)

[28] Microsoft Corporation, What is Azure Rights Management?, 1. 2. 2016 (https://technet.microsoft.com/en-us/library/jj585026.aspx#BKMK_RMScrytographics)

[29] Microsoft Technet: Windows Enforcement of Authenticode Code Signing and Timestamping, 24. 9. 2015 (http://aka.ms/sha1)

[30] Microsoft Technet: Planning and Implementing Your Azure Rights Management Tenant Key, 1. 2. 2016 (https://technet.microsoft.com/library/dn440580.aspx)

[31] Microsoft Technet: Decommissioning and Deactivating Azure Rights Management, 1. 12. 2015 (https://technet.microsoft.com/en-us/library/jj658940.aspx)

[32] Office 365 Team: Announcing Customer Lockbox for Office 365, 21.4.2015 (https://blogs.office.com/2015/04/21/announcing-customer-lockbox-for-office-365/)

[33] ISO/IEC FDIS 29134:2016 - Information technology — Security techniques — Privacy impact assessment – Guidelines, ISO, 2016 (draft)

[34] Manage eDiscovery cases in the Security & Compliance Center (https://support.office.com/en-us/article/Manage-eDiscovery-cases-in-the-Office-365-Security-Compliance-Center-edea80d6-20a7-40fb-b8c4-5e8c8395f6da?ui=en-US&rs=en-US&ad=US&fromAR=1)

[35] Microsoft Azure: Azure Active Directory Reporting Guide, 7.3.2016 (https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-guide/)

[36] Microsoft Corporation: Azure Active Directory Audit Report Events, 7. 12. 2015 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-reporting-audit-events/)

[37] Microsoft Corporation: Office 365 SoA 2014 Security and Privacy ISO 27001.2013 & 27018, 31. 10. 2014

[38] NIST: Windows Server 2008 R2 BitLocker Drive Encryption Security Policy For FIPS 140-2 Validation, 31. 8. 2011

[39] Microsoft Corporation: Azure AD Privileged Identity Management, 21. 1. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-privileged-identity-management-configure/)

[40] Microsoft Corporation: What is Azure Active Directory?, 14. 1. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-whatis/)

[41] MSDN: Password policy in Azure AD, 8. 6. 2015 (https://msdn.microsoft.com/en-us/library/azure/jj943764.aspx)

[42] Microsoft Corporation: Azure Role-Based Access Control, 10. 2. 2016 (https://azure.microsoft.com/en-us/documentation/articles/role-based-access-control-configure/)

[43] Microsoft Corporation: View your access and usage reports, 7. 12. 2015 (https://azure.microsoft.com/cs-cz/documentation/articles/active-directory-view-access-usage-reports/)

[44] Microsoft Corporation: Microsoft Antimalware for Azure Cloud Services and Virtual Machines, 10. 12. 2015 (https://azure.microsoft.com/cs-cz/documentation/articles/azure-security-antimalware/)

[45] Microsoft Corporation, Introduction to Azure Security Center, 9. 2. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/security-center-intro/)

[46] Microsoft Corporation, What is Azure Information Protection?, 12. 10. 2016 (https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection)

[47] Microsoft Corporation, Microsoft Trust Centrum (https://www.microsoft.com/en-us/TrustCenter/Security/DesignOpSecurity)

[48] Microsoft Corporation, Service Level Agreement for Microsoft Online Services, 1. 2. 2016

[49] Microsoft Corporation: What is, Azure Backup?, 5. 2. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/backup-introduction-to-azure-backup/)

[50] Microsoft Corporation: What is Site Recovery?, 22. 2. 2016 (https://azure.microsoft.com/en-us/documentation/articles/site-recovery-overview/)

[51] MSDN: About Keys and Secrets, 16. 10. 2015 (https://msdn.microsoft.com/library/azure/dn903623.aspx)

[52] Microsoft Corporation: What is Azure Key Vault?, 8. 1. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/key-vault-whatis/)

[53] Microsoft Azure: Encrypt and decrypt blobs in Microsoft Azure Storage using Azure Key Vault, 6.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/storage-encrypt-decrypt-blobs-key-vault/)

