Analýza rizik provozu spisové služby v Microsoft Azure

v1.1 (Final)

Dokument ze dne 23.12.2016

mainstream TECHNOLOGIES

PIERSTONE

Dodavatel:	Mainstream Technologies, s.r.o.
Kontaktní osoba:	Jakub Lukeš
Funkce:	Account Manager
Tel.:	+420 734 434 005
E-mail:	Jakub.lukes@mainstream.cz
Datum předání:	23. 12. 2016
Verze:	1.1 (Final draft)

Analýza rizik provozu spisové služby GINIS v Microsoft Azure

Zákazník:	Microsoft Czech Republic Vyskočilova 140 00 Praha 4
Kontaktní osoba:	Zdeněk Jiříček
Funkce:	National Technology Officer
Tel.:	+420 725 517 517
E-mail:	zdenekj@microsoft.com

Na dokumentu spolupracovali:	Risk Analysis Consultants, s. r. o
	Libor Široký, Zbyněk Marx
	Mainstream Technologies, s.r.o.
	Jakub Lukeš, Michael Grafnetter
	PIERSTONE s.r.o.
	Jana Pattynová, Stefan Král
	GORDIC spol. s.r.o.
	Jiří Čech, Miroslav Čejka

Obsah

1. Manažerské shrnutí 4

1.1. Cíl analýzy rizik 4

1.2. Skladba analýzy rizik 4

1.3. Hlavní závěry analýzy rizik 4

2. Popis metodiky 7

2.1. Identifikace aktiv 7

2.2. Identifikace rizik 7

2.3. Hodnocení dopadu a pravděpodobnosti rizik 7

2.3.1. Hodnocení dopadů 7

2.3.2. Hodnocení pravděpodobnosti 9

2.3.3. Výpočet velikosti rizik 10

2.4. Pokrytí zjištěných rizik 12

2.5. Míra pokrytí rizik opatřeními 12

3. Hodnocení dopadů 13

4. Identifikace a hodnocení rizik 14

4.1. Reputace 15

4.2. Politiky bezpečnosti informací 15

4.3. Organizace bezpečnosti informací 16

4.4. Bezpečnost lidských zdrojů 16

4.5. Řízení aktiv 16

4.6. Řízení přístupu 17

4.7. Kryptografie 17

4.8. Fyzická bezpečnost a bezpečnost prostředí 18

4.9. Bezpečnost provozu 19

4.10. Bezpečnost komunikací 20

4.11. Akvizice, vývoj a údržba systémů 21

4.12. Dodavatelské vztahy 21

4.13. Řízení incidentů bezpečnosti informací 22

4.14. Aspekty řízení kontinuity činností 22

4.15. Soulad s požadavky 22

5. Pokrytí zjištěných rizik 25

5.1. Pokrytí identifikovaných rizik 25

5.2. Soulad s mezinárodními standardy 31
5.2.1. Cloudové prostředí Microsoft 31
5.2.2. Spisová služba GINIS 32

5.3. Míra pokrytí rizik opatřeními 33

6. Použité zdroje 35

Příloha A. Identifikace a analýza legislativních požadavků 38

1.1 Obecné nařízení o ochraně osobních údajů (EU) 38

1.2 Zákon č. 101/2000 Sb., o ochraně osobních údajů 51

1.3 Zákon č. 499/2004 Sb., o archivnictví a spisové službě 57

1. Manažerské shrnutí

Účelem dokumentu *Analýza Rizik provozu spisové služby v Microsoft AZURE* (dále také *analýza* nebo *analýzy rizik*) je popsat postup práce a závěry z provedené analýzy rizik spisové služby Gordic GINIS, provozované reálnou organizací státní správy v prostředí Microsoft Azure.

1.1. Cíl analýzy rizik

Hlavním cílem analýzy bylo identifikovat a ohodnotit rizika spojená s využitím spisové služby Gordic GINIS v cloudovém prostředí Microsoft Azure a určit míru jejich pokrytí bezpečnostními opatřeními. Do rozsahu analýzy byla zahrnuta i cloudová služba Office 365, kterou organizace státní správy rovněž využívá.

1.2. Skladba analýzy rizik

Metodika práce, podle které byla vytvořena analýza rizik, je popsána v kapitole *2 Popis metodiky*. Výsledky z analýzy rizik jsou uvedeny v kapitole *4 Identifikace a hodnocení rizik*, způsob a míra pokrytí rizik opatřeními pak v *kapitole 5 Pokrytí zjištěných rizik*.

1.3. Hlavní závěry analýzy rizik

V rámci analýzy rizik byly zohledněny tyto zákony a standardy:

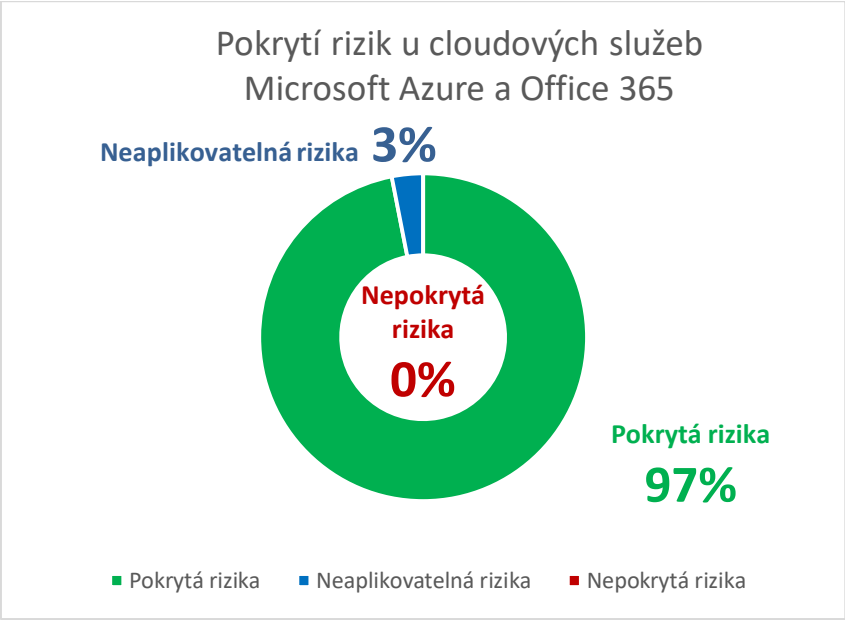
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 499/2004 Sb. o archivnictví a spisové službě
- EU GDPR - Nařízení Evropského parlamentu a rady (EU) 2016/579 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- ISO/IEC 27001:2013
- ISO/IEC 27005:2011
- ISO/IEC 27017:2015
- ISO/IEC 27018:2014.

Celkem bylo **identifikováno 66 rizik**. Nevyššími riziky (velikost 5) jsou:

- 0701 Nedostatečné školení/prověření zaměstnanců
- 0801 Zneužití přenosných/vyměnitelných nosičů dat
- 0802 Špionáž, odposlech, prozrazení dat
- 0804 Odposlouchávání/modifikace dat prostřednictvím softwarového vybavení
- 0901 Distributed denial of service (DDoS)
- 1102 Nedostatečně smazaná data
- 1301 Zachytávání dat v sítích
- 1302 Skenování a testování bezpečnosti cloudové služby útočníkem
- 1401 Nedostatečné řízení rizik - analýza rizik
- 1402 Nedostatečná bezpečnost v procesech vývoje a podpory.

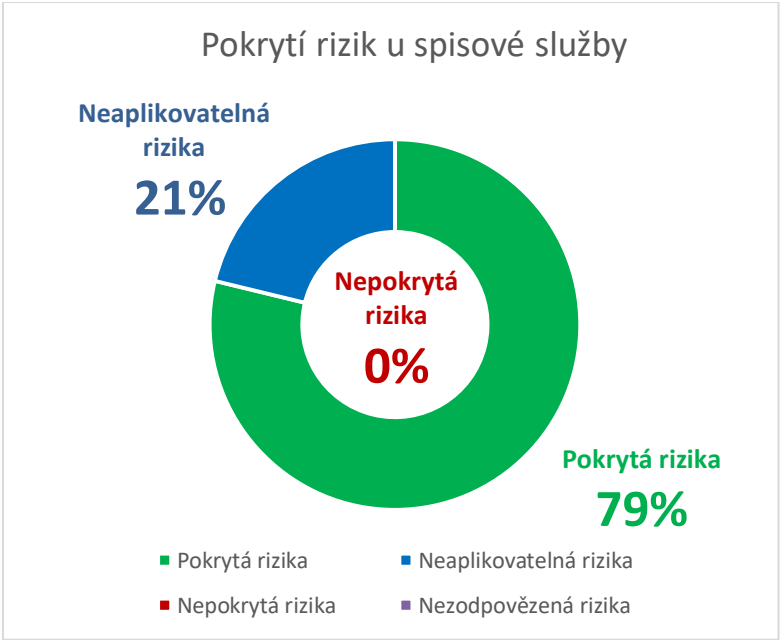
Poznámka: Detailnější popis jednotlivých rizik včetně jejich hodnocení je uveden v kapitole 4 Identifikace a hodnocení rizik.

- Společnost Microsoft v rámci nabízených cloudových služeb Azure a Office 365 pokrývá 97 % identifikovaných rizik. Zbývající 3 % rizik jsou na poskytovatele cloudové služby neaplikovatelná.



Graf 1 Pokrytí rizik u cloudových služeb Microsoft Azure a Office 365

- Společnost Gordic u spisové služby Ginis pokrývá 79 % identifikovaných rizik, 21 % rizik je neaplikovatelných.



Graf 2 Pokrytí rizik u spisové služby

- Organizace státní správy může pokrýt 77 % identifikovaných rizik, 23 % je neaplikovatelných.

Graf 3 Možnosti pokrytí rizik u organizace státní správy

2. Popis metodiky

Kapitola popisuje metodický postup, podle kterého bylo při tvorbě analýzy rizik postupováno.

V rámci *Analýzy rizik provozu spisové služby v Microsoft Azure* byl v prvním kroku stanoven cíl analýzy (*kapitola1.1* Cíl analýzy rizik). Dále byla identifikována aktiva, která souvisí s používáním spisové služby GINIS v cloudovém prostředí Microsoft Azure (*2.1 Identifikace aktiv*) a aktiva ohodnocena z pohledu dopadu jejich narušení na organizaci státní správy (*2.3.1 Hodnocení dopadů*). Ve třetím kroku byla určena míra pravděpodobnosti, že dojde k realizaci daného rizika (*2.3.2 Hodnocení pravděpodobnosti*). Následně ve čtvrtém kroku byla na základě dříve stanovené velikosti dopadů a pravděpodobnosti vypočtena velikost jednotlivých rizik (*2.3.3 Výpočet velikosti rizik*). V pátém kroku došlo ke stanovení míry pokrytí jednotlivých rizik u poskytovatele cloudové služby, v rámci níž je provozována spisová služba GINIS a zákazníka (*2.4 Pokrytí zjištěných rizik*) a posouzena velikost rizik po aplikaci bezpečnostních opatření. V posledním šestém kroku byla vyhodnocena míra pokrytí rizik bezpečnostními opatřeními (*2.5 Míra pokrytí rizik opatřeními*).

2.1. Identifikace aktiv

Identifikace aktiv v organizaci státní správy byla provedena v rámci analýzy dopadů při interview s respondenty zastupující jednotlivá oddělení organizace státní správy. Seznam identifikovaných typových aktiv, včetně jejich hodnocení, je uveden v *3 Hodnocení dopadů* .

2.2. Identifikace rizik

Jako zdroj pro identifikaci rizik byly použity bezpečnostní mezinárodní standardy (ISO/IEC 27001:2013, ISO/IEC 27005:2011, ISO/IEC 27017:2015, ISO/IEC 27018:2014), Obecné nařízení o ochraně osobních údajů (GDPR), zákon o kybernetické bezpečnosti č. 181/2014 Sb., zákon č. 499/2004 Sb. o archivnictví a spisové službě, dokument od The European Network and Information Security Agency (ENISA) nazvaný: „Cloud Computing - Benefits, risks and recommendations for information security" a informace od zaměstnanců státní správy.

Poznámka: Konkrétní identifikovaná rizika jsou popsána a ohodnocena v kapitole 4 Identifikace a hodnocení rizik.

2.3. Hodnocení dopadu a pravděpodobnosti rizik

Postup hodnocení rizik cloudových služeb zahrnuje dva základní kroky:

1. Hodnocení dopadů
2. Hodnocení pravděpodobností

2.3.1. Hodnocení dopadů

Hodnocení dopadů u cloudové služby/spisové služby znamená posouzení dopadu na organizaci v případě, pokud bude cloudová služba/spisová služba z důvodu realizace rizika například nedostupná, data v cloudu budou prozrazena nebo modifikována. Hodnocení dopadů probíhalo v rámci pětistupňové škály (1-5), kde nízká hodnota (1, 2) představovala nízký dopad, naopak vysoka hodnota (4, 5) vysoký dopad. Popis jednotlivých stupňů hodnocení, včetně popisu vodítek, na základě kterých hodnocení probíhalo, zobrazuje *Tabulka 1 Vodítka pro hodnocení dopadů*. Hodnocení dopadů probíhalo expertně v rámci interview s pracovníky státní správy dotazníkovou metodou.

Vodítka pro hodnocení dopadů

Hodnocení	Popis	Definice
5	Extrémní	• Dlouhodobě negativní ohlas v tuzemských i mezinárodních médiích, kritická ztráta podílu na trhu. • Častá trestní stíhání a pokuty přesahující 10 mil. Kč, soudní spory včetně žalob, odnětí svobody pro představitele vedení. • Značná zranění nebo smrt vlastních zaměstnanců nebo třetích stran (zákazníci, prodejci). • Odchod více seniorních představitelů organizace. • Závažným způsobem poškozuje účinný rozvoj nebo provoz organizace nebo způsobí ukončení nebo jiné závažné narušení významech činností organizace. • Přímo nebo nepřímo povede ke ztrátám přesahujícím 1 mld. Kč.
4	Významný	• Dlouhodobě negativní ohlas v tuzemských médiích, značná ztráta podílu na trhu. • Incidenty musí být nahlášeny zřizovateli a je potřeba okamžitě zavést nápravná opatření. • Nutná hospitalizace (déle jak 24h) pro zaměstnance nebo třetí strany (zákazníci, prodejci). • Odchod některých seniorních manažerů, velká fluktuace zkušených zaměstnanců, nízký zájem nových uchazečů o zaměstnání. • Znevýhodňuje organizaci při obchodních nebo strategických jednáních s partnery. • Přímo nebo nepřímo povede ke ztrátám od 100 mil. do 1 mld. Kč. • Narušení legislativních či regulatorních požadavků vedoucí k pokutě nebo škodě do 10 mil. Kč.
3	Střední	• Krátkodobý negativní ohlas v tuzemských médiích. • Ohlášení incidentů s nutností okamžitého zavedení nápravných opatření. • Ambulantní léčba pro zaměstnance nebo třetí strany (zákazníci, prodejci). • Vysoká fluktuace a rozsáhlé problémy s pracovní morálkou zaměstnanců. • Bude bránit v provádění důležitých činností organizace. • Přímo nebo nepřímo povede ke ztrátám od 10 mil. do 100 mil. Kč.
2	Malý	• Poškození pověsti na lokální úrovni. • Ohlašování incidentů k regulátorovi, bez nutnosti nápravných opatření. • Žádná, popř. malá zranění zaměstnanců nebo třetích stran (zákazníci, prodejci). • Obecné problémy s morálkou zaměstnanců, zvýšená míra fluktuace. • Naruší řádné řízení a fungování organizace. • Přímo nebo nepřímo povede ke ztrátám od 1 mil do 10 mil. Kč. • Narušení legislativních či regulatorních požadavků vedoucí k pokutě nebo škodě do 100 tis. Kč.

Vodítka pro hodnocení dopadů

Hodnocení	Popis	Definice
1	Nepatrný	• Rychle opadající pozornost v médiích. • Bez nutnosti reportovat regulátorovi. • Bez zranění zaměstnanců a třetích stran (zákazníci, prodejci). • Pracovní nespokojenost několika zaměstnanců. • Způsobí neefektivní fungování jedné části organizace. • Přímo nebo nepřímo povede ke ztrátám do 1 mil. Kč • Narušení emocionální rovnováhy osoby, nikoliv však porušení legislativních či regulatorních požadavků.

Tabulka 1 Vodítka pro hodnocení dopadů

Příklad hodnocení dopadu rizika

U hodnocení dopadu se vždy uvažuje ten nejhorší dopad, pro případ, že by dané riziko bylo realizováno. Pokud by například při realizaci rizika *Nesoulad se zákonem o ochraně osobních údajů* došlo nanejvýše k poškození pověsti společnosti na lokální úrovni, znamenalo by to malý dopad, tedy stupeň 2, viz tabulka níže.

2	Malý	• Poškození pověsti na lokální úrovni. • Ohlašování incidentů k regulátorovi, bez nutnosti nápravných opatření. • Žádná, popř. malá zranění zaměstnanců nebo třetích stran (zákazníci, prodejci). • Obecné problémy s morálkou zaměstnanců, zvýšená míra fluktuace. • Naruší řádné řízení a fungování organizace. • Přímo nebo nepřímo povede ke ztrátám od 1 mil do 10 mil. Kč. • Narušení legislativních či regulatorních požadavků vedoucí k pokutě nebo škodě do 100 tis. Kč.