[54] Microsoft Azure: Client-Side Encryption and Azure Key Vault for Microsoft Azure Storage (https://docs.microsoft.com/en-us/azure/storage/storage-client-side-encryption)

[55] Microsoft Technet: Azure Key Vault – Making the cloud safer, 8.1.2015, (https://blogs.technet.microsoft.com/kv/2015/01/08/azure-key-vault-making-the-cloud-safer/)

[56] Microsoft Azure: Azure Storage Service Encryption for Data at Rest, 16.9.2016 (https://docs.microsoft.com/en-us/azure/storage/storage-service-encryption)

[57] Microsoft Corporation: Azure Resource Manager overview, 2. 2. 2016 (https://azure.microsoft.com/en-us/documentation/articles/resource-group-overview/)

[58] Microsoft Corporation: Audit operations with Resource Manager, 2. 12. 2015 (https://azure.microsoft.com/en-us/documentation/articles/resource-group-audit/)

[59] Microsoft Corporation: RBAC: Built-in roles, 21. 1. 2016 (https://azure.microsoft.com/en-us/documentation/articles/role-based-access-built-in-roles/)

[60] Stefan Keir Gordon: Storing Data Securely in Azure Blob Storage with Azure Encryption Extensions, 17. 6. 2015 (http://blogs.msdn.com/b/partnercatalystteam/archive/2015/06/17/storing-data-securely-in-azure-blob-storage-with-azure-encryption-extensions.aspx)

[61] Microsoft Corporation: Shared Access Signatures, Part 1: Understanding the SAS model, 14. 2. 2016 (https://azure.microsoft.com/en-us/documentation/articles/storage-dotnet-shared-access-signature-part-1/)

[62] Microsoft Corporation: Azure Site Recovery: Our Commitment to Keeping Your Data Secure, 2. 9. 2014 (https://azure.microsoft.com/en-us/blog/azure-site-recovery-privacy-security-part1/)

[63] Microsoft Corporation: ExpressRoute circuits and routing domains, 16. 1. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/expressroute-circuit-peerings/)

[64] Microsoft Technet: Architecture guidance for protecting company email and documents, 30. 9. 2015 (https://technet.microsoft.com/en-us/library/mt574220.aspx)

[65] Microsoft Technet: Introduction to Server and Domain Isolation, 20. 1. 2009 (https://technet.microsoft.com/en-us/library/cc725770(v=ws.10).aspx)

[66] Microsoft Technet: Changes in Kerberos Authentication, 10. 5. 2012 (https://technet.microsoft.com/en-us/library/dd560670(v=ws.10).aspx)

[67] Microsoft Technet: Network security: Configure encryption types allowed for Kerberos, 15. 11. 2012 (https://technet.microsoft.com/en-us/library/jj852180.aspx)

[68] Microsoft Technet: Security and Archiving in Skype for Bussiness, 27.4.2017 (https://technet.microsoft.com/en-us/library/skype-for-business-online-security-and-archiving.aspx)

[69] Microsoft Technet: Skype for Business Online Meetings, 26.1.2017 (https://technet.microsoft.com/en-us/library/skype-for-business-online-meetings.aspx)

[70] Microsoft Corporation: What is Azure Multi-Factor Authentication?, 3. 3. 2016 (https://azure.microsoft.com/cs-cz/documentation/articles/multi-factor-authentication/)

[71] Microsoft Corporation: How to generate and transfer HSM-protected keys for Azure Key Vault, 1. 2. 2016 (https://azure.microsoft.com/en-us/documentation/articles/key-vault-hsm-protected-keys/#step-4-prepare-your-key-for-transfer)

[72] Microsoft Corporation: Always Encrypted (Database Engine), 4. 3. 2016 (https://msdn.microsoft.com/en-us/library/mt163865.aspx)

[73] MSDN: Extensible Key Management Using Azure Key Vault (SQL Server), 10. 12. 2015 (https://msdn.microsoft.com/en-us/library/dn198405.aspx)

[74] MSDN: Transparent Data Encryption (TDE), 23. 11. 1015 (https://msdn.microsoft.com/en-us/library/bb934049.aspx)

[75] MSDN: Transparent Data Encryption with Azure SQL Database, 28. 1. 2016 (https://msdn.microsoft.com/en-us/library/dn948096.aspx)