2.3.2. Hodnocení pravděpodobnosti

Hodnocení pravděpodobnosti, že dojde k realizaci daného rizika vůči uvažované cloudové službě/zákazníkovi, probíhalo podobně jako u hodnocení dopadů, prostřednictvím pětistupňové škály. Malou pravděpodobnost výskytu realizace rizika reprezentovaly nízké hodnoty (1,2), naopak vysokou pravděpodobnost vysoké hodnoty (4, 5). Vodítka pro hodnocení pravděpodobnosti zachycuje *Tabulka 2 Hodnocení pravděpodobnosti realizace rizika*. Hodnocení pravděpodobnosti realizace rizika probíhalo expertně v rámci pracovníků státní správy dotazníkovou metodou. Při určování pravděpodobnosti byl zohledněn i vliv zranitelnosti.

Vodítka pro hodnocení pravděpodobnosti

Hodnocení	Popis	Definice
5	Častá, téměř jistá	90% nebo větší šance výskytu v průběhu životnosti aktiva nebo projektu
4	Pravděpodobná	65% - 90% nebo šance výskytu v průběhu životnosti aktiva nebo projektu

Vodítka pro hodnocení pravděpodobnosti

3	**Možná**	35% - 65% nebo šance výskytu v průběhu životnosti aktiva nebo projektu
2	**Nepravděpodobná**	10% - 35% nebo šance výskytu v průběhu životnosti aktiva nebo projektu
1	**Vzácná**	Méně než 10% šance výskytu v průběhu životnosti aktiva nebo projektu

Tabulka 2 Hodnocení pravděpodobnosti realizace rizika

Příklad hodnocení pravděpodobnosti realizace rizika

Při hodnocení pravděpodobnosti bylo hodnocení posuzováno na základě statistických dat a praktických zkušeností jednotlivých respondentů. Například, pokud bylo známo, že riziko zemětřesení v dané oblasti nikdy nebylo, pravděpodobnost realizace rizika byla stanovena jako vzácná, tedy stupeň pravděpodobnosti 1, viz příklad v tabulce níže.

Vodítka pro hodnocení pravděpodobnosti

Hodnocení	Popis	Vodítka - procenta
5	**Častá, téměř jistá**	90% nebo větší šance výskytu v průběhu životnosti aktiva nebo projektu
4	**Pravděpodobná**	65% - 90% nebo šance výskytu v průběhu životnosti aktiva nebo projektu
3	**Možná**	35% - 65% nebo šance výskytu v průběhu životnosti aktiva nebo projektu
2	**Nepravděpodobná**	10% - 35% nebo šance výskytu v průběhu životnosti aktiva nebo projektu
1	**Vzácná**	Méně než 10% šance výskytu v průběhu životnosti aktiva nebo projektu

2.3.3. Výpočet velikosti rizik

Výpočet rizika vychází z průniku výše získaných hodnot - velikosti dopadu rizika a pravděpodobnosti realizace rizika. Na základě průniku těchto dvou hodnot je stanovena velikost rizika viz *Tabulka 3 Vodítka pro stanovení velikosti rizik*. S použitím tabulky se k určení velikosti rizika dojde tak, že v levém sloupci je vybrán stupeň, který byl stanoven k riziku v rámci hodnocení pravděpodobnosti, viz kapitola *2.3.2 Hodnocení pravděpodobnosti*. Obdobně

ve sloupci *Dopad* se vybere velikost dopadu daného rizika, jehož hodnota byla stanovena v rámci hodnocení dopadů viz kapitola *2.3.1 Hodnocení dopadů*. Následně průsečík/průnik dvou výše uvedených hodnot v tabulce *Tabulka 3 Vodítka pro stanovení velikosti rizik* stanoví velikost celkového rizika.

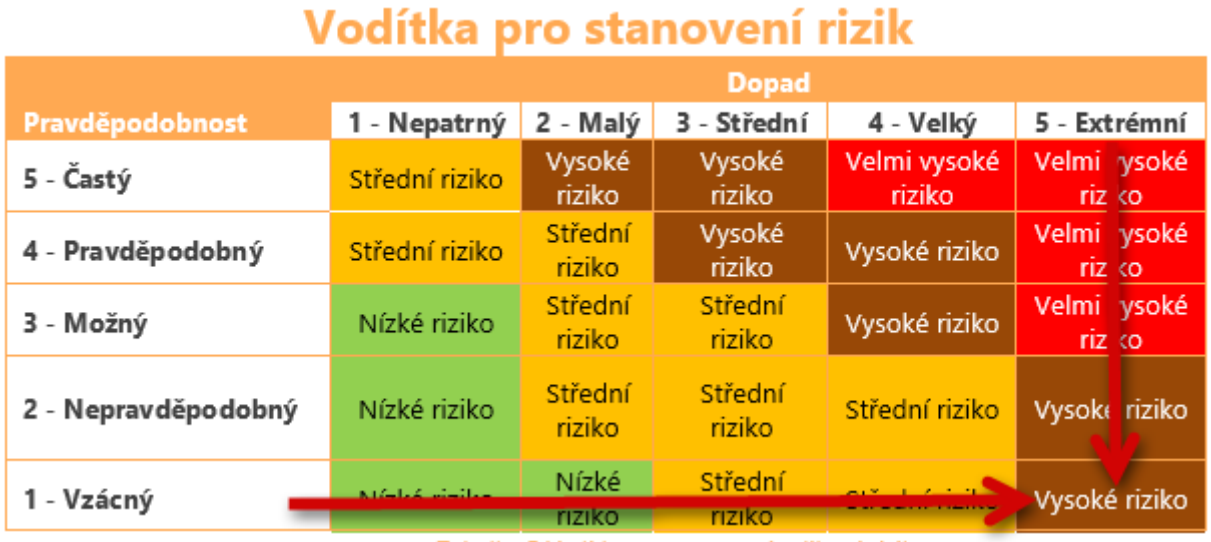
Vodítka pro stanovení rizik

	Dopad				
Pravděpodobnost	**1 - Nepatrný**	**2 - Malý**	**3 - Střední**	**4 - Významný**	**5 - Extrémní**
5 - Častý	Střední riziko	Vysoké riziko	Vysoké riziko	Velmi vysoké riziko	Velmi vysoké riziko
4 - Pravděpodobný	Střední riziko	Střední riziko	Vysoké riziko	Vysoké riziko	Velmi vysoké riziko
3 - Možný	Nízké riziko	Střední riziko	Střední riziko	Vysoké riziko	Velmi vysoké riziko
2 - Nepravděpodobný	Nízké riziko	Střední riziko	Střední riziko	Střední riziko	Vysoké riziko
1 - Vzácný	Nízké riziko	Nízké riziko	Střední riziko	Střední riziko	Vysoké riziko

Tabulka 3 Vodítka pro stanovení velikosti rizik

Příklad výpočtu rizika

Pokud velikost pravděpodobnosti úspěšnosti realizace rizika byla stanovena na *stupeň 1 – (vzácný)*, a velikost dopadu rizika na společnost *na stupeň 5 (extrémní)*, výsledkem je *Vysoké riziko,* viz příklad v tabulce níže.



Význam jednotlivých rizik popisuje *Tabulka 4 Popis stupňů rizik*.

Význam jednotlivých stupňů rizik

Velmi vysoké riziko (červená) - značí neakceptovatelné riziko. Jakékoliv riziko v této oblast by mělo spustit okamžitou reakci pro řízení rizika.
Vysoké riziko (hnědá) - indikuje nepřijatelné riziko. Organizace by měla požadovat zmírnění rizika nebo definovat jinou adekvátní odezvu.
Střední riziko (žlutá) - označuje normální akceptovatelnou úroveň rizika, obvykle bez nutnosti aplikace speciálních opatření.
Nízké riziko (zelená) - udává velmi nízké riziko, kde snížením stupně kontroly mohou být identifikovány příležitosti pro úsporu nákladů.

Tabulka 4 Popis stupňů rizik

2.4. Pokrytí zjištěných rizik

V rámci zjištění stavu pokrytí jednotlivých rizik u cloudové služby O365 a spisové služby Gordic GINIS v cloudovém prostředí Microsoft Azure byla identifikovaná a hodnocená rizika (viz kapitola *2.3.3 Výpočet velikosti rizik)* vztažena na uvedené dvě služby a stanoven stav jejich pokrytí ze strany provozovatele, společností Microsoft, Gordic a organizace státní správy. Stav pokrytí jednotlivých rizik opatřeními je uveden v kapitole *5.1 Pokrytí identifikovaných rizik. Rovněž bylo s ohledem na zavedená opatření revidováno hodnocení velikosti pravděpodobnosti, dopadů a rizik. Hodnocení je uvedeno* v Excel souboru *Cloud Risk Assessment.xlsx*, na záložce *Cloud Risk Register*.

2.5. Míra pokrytí rizik opatřeními

V rámci zjištění celkové míry pokrytí rizik opatřeními u poskytovatele a zákazníka spisové služby v cloudovém prostředí Azure, byl v kapitole *2.5 Míra pokrytí rizik* spočten celkový počet pokrytých, neaplikovatelných a nepokrytých rizik opatřeními a jejich poměr vyjádřen graficky v koláčovém grafu.

3. Hodnocení dopadů

Kapitola popisuje, jak byly ohodnoceny dopady narušení aktiv spisové služby a organizace státní správy.

Aktiva spisové služby a organizace státní správy byly ohodnoceny dle metodiky uvedené v kapitole *2.3 Hodnocení dopadu a pravděpodobnosti rizik*. Data hodnotili zaměstnanci organizace státní správy. Seznam typových aktiv, jejich vlastník a hodnocení je uvedeno v tabulce níže.

ID + Název sloupce	Vlastník	Hodnota dopadu (velmi malá, malá, střední, vysoká, velmi vysoká)
1 Pověst společnosti	Zákazník	Vysoká
2 Důvěra zákazníka	Zákazník	Vysoká
3 Věrnost a zkušenost zaměstnance	Zákazník	Vysoká
4 Duševní vlastnictví	Zákazník	Vysoká
6 Osobní data	Zákazník/Poskytovatel	Střední (provozní hodnota) / Vysoká (hodnota při ztrátě)
10 Dodávka služby	Zákazník/Poskytovatel	Střední
11 Kontrola přístupu/autentizace (root/admin)	Zákazník/Poskytovatel	Vysoká
12 Uživatelské oprávnění	Zákazník	Velmi vysoká
14 Rozhraní pro řízení cloudových služeb	Zákazník/Poskytovatel	Velmi vysoká
15 Řídící rozhraní API	Zákazník/Poskytovatel /EuropeanHealth	Střední
16 Síťová zařízení, spojení	Zákazník/Poskytovatel	Vysoká
17 Hardware	Zákazník/Poskytovatel	Nízká (záleží, kolik a jakého zařízení se ztratí) / Střední (může být závažné, pokud se ztratí a není chráněno, například šifrováním)
18 Fyzické budovy	Zákazník/Poskytovatel	Vysoká
19 Aplikace cloudového poskytovatele (Zdrojový kód)	Zákazník/Poskytovatel	Vysoká
20 Certifikace	Zákazník/Poskytovatel	Střední
21 Provozní logy (zákazníků, poskytovatele)	Zákazník/Poskytovatel	Střední
22 Bezpečnostní logy	Zákazník/Poskytovatel	Střední
23 Zálohy či archivovaná data	Zákazník/Poskytovatel	Střední

Tabulka 5 Hodnocení dopadů aktiv organizace státní správy

4. Identifikace a hodnocení rizik

Kapitola popisuje identifikovaná rizika, a jejich velikost a vlastníky.

V analýze rizik pro provoz spisové služby v cloudovém prostředí Microsoft Azure bylo identifikováno celkem 65 rizik. Pro větší přehlednost byla rizika rozdělena do následujících 15 skupin:

- Reputace
- Politiky bezpečnosti informací
- Organizace bezpečnosti informací
- Bezpečnost lidských zdrojů
- Řízení aktiv
- Řízení přístupu
- Kryptografie
- Fyzická bezpečnost a bezpečnost prostředí
- Bezpečnost provozu
- Bezpečnost komunikací
- Akvizice, vývoj a údržba systémů
- Dodavatelské vztahy
- Řízení incidentů bezpečnosti informací
- Aspekty řízení kontinuity činností
- Soulad s požadavky

Rizika byla hodnocena ve spojení s cloudovými službami O365, Azure a spisovou službou GINIS používanou organizací státní správy. Výpočet velikosti rizik byl proveden v souladu s metodikou uvedenou v kapitole *2.3.3 Výpočet velikosti rizik*. Hodnocení pravděpodobnosti realizace rizika a velikosti dopadů probíhalo expertně v rámci pracovníků státní správy dotazníkovou metodou. Data z hodnocení rizik jsou uvedena v podkapitolách níže a podrobněji pak v Excel souboru *Cloud Risk Assessment.xlsx*, na záložce *Cloud Risk Register*. Velikost rizik uvedených níže je stanovena bez ohledu na přijatá bezpečnostní opatření.

Jako nevyšší rizika o velikosti 5 byla vyhodnocena:

- 0701 Nedostatečné školení/prověření zaměstnanců
- 0801 Zneužití přenosných/vyměnitelných nosičů dat
- 0802 Špionáž, odposlech, prozrazení dat
- 0804 Odposlouchávání/modifikace dat prostřednictvím softwarového vybavení
- 0901 Distributed denial of service (DDoS)
- 1102 Nedostatečně smazaná data
- 1301 Zachytávání dat v sítích
- 1302 Skenování a testování bezpečnosti cloudové služby útočníkem
- 1401 Nedostatečné řízení rizik - analýza rizik
- 1402 Nedostatečná bezpečnost v procesech vývoje a podpory.

4.1. Reputace

Název rizika (ID 0101)	Odpovědnost	Riziko
Poškození reputace cloudové služby v důsledku chování jiných subjektů	Cloudový poskytovatel Zákazník	Střední

Reputace zákazníka cloudové služby je porušena na základě chování jiného zákazníka. Například posílání spamu, ukládání warezu, provádění hackerských praktik, DOS útoků a atp.

4.2. Politiky bezpečnosti informací

Název rizika (ID 0501)	Odpovědnost	Riziko
Chybějící strategie pro ukončení smluvního vztahu s poskytovatelem	Zákazník	Vysoké

Pokud zákazník chce, nebo musí z důvodu ukončení služby, odejít od poskytovatele cloudové služby, tak zde existuje určité riziko. Není-li zavedena úniková "exit" strategie, všechna data v cloudovém prostředí mohou být nedostupná nebo ztracena, jakmile dojde k ukončení služeb (očekávanému i neočekávanému) poskytovatele.

Název rizika (ID 0502)	Odpovědnost	Riziko
Porušení bezpečnostní politiky cloudové služby	Cloudový poskytovatel Zákazník	Vysoké

Zaměstnanci poskytovatele cloudu nebo zákazníka poruší bezpečnostní politiku cloudové služby.

Název rizika (ID 0503)	Odpovědnost	Riziko
Absence "přijetí cloudové platformy" v IT strategii společnosti.	Zákazník	Vysoké

Bez správně nastavené IT strategie (zahrnující přijetí cloudové platformy) existuje riziko, že společnost nebude mít své IT činnosti v souladu s obchodními cíli společnosti

Název rizika (ID 0504)	Odpovědnost	Riziko
Nedostatečný systém řízení bezpečnosti informací (ISMS), chybějící postupy/politiky	Cloudový poskytovatel	Vysoké

Systém pro řízení bezpečnosti informací (ISMS) není zaveden v dostatečné kvalitě. Nejsou stanoveny potřebné bezpečnostní postupy a politiky.

Název rizika (ID 0505)	Odpovědnost	Riziko
Konflikt mezi bezpečnostními politikami zákazníka a cloudového poskytovatele	Cloudový poskytovatel, Zákazník	Vysoké

Kladení různých požadavků na bezpečnost z pohledu zákazníka a cloudového poskytovatele.

4.3. Organizace bezpečnosti informací

Název rizika (ID 0601)	Odpovědnost	Riziko
Nedostatečná izolace zákazníků	Cloudový poskytovatel	Vysoké

Zahrnuje chyby v přidělovaném úložném, síťovém prostoru atp.

Název rizika (ID 0602)	Odpovědnost	Riziko
Zneužití oprávnění	Cloudový poskytovatel	Střední

Správce cloudového prostředí může zneužít přidělená oprávnění.

4.4. Bezpečnost lidských zdrojů

Název rizika (ID 0701)	Odpovědnost	Riziko
Nedostatečné školení/prověření zaměstnanců	Cloudový poskytovatel Zákazník	Velmi vysoké

Mezi zaměstnanci jak zákazníka tak cloudového poskytovatele není prováděno dostatečné školení s ohledem na používání programového vybavení a bezpečnost při práci. Ohrozí chybné použití/nastavení aplikace/úlohy nebo úspěšné provedení útoku prostřednictvím sociálního inženýrství, emailu, telefonu atp.

Zaměstnanci poskytovatele cloudu nejsou při nástupu do zaměstnání dostatečně prověřeni (rejstřík trestů, reference od předchozích zaměstnavatelů, mimopracovní aktivity, střet zájmů atp.)

Název rizika (ID 0702)	Odpovědnost	Riziko
Nedostatek zaměstnanců s potřebnou odbornou úrovní	Cloudový poskytovatel	Střední

Při nemoci, nehodě hrozí nedostatek zaměstnanců s potřebnou odbornou úrovní.

4.5. Řízení aktiv

Název rizika (ID 0801)	Odpovědnost	Riziko
Zneužití přenosných/vyměnitelných nosičů dat	Cloudový poskytovatel	Velmi vysoké

Odcizení vyměnitelných/přenosných nosičů dat, prozrazení informací, modifikace/ztráta dat.

Název rizika (ID 0802)	Odpovědnost	Riziko
Špionáž, odposlech, prozrazení dat	Cloudový poskytovatel	Velmi vysoké

Poskytovatel cloudové služby je odposloucháván (data, telefon, místnost, serverovna, kamery), infikován špiónem atp.