[76] Microsoft Azure: Azure Disk Encryption for Windows and Linux IaaS VMs, 29.1.2016 (https://azure.microsoft.com/en-us/documentation/articles/azure-security-disk-encryption/)

[77] Sharing in Exchange Online, 9.3.2015 (https://technet.microsoft.com/en-us/library/jj916670(v=exchg.150).aspx)

[78] Retention in the Office 365 Security & Compliance Center (https://support.office.com/en-us/article/Retention-in-the-Office-365-Security-Compliance-Center-2a0fc432-f18c-45aa-a539-30ab035c608c)

[79] Microsoft Azure: Azure Storage replication, 25.10.2016 (https://docs.microsoft.com/en-us/azure/storage/storage-redundancy)

[80] Microsoft Azure: Smlouva SLA pro Storage, duben 2016 (https://azure.microsoft.com/cs-cz/support/legal/sla/storage/v1_1/)

[81] 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, CELEX:32016R0679

[82] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[83] Lze využít cloud computing pro zpracování osobních údajů? (https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=11337&n=lze%2Dvyuzit%2Dcloud%2Dcomputing%2Dpro%2Dzpracovani%2Dosobnich%2Dudaju&p1=1659)

[84] K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb (https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002)

[85] Stanovisko č. 05/2012 ke cloud computingu (https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=16706)

[86] Information Security Management System for Microsoft's Cloud Infrastructure - Online Services Security and Compliance, 2015, Microsoft

[87] Office 365, Information Security Management System (ISMS) Manual, datum publikace 28.6.2015, Microsoft

[88] Microsoft Cloud Infrastructure and Operations – ISO/IEC 27001:2013 ISMS Statement of Applicability, Statement of Applicability, datum publikace 18.02.2016, Microsoft

[89] Microsoft Office ISO 27001:2013 Statement of Applicability, 15.10.2016, Microsoft

[90] Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014, 17.6.2016, Microsoft

[91] Certificate of Registration, Information Security Management System – ISO/IEC 27001:2013, Microsoft Cloud Infrastructure and Operations, IS 533913, 26.10.2016, BSI

[92] Assesment Report - Microsoft Cloud Infrastructure and Operations, 35.5.2016, BSI

[93] Assesment Report - Microsoft Office 365, 19.10.2016, BSI

[94] Microsoft Corporation - Microsoft Azure and Microsoft Datacenters: Report on a Description of System and the Suitability of the Design and Operating Effectiveness of Controls (SSAE16 SOC 1 Type II Report), 28.10.2016, Deloitte & Touche LLP

[95] Microsoft Corporation - Microsoft Azure and Microsoft Datacenters: Report on Controls at Service Organization relevant to Security, Availability, Processing Integrity and Confidentiality Trust principles (SOC 2) and Cloud Matrix (CCM) Criteria (AT 101 SOC 2 Type II Report), 28.10.2016, Deloitte & Touche LLP

[96] Microsoft Corporation – Office 365, Report on a Description of Microsoft Office 365 and Office 365, and the Suitability of the Design and Operating Effectivenes of Controls (Office 365 ISAE 3402 SOC 2 Type II Report), 13.1.2017, Deloitte & Touche LLP

[97] Microsoft Corporation – Office 365, Report on Controls at Service Organization Relevant to Security, Avalability, Confidentiality, and Processing Integrity (Office 365 AT 101 SOC 2 Type II Report), 13.1.2017, Deloitte & Touche LLP

[98] PWC ISAE 3000 Risk Assurance Report – Řízení rizik v cloudu (Zpráva poskytující přiměřenou jistotu o metodologii posuzování rizik Microsoft Online Services), 31.8.2015, PricewaterhouseCoopers Česká republika

[99] Embracing Cloud in Health: a European Risk Assessment Framework (A guide to privacy and security considerations for the adoption of cloud services in the health sector), prosinec 2014, Microsoft

[100] Shared Responsibilities For Cloud Computing, březen 2016, Microsoft

13 PŘÍLOHY


Příloha 1 -
Metodika analýzy riz


Příloha 2 - AR pro
scenar 1.pdf


Příloha 3 - AR pro
scenar 2.pdf


Příloha 4 - AR pro
scenar 3.pdf