Název rizika (ID 0803)	Odpovědnost	Riziko
Odposlouchávání/modifikace dat prostřednictvím technického vybavení	Cloudový poskytovatel	Vysoké

Data z cloudové služby jsou modifikována/odposlouchávána prostřednictvím technického vybavení (router, firewall, odposlech Wi-Fi, Bluetooth, GSM, kamera, tiskárna, firmware, stisky kláves klávesnice atp.)

Název rizika (ID 0804)	Odpovědnost	Riziko
Odposlouchávání/modifikace dat prostřednictvím softwarového vybavení	Cloudový poskytovatel	Velmi vysoké

Data z cloudové služby jsou modifikována/odposlouchána prostřednictvím softwarového vybavení (sw router, sw firewall, aplikace, program, OS, keyloger, backdoor).

Název rizika (ID 0805)	Odpovědnost	Riziko
Data/sw/hw pocházejí z nedůvěryhodných zdrojů	Cloudový poskytovatel	Střední

Cloudový poskytovatel nedostatečně prověřuje původ/důvěryhodnost dat/hardwaru/softwaru.

4.6. Řízení přístupu

Název rizika (ID 0901)	Odpovědnost	Riziko
Distributed denial of service (DDoS)	Cloudový poskytovatel	Velmi vysoké

Služba je vystavena útoku, či jejím prostřednictvím je veden útok Distributed denial of service (DDoS).

Název rizika (ID 0902)	Odpovědnost	Riziko
Economic denial of service (EDoS)	Cloudový poskytovatel Zákazník	Střední

Existuje několik scénářů jak zneužít zákazníkem používanou cloudovou službu a způsobit tím zákazníkovi finanční ztrátu. Mezi ně patří například odcizení zákazníkovi identity, kdy útočník používá zákazníkův cloudový účet a cloudové zdroje pro svoje potřeby nebo s cílem poškodit zákazníka. V jiném případě, kdy zákazník platí za cloudovou službu na základě zpracovaných požadavků, lze pro vytvoření škody použít DDoS útok.

Název rizika (ID 0903)	Odpovědnost	Riziko
Kompromitace cloudové služby, hypervisoru	Cloudový poskytovatel	Vysoké

Každá cloudová architektura obsahuje platformu, která je umístěna nad hardwarovou vrstvou a řídí přidělování prostředků z této vrstvy. V architektuře IaaS se jedná například o hypervisor. V případě, že útočník ovládne hypervisor (řízení cloudové služby), může teoreticky kompromitovat veškerá data, která cloudová služba zpracovává.

Název rizika (ID 0904)	Odpovědnost	Riziko
Zneužití identity fyzické osoby	Cloudový poskytovatel Zákazník	Vysoké

Zneužití identity fyzické osoby - odcizení uživatelského účtu.

4.7. Kryptografie

Název rizika (ID 1001)	Odpovědnost	Riziko
Nedostatečné šifrování přenášených dat v rámci cloudu	Cloudový poskytovatel	Vysoké

Data přenášená v rámci aplikací a systémů cloudové služby nejsou šifrována, či jsou šifrována nedostatečně. Bez šifrování přenášených dat existuje riziko neautorizovaného přístupu k citlivým datům zákazníka.

Název rizika (ID 1002)	Odpovědnost	Riziko

Nedostatečné šifrování přenášených dat k zákazníkovi	Cloudový poskytovatel Zákazník	Vysoké

Data přenášená od zákazníka do cloudové služby nejsou šifrována, či jsou šifrována nedostatečně. Bez šifrování přenášených dat existuje riziko neautorizovaného přístupu k citlivým datům zákazníka.

Název rizika (ID 1003)	Odpovědnost	Riziko
Nedostatečné šifrování uložených dat	Cloudový poskytovatel Zákazník	Střední

Data uložená v cloudové službě nejsou šifrována, či jsou šifrována nedostatečně.

Název rizika (ID 1004)	Odpovědnost	Riziko
Nevhodné šifrovací algoritmy	Cloudový poskytovatel Zákazník	Střední

Pokud poskytovatel šifruje data, je nutné, aby zákazník znal použitý algoritmus. Ne všechny algoritmy jsou rovnocenné. Použití nevhodného šifrovací algoritmu může způsobit neoprávněné zveřejnění a únik přenášených a uložených dat.

Název rizika (ID 1005)	Odpovědnost	Riziko
Nepřiměřená síla/délka šifrovacího klíče	Cloudový poskytovatel Zákazník	Střední

Nevhodný síla / délka šifrovacích klíčů může způsobit neoprávněný přístup k údajům klienta.

Název rizika (ID 1006)	Odpovědnost	Riziko
Nevhodné uložení klíčů pro šifrování	Cloudový poskytovatel Zákazník	Vysoké

Klíče používané pro šifrování nejsou bezpečně uloženy/spravovány. Například, pokud jsou šifrovací klíče uloženy u cloudového poskytovatele, existuje riziko, že uložené klíče budou poskytovatelem či třetí stranou zneužity.

Název rizika (ID 1007)	Odpovědnost	Riziko
Ztráta klíčů pro šifrování	Cloudový poskytovatel Zákazník	Střední

Klíče pro šifrování dat jsou ztraceny/smazány/odcizeny/zašifrovány (ransomware).

4.8. Fyzická bezpečnost a bezpečnost prostředí

Název rizika (ID 1101)	Odpovědnost	Riziko
Selhání IT zařízení	Cloudový poskytovatel Zákazník	Střední

Selhání/chybné fungování IT zařízení (sítě, PC, HW serveru).

Název rizika (ID 1102)	Odpovědnost	Riziko
Nedostatečně smazaná data	Cloudový poskytovatel	Vysoké riziko

Data nejsou po ukončení používání smazána/dostatečně kvalitně smazána či zlikvidována/skartována (papír).

Název rizika (ID 1103)	Odpovědnost	Riziko

Neoprávněný fyzický přístup do DC	Cloudový poskytovatel	Střední

Cloudový poskytovatel je zodpovědný za zajištění fyzické bezpečnosti k zajištění zákazníkových dat před neoprávněným přístupem. Nedostatečné kontrolní mechanismy mohou mít v případě neoprávněného přístupu do serverové místnosti za následek poškození počítačového vybavení.

Název rizika (ID 1104)	Odpovědnost	Riziko
Krádež/neoprávněné použití HW zařízení a datových médií	Cloudový poskytovatel	Střední

Krádež HW zařízení/datových médií, může způsobit prozrazení/ztrátu/modifikaci dat.

Název rizika (ID 1105)	Odpovědnost	Riziko
Přírodní katastrofa	Cloudový poskytovatel	Střední

Přírodní katastrofa může způsobit zatopení datacentra, výpadek el. energie, přerušení síťového spojení atp.

Název rizika (ID 1107)	Odpovědnost	Riziko
Nedostatečné údržba datového centra	Cloudový poskytovatel	Střední

Cloudový poskytovatel provádí nedostatečně údržbu - elektřina, voda, klimatizace, IT.

Název rizika (ID 1108)	Odpovědnost	Riziko
Poruchy způsobené zářením	Cloudový poskytovatel	Střední

Poruchy zařízení způsobené elektromagnetickým, termálním zářením.

4.9. Bezpečnost provozu

Název rizika (ID 1201)	Odpovědnost	Riziko
Nedostatečné prostředky/zdroje cloudové služby, nedostupnost služby	Cloudový poskytovatel	Střední

Cloudová služba je přetížená či nedostupná. Zákazník se do služby nemůže přihlásit, služba vykazuje dlouhou odezvu, některé funkce/zdroje služby nejsou dostupné, mají pomalou odezvu atp.

Název rizika (ID 1202)	Odpovědnost	Riziko
Kompromitace rozhraní pro řízení cloudové služby	Cloudový poskytovatel	Vysoké

Rozhraní pro řízení (management interface) cloudové služby je kompromitováno - je s ním manipulováno mimo relevantní používání a oprávnění, je nedostupné.

Název rizika (ID 1203)	Odpovědnost	Riziko
Selhání programového vybavení	Cloudový poskytovatel	Vysoké

Software v rámci cloudové služby korektně nezpracovává vstupní požadavky, či nepodává korektní výstupy.

Název rizika (ID 1204)	Odpovědnost	Riziko
Nedostatečné logování, kompromitace provozních či bezpečnostních logů	Cloudový poskytovatel Zákazník	Střední

Požadované události nejsou dostatečně logovány/zaznamenávány. Provozní či bezpečnostní logy/záznamy mohou být změněny, smazány či jinak zneužity. Mohou například ovlivnit forenzní vyšetřování.

Název rizika (ID 1205)	Odpovědnost	Riziko
Kompromitace či ztráta záložních/archivních dat	Cloudový poskytovatel Zákazník	Střední

Záložní či archivovaná data mohou být změněna, smazána, či prozrazena. Není dodržena doba uchování pro administrativní bezpečnostní politiky a pokyny.

Název rizika (ID 1206)	Odpovědnost	Riziko
Nedostatečný/neaktuální/neodladěný antimalware	Cloudový poskytovatel Zákazník	Vysoké

Nedostatečně odladěná antimalwarová ochrana může vést k poškození nebo ztrátě dat, nebo způsobit nedostupnost datových a informačních systémů používaných poskytovatelem/zákazníkem cloudové služby.
Neaktuální/nedostatečná antivirová ochrana zvyšuje pravděpodobnost virové infekce a možné ztráty/modifikace/nedostupnosti dat.

Název rizika (ID 1207)	Odpovědnost	Riziko
Nedostatečně fungující vulnerability a patch management	Cloudový poskytovatel	Vysoké

Nefunguje nebo funguje nedostatečně vyhledávání zranitelností a jejich záplatování.

Název rizika (ID 1209)	Odpovědnost	Riziko
Výpadek podpůrných služeb v dodavatelském řetězci cloudového poskytovatele	Cloudový poskytovatel	Střední

Výpadek služeb dodávaných od třetích stran, které cloudový poskytovatel využívá pro běh cloudové služby. V důsledku výpadku poskytovatelů třetích stran může být cloudová služba omezena na kvalitě, funkčnosti či dostupnosti. Jedná se například o dodavatele elektrické energie, konektivity do internetu, klimatizace, autentizace, bezpečnostní služby atp.

Název rizika (ID 1210)	Odpovědnost	Riziko
Nemožnost vlastní kontroly účinnosti bezpečnostních opatření u cloudového poskytovatele	Cloudový poskytovatel	Střední

Zákazníkovy cloudové služby není umožněno provádět kontrolu účinnosti bezpečnostních opatření, například penetrační testování, skenování portů, hledání zranitelností atp.)

4.10. Bezpečnost komunikací

Název rizika (ID 1301)	Odpovědnost	Riziko
Zachytávání dat v sítích	Cloudový poskytovatel Zákazník	Velmi vysoké

Distribuovaná data z/do cloudové služby jsou zachytávána (útočníky). Jedná se například o útoky MIMT, sniffing, spoofing.

Název rizika (ID 1302)	Odpovědnost	Riziko
Skenování a testování bezpečnosti cloudové služby útočníkem	Cloudový poskytovatel	Velmi vysoké

Prostředky cloudové služby jsou natolik přístupné, že útočník může provádět bezpečnostní skenování otevřených portů a zranitelností a jiné testy ohledně stavu bezpečnosti cloudové služby.

Název rizika (ID 1303)	Odpovědnost	Riziko
Přerušení síťové komunikace	Cloudový poskytovatel Zákazník	Vysoké

Riziko, že síťová komunikace bude přerušena - prokopnutí kabelu, rušení přenášeného signálu, chybná konfigurace směrování na distribučních prvcích.

4.11. Akvizice, vývoj a údržba systémů

Název rizika (ID 1401)	Odpovědnost	Riziko
Nedostatečné řízení rizik - analýza rizik	Cloudový poskytovatel	Velmi vysoké

Poskytovatel cloudové služby by měl pravidelně revidovat analýzu rizik, prohlášení o aplikovatelnosti (SoA), plán zvládání rizik (RTP) a měření účinnosti zavedených opatření.

Název rizika (ID 1402)	Odpovědnost	Riziko
Nedostatečná bezpečnost v procesech vývoje a podpory	Cloudový poskytovatel	Velmi vysoké

Pokud poskytovatel cloudové služby vyvíjí nástroje, které používá v rámci poskytované služby, musí mít zavedenou politiku a pravidla bezpečného vývoje a podpory. Jinak hrozí, že sw bude například obsahovat chyby, citlivá provozní data budou použita pro testování, nástroj nebude odpovídat zavedeným standardům, podpora nebude poskytována v dostatečné kvalitě atp.

4.12. Dodavatelské vztahy

Název rizika (ID 1501)	Odpovědnost	Riziko
Netransparentní sub-processing	Cloudový poskytovatel	Vysoké

Cloudový poskytovatel je netransparentní ohledně subdodavatelů - kdo jsou subdodavatelé, na jakých úlohách v rámci poskytovaných služeb se podílejí, jaké mají role, kdo zodpovídá za jejich činnost, jak jsou nastaveny smluvní vztahy včetně požadavků na bezpečnosti informací, k jakým zákaznickým datům mají přístup atp.

Název rizika (ID 1502)	Odpovědnost	Riziko
Nedostatečné obchodní podmínky	Cloudový poskytovatel Zákazník	Vysoké

Service Level Agreement (SLA) - podmínky úrovně služeb.
Online Services Terms (OST) - ostatní smluvní závazky.

Pokud SLA nebo OST neexistuje, není aktuální či nejasně definovaná (detail, rozsah), nemusí odrážet současnou situaci jak u zákazníka, tak u poskytovatele cloudové služby.

Zákazník nemusí být schopen nastavit vhodné podmínky, aby efektivně řídil služby poskytované dodavatelem.

Zákazník není včas cloudovým poskytovatelem informován o plánovaných/provedených změnách v cloudové službě.

Není smluvně zakotveno, že zpracovávané informace nebudou zpracovávány pro jakýmkoliv jiný účel, než je definováno ve smlouvě.

Zákazníkovi služeb hrozí, že mu budou odepřeny prostředky, které mu umožní splnit svůj závazek ohledně opravy a / nebo vymazání osobních údajů.

Hrozí, že zpracovatel osobních údajů ve veřejném cloudu neinformuje zákazníka cloudové služby v souladu s postupy a lhůtami dohodnutými ve smlouvě o jakékoli právně závazné žádosti o sdělení osobních údajů, ze strany oprávněných orgánů, pokud je takové sdělení jinak zakázáno.

Hrozí zatajení subdodavatelů poskytovatele cloudové služby.
Neuzavření dohody o mlčenlivosti (NDA).

Název rizika (ID 1503)	Odpovědnost	Riziko
Nedostatečná integrace mezi IRM a SLA	Zákazník	Střední

V případě, že výsledky hodnocení rizik nebudou začleněny do SLA a OST mezi zákazníkem a poskytovatelem cloudové služby, existuje riziko, že zákazník nebude schopen splnit své strategické cíle.

Název rizika (ID 1504)	Odpovědnost	Riziko
Nejasné rozdělení odpovědností za implementaci bezpečnostních opatření	Cloudový poskytovatel Zákazník	Vysoké

Nejasné rozdělení odpovědností za implementaci bezpečnostních opatření - jaká opatření spravuje zákazník a jaká dodavatel cloudové služby.

4.13. Řízení incidentů bezpečnosti informací

Název rizika (ID 1601)	Odpovědnost	Riziko
Nedostatečné řešení incidentů	Cloudový poskytovatel Zákazník	Střední

Nastalé incidenty nejsou mezi zákazníkem a poskytovatelem cloudové služby řešeny v dostatečné kvalitě. Např. incidenty jsou hlášeny pozdě, neúplně, nesprávným osobám, nestandardní formou (tel, email, dopis...), formátem (xls, doc, html...) atp.

4.14. Aspekty řízení kontinuity činností

Název rizika (ID 1701)	Odpovědnost	Riziko
Nedostatečné DRP a BCP	Cloudový poskytovatel	Vysoké

Absence testování a dokumentování DR a BC plánů by mohla vést k tomu, že poskytovatel cloudu nebude schopen dostatečně (z pohledu času a požadované kvality) obnovit své klíčové procesy a systémy v případě výpadku. Kromě toho se také může stát, že zaměstnanci nebudou obeznámeni s obsahem BC a DR plánů => nebudou řádně proškoleni v postupech pro krizové situace a jejich následná reakce může být vhodná.

4.15. Soulad s požadavky

Název rizika (ID 1801)	Odpovědnost	Riziko
Chybějící bezpečnostní certifikace poskytovatele cloudu	Cloudový poskytovatel	Střední

Absence jakékoliv bezpečnostní certifikace poskytovatele služeb může znamenat, že procesy poskytovatele nejsou nastaveny v souladu s nejlepšími bezpečnostními postupy. Ta situace může vést k existenci nepokrytých bezpečnostních slabin v rámci celé platformy.

Název rizika (ID 1802)	Odpovědnost	Riziko
Riziko ztráty certifikace, nedostupnost dokumentace k prokázání certifikace	Cloudový poskytovatel	Střední

Riziko ztráty certifikace u cloudového poskytovatele. Dokumentace pro doložení certifikace není dostupná.

Název rizika (ID 1803)	Odpovědnost	Riziko
Nesoulad s nadnárodními zákony	Cloudový poskytovatel Zákazník	Střední

V případě porušení zákonných požadavků a vydání soudního/vládního rozhodnutí, může dojít k zabavení hardwarového vybavení cloudového poskytovatele a rovněž k prozrazení/nedostupnosti/ztrátě informací.

E-discovery je vládní vyšetřovací metoda pro elektronicky ukládané informace.
Obecně platí, že vlády mají právo podle vnitrostátních právních předpisů pro přístup k soukromým datům v případech, kdy je ohrožena národní bezpečnost. Vyšší riziko je v případě, kdy jsou údaje umístěny v zemích, které mají nepředvídatelné právní vymáhání.

Název rizika (ID 1804)	Odpovědnost	Riziko
Nesoulad v multijurisdikčních zákonech o datech	Cloudový poskytovatel Zákazník	Střední

Riziko dopadů uložení dat mimo oblast jurisdikce EU a nedostatek transparentnosti. Riziko legislativních změn může negativně ovlivnit podnikání. Takové změny mohou mít za následek významné změny v rámci odvětví, popř. v nákladové struktuře.

Název rizika (ID 1805)	Odpovědnost	Riziko
Nesoulad se zákonem č. 101/2000 Sb. o ochraně osobních údajů	Cloudový poskytovatel	Střední

Pro společnost, která nakládá s osobními údaji a zároveň migruje do cloudu, je nezbytné posoudit, zda poskytovatel cloudu plní podmínky stanovené Úřadem pro ochranu osobních údajů.
V případě, kdy poskytovatel cloudových služeb bude zpracovávat osobní údaje podle zákona č.101/2000 Sb., o ochraně osobních údajů, v aktuálním znění, vystupuje v roli zpracovatele osobních údajů a správce s ním musí uzavřít smlouvu o zpracování osobních údajů. Zároveň musí dodavatel cloudových služeb plnit požadavky zákona č.101/2000 Sb. nebo směrnice 95/46/ES pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích. Při nenaplnění těchto požadavků může dojít k uplatnění právních sankcí – finančních nebo s dopadem na dobré jméno. Každý poskytovatel cloudu může získat od Úřadu na ochranu osobních údajů oficiální potvrzení, že splňuje požadavky, a využívat je jako podklad pro doložení souladu se zákonem.

Název rizika (ID 1806)	Odpovědnost	Riziko
Nesoulad se zákonem č. 181/2014 Sb. a souvisejícími vyhláškami o kybernetické bezpečnosti	Cloudový poskytovatel Zákazník	Střední

Zákazník či poskytovatel cloudové služby, který podléhá zákonu 181/2014, nenaplňuje veškeré relevantní požadavky zákona a s ním souvisejících vyhlášek.

Název rizika (ID 1807)	Odpovědnost	Riziko
Nesoulad s požadavky normy ISO/IEC 27001/2013	Cloudový poskytovatel	Střední

Cloudový poskytovatel není v souladu s normoul SO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (second edition).

Název rizika (ID 1808)	Odpovědnost	Riziko
Nesoulad s doporučeními normy ISO/IEC 27017:2015	Cloudový poskytovatel	Střední

Cloudový poskytovatel není v souladu s normou ISO/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

Název rizika (ID 1809)	Odpovědnost	Riziko
Nesoulad s doporučeními normy ISO/IEC 27018:2014	Cloudový poskytovatel	Střední

Cloudový poskytovatel není v souladu s normou ISO/IEC 27018:2014 — Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

Název rizika (ID 1810)	Odpovědnost	Riziko
Nesoulad se zákonem č. 499/2004 Sb. o archivnictví	Cloudový poskytovatel Zákazník	Střední

Cloudový poskytovatel není v souladu se zákonem č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů.

Název rizika (ID 1812)	Odpovědnost	Riziko
Riziko nedodržení zákonných požadavků, opuštění jurisdikčního prostředí na straně dodavatele	Cloudový poskytovatel	Střední

Cloudový poskytovatel vědomě nedodržuje zákonné požadavky, zřekl se respektování jurisdikčního prostředí (např. respektování pouze práva USA, nikoli EU).

Název rizika (ID 1811)	Odpovědnost	Riziko
Nesoulad s GDPR EU	Cloudový poskytovatel Zákazník	Střední

Cloudový poskytovatel či zákazník není v souladu s regulatorním nařízením General Data Protection Regulation (GDPR) - regulace EU dopadající na všechny společnosti zpracovávající osobní data.

Název rizika (ID 1813)	Odpovědnost	Riziko
Licenční riziko	Cloudový poskytovatel Zákazník	Střední

Porušení licenčních podmínek. Riziko se vztahuje např. na sw licence (os, aplikace), licence duševního vlastnictví atp.

5. Pokrytí zjištěných rizik

Kapitola popisuje, jak jsou výše identifikovaná rizika pokryta opatřeními.

5.1. Pokrytí identifikovaných rizik

V rámci zjištění stavu pokrytí rizik u cloudových služeb Azure, spisové služby GINIS a O365, byla výše identifikovaná a ohodnocená rizika vztažena na uvedené tři služby a stanoven stav jejich pokrytí bezpečnostními opatřeními ze strany provozovatele, společností Microsoft a Gordic a zákazníka, organizace státní správy. Stav pokrytí jednotlivých rizik mapuje tabulka uvedená níže. Tabulka zachycuje název identifikovaného rizika a jeho stav ohledně pokrytí opatřeními.

ID rizika	Název rizika	Riziko pokryto (Ano/Ne/Neaplikovatelné) Microsoft
0101	Poškození reputace cloudové služby v důsledku chování jiných subjektů	Ano
0501	Chybějící strategie pro ukončení smluvního vztahu s poskytovatelem	Ano
0502	Porušení bezpečnostní politiky cloudové služby	Ano
0503	Absence "přijetí cloudové platformy" v IT strategii společnosti.	Neaplikovatelné
0504	Nedostatečný systém řízení bezpečnosti informací (ISMS), chybějící postupy/politiky	Ano
0505	Konflikt mezi bezpečnostními politikami zákazníka a cloudového poskytovatele	Ano
0601	Nedostatečná izolace zákazníků	Ano
0602	Zneužití oprávnění	Ano
0701	Nedostatečné školení/prověření zaměstnanců	Ano
0702	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Ano
0801	Zneužití přenosných/vyměnitelných nosičů dat	Ano
0802	Špionáž, odposlech, prozrazení dat	Ano
0803	Odposlouchávání/modifikace dat prostřednictvím technického vybavení	Ano
0804	Odposlouchávání/modifikace dat prostřednictvím softwarového vybavení	Ano
0805	Data/sw/hw pocházejí z nedůvěryhodných zdrojů	Ano)
0901	Distributed denial of service (DDoS)	Ano
0902	Economic denial of service (EDoS)	Ano
0903	Kompromitace cloudové služby, hypervisoru	Ano
0904	Zneužití identity fyzické osoby	Ano
1001	Nedostatečné šifrování přenášených dat v rámci cloudu	Ano
1002	Nedostatečné šifrování přenášených dat k zákazníkovi	Ano
1003	Nedostatečné šifrování uložených dat	Ano
1004	Nevhodné šifrovací algoritmy	Ano

ID rizika	Název rizika	Riziko pokryto (Ano/Ne/Neaplikovatelné) Microsoft
1005	Nepřiměřená síla/délka šifrovacího klíče	Ano
1006	Nevhodné uložení klíčů pro šifrování	Ano
1007	Ztráta klíčů pro šifrování	Ano
1101	Selhání IT zařízení	Ano
1102	Nedostatečně smazaná data	Ano
1103	Neoprávněný fyzický přístup do DC	Ano
1104	Krádež/neoprávněné použití HW zařízení a datových médií	Ano
1105	Přírodní katastrofa	Ano
1107	Nedostatečné údržba datového centra	Ano
1108	Poruchy způsobené zářením	Ano
1201	Nedostatečné prostředky/zdroje cloudové služby, nedostupnost služby	Ano
1202	Kompromitace rozhraní pro řízení cloudové služby	Ano
1203	Selhání programového vybavení	Ano
1204	Nedostatečné logování, kompromitace provozních či bezpečnostních logů	Ano
1205	Kompromitace či ztráta záložních/archivních dat	Ano
1206	Nedostatečný/neaktuální/neodladěný antimalware	Ano
1207	Nedostatečně fungující vulnerability a patch management	Ano
1209	Výpadek podpůrných služeb v dodavatelském řetězci cloudového poskytovatele	Ano
1210	Nemožnost vlastní kontroly účinnosti bezpečnostních opatření u cloudového poskytovatele	Ano
1301	Zachytávání dat v sítích	Ano
1302	Skenování a testování bezpečnosti cloudové služby útočníkem	Ano
1303	Přerušení síťové komunikace	Ano
1401	Nedostatečné řízení rizik - analýza rizik	Ano
1402	Nedostatečná bezpečnost v procesech vývoje a podpory	Ano
1501	Netransparentní sub-processing	Ano
1502	Nedostatečné obchodní podmínky	Ano
1503	Nedostatečná integrace mezi IRM a SLA	Neaplikovatelné
1504	Nejasné rozdělení odpovědností za implementaci bezpečnostních opatření	Ano
1601	Nedostatečné řešení incidentů	Ano
1701	Nedostatečné DRP a BCP	Ano
1801	Chybějící bezpečnostní certifikace poskytovatele cloudu	Ano
1802	Riziko ztráty certifikace, nedostupnost dokumentace k prokázání certifikace	Ano

ID rizika	Název rizika	Riziko pokryto (Ano/Ne/Neaplikovatelné) Microsoft
1803	Nesoulad s nadnárodními zákony	Ano
1804	Nesoulad v multijurisdikčních zákonech o datech	Ano
1805	Nesoulad se zákonem č. 101/2000 Sb. o ochraně osobních údajů	Ano
1806	Nesoulad se zákonem č. 181/2014 Sb. a souvisejícími vyhláškami o kybernetické bezpečnosti	Ano
1807	Nesoulad s požadavky normy ISO/IEC 27001/2013	Ano
1808	Nesoulad s doporučeními normy ISO/IEC 27017:2015	Ano
1809	Nesoulad s doporučeními normy ISO/IEC 27018:2014	Ano
1810	Nesoulad se zákonem č. 499/2004 Sb. o archivnictví	Ano
1811	Nesoulad s GDPR EU	Ano
1812	Riziko nedodržení zákonných požadavků, opuštění jurisdikčního prostředí na straně dodavatele	Ano
1813	Licenční riziko	Ano

Tabulka 6 Pokrytí rizik opatřeními u cloudových služeb Microsoft Azure a Office 365

ID rizika	Název rizika	Riziko pokryto [Ano/Ne/Neaplikovatelné] Gordic
0101	Poškození reputace cloudové služby v důsledku chování jiných subjektů	Ano
0501	Chybějící strategie pro ukončení smluvního vztahu s poskytovatelem	Neaplikovatelné
0502	Porušení bezpečnostní politiky cloudové služby	Ano
0503	Absence "přijetí cloudové platformy" v IT strategii společnosti.	Neaplikovatelné
0504	Nedostatečný systém řízení bezpečnosti informací (ISMS), chybějící postupy/politiky	Ano
0505	Konflikt mezi bezpečnostními politikami zákazníka a cloudového poskytovatele	Ano
0601	Nedostatečná izolace zákazníků	Ano
0602	Zneužití oprávnění	Ano
0701	Nedostatečné školení/prověření zaměstnanců	Ano
0702	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Ano
0801	Zneužití přenosných/vyměnitelných nosičů dat	Ano
0802	Špionáž, odposlech, prozrazení dat	Ano
0803	Odposlouchávání/modifikace dat prostřednictvím technického vybavení	Ano
0804	Odposlouchávání/modifikace dat prostřednictvím softwarového vybavení	Ano
0805	Data/sw/hw pocházejí z nedůvěryhodných zdrojů	Ano
0901	Distributed denial of service (DDoS)	Ano

0902	Economic denial of service (EDoS)	Ano
0903	Kompromitace cloudové služby, hypervisoru	Ano
0904	Zneužití identity fyzické osoby	Ano
1001	Nedostatečné šifrování přenášených dat v rámci cloudu	Ano
1002	Nedostatečné šifrování přenášených dat k zákazníkovi	Ano
1003	Nedostatečné šifrování uložených dat	Ano
1004	Nevhodné šifrovací algoritmy	Ano
1005	Nepřiměřená síla/délka šifrovacího klíče	Ano
1006	Nevhodné uložení klíčů pro šifrování	Ano
1007	Ztráta klíčů pro šifrování	Ano
1101	Selhání IT zařízení	Neaplikovatelné
1102	Nedostatečně smazaná data	Ano
1103	Neoprávněný fyzický přístup do DC	Neaplikovatelné
1104	Krádež/neoprávněné použití HW zařízení a datových médií	Ano
1105	Přírodní katastrofa	Ano
1107	Nedostatečné údržba datového centra	Neaplikovatelné
1108	Poruchy způsobené zářením	Neaplikovatelné
1201	Nedostatečné prostředky/zdroje cloudové služby, nedostupnost služby	Ano
1202	Kompromitace rozhraní pro řízení cloudové služby	Neaplikovatelné
1203	Selhání programového vybavení	Ano
1204	Nedostatečné logování, kompromitace provozních či bezpečnostních logů	Ano
1205	Kompromitace či ztráta záložních/archivních dat	Ano
1206	Nedostatečný/neaktuální/neodladěný antimalware	Neaplikovatelné
1207	Nedostatečně fungující vulnerability a patch management	Ano
1209	Výpadek podpůrných služeb v dodavatelském řetězci cloudového poskytovatele	Neaplikovatelné
1210	Nemožnost vlastní kontroly účinnosti bezpečnostních opatření u cloudového poskytovatele	Ano
1301	Zachytávání dat v sítích	Ano
1302	Skenování a testování bezpečnosti cloudové služby útočníkem	Neaplikovatelné
1303	Přerušení síťové komunikace	Neaplikovatelné
1401	Nedostatečné řízení rizik - analýza rizik	Ano
1402	Nedostatečná bezpečnost v procesech vývoje a podpory	Ano
1501	Netransparentní sub-processing	Ano
1502	Nedostatečné obchodní podmínky	Ano
1503	Nedostatečná integrace mezi IRM a SLA	Neaplikovatelné
1504	Nejasné rozdělení odpovědností za implementaci bezpečnostních opatření	Ano

1601	Nedostatečné řešení incidentů	Ano
1701	Nedostatečné DRP a BCP	Ano
1801	Chybějící bezpečnostní certifikace poskytovatele cloudu	Ano
1802	Riziko ztráty certifikace, nedostupnost dokumentace k prokázání certifikace	Ano
1803	Nesoulad s nadnárodními zákony	Ano
1804	Nesoulad v multijurisdikčních zákonech o datech	Neaplikovatelné
1805	Nesoulad se zákonem č. 101/2000 Sb. o ochraně osobních údajů	Ano
1806	Nesoulad se zákonem č. 181/2014 Sb. a souvisejícími vyhláškami o kybernetické bezpečnosti	Ano
1807	Nesoulad s požadavky normy ISO/IEC 27001/2013	Ano
1808	Nesoulad s doporučeními normy ISO/IEC 27017:2015	Ano
1809	Nesoulad s doporučeními normy ISO/IEC 27018:2014	Ano
1810	Nesoulad se zákonem č. 499/2004 Sb. o archivnictví	Ano
1811	Nesoulad s GDPR EU	Neaplikovatelné
1812	Riziko nedodržení zákonných požadavků, opuštění jurisdikčního prostředí na straně dodavatele	Ano
1813	Licenční riziko	Ano

Tabulka 7 Pokrytí rizik opatřeními u spisové služby Ginis

ID rizika	Název rizika	Riziko lze pokrýt [Ano/Ne/Neaplikovatelné] (Organizace státní správy)
0101	Poškození reputace cloudové služby v důsledku chování jiných subjektů	Ano
0501	Chybějící strategie pro ukončení smluvního vztahu s poskytovatelem	Ano
0502	Porušení bezpečnostní politiky cloudové služby	Ano
0503	Absence "přijetí cloudové platformy" v IT strategii společnosti.	Ano
0504	Nedostatečný systém řízení bezpečnosti informací (ISMS), chybějící postupy/politiky	Ano
0505	Konflikt mezi bezpečnostními politikami zákazníka a cloudového poskytovatele	Ano
0601	Nedostatečná izolace zákazníků	Neaplikovatelné
0602	Zneužití oprávnění	Ano
0701	Nedostatečné školení/prověření zaměstnanců	Ano
0702	Nedostatek zaměstnanců s potřebnou odbornou úrovní	Ano
0801	Zneužití přenosných/vyměnitelných nosičů dat	Ano
0802	Špionáž, odposlech, prozrazení dat	Ano
0803	Odposlouchávání/modifikace dat prostřednictvím technického vybavení	Ano

0804	Odposlouchávání/modifikace dat prostřednictvím softwarového vybavení	Ano
0805	Data/sw/hw pocházejí z nedůvěryhodných zdrojů	Ano
0901	Distributed denial of service (DDoS)	Ano
0902	Economic denial of service (EDoS)	Ano
0903	Kompromitace cloudové služby, hypervisoru	Ano
0904	Zneužití identity fyzické osoby	Ano
1001	Nedostatečné šifrování přenášených dat v rámci cloudu	Neaplikovatelné
1002	Nedostatečné šifrování přenášených dat k zákazníkovi	Ano
1003	Nedostatečné šifrování uložených dat	Ano
1004	Nevhodné šifrovací algoritmy	Ano
1005	Nepřiměřená síla/délka šifrovacího klíče	Ano
1006	Nevhodné uložení klíčů pro šifrování	Ano
1007	Ztráta klíčů pro šifrování	Ano
1101	Selhání IT zařízení	Ano
1102	Nedostatečně smazaná data	Ano
1103	Neoprávněný fyzický přístup do DC	Ano
1104	Krádež/neoprávněné použití HW zařízení a datových médií	Ano
1105	Přírodní katastrofa	Ano
1107	Nedostatečné údržba datového centra	Neaplikovatelné
1108	Poruchy způsobené zářením	Neaplikovatelné
1201	Nedostatečné prostředky/zdroje cloudové služby, nedostupnost služby	Neaplikovatelné
1202	Kompromitace rozhraní pro řízení cloudové služby	Neaplikovatelné
1203	Selhání programového vybavení	Neaplikovatelné
1204	Nedostatečné logování, kompromitace provozních či bezpečnostních logů	Ano
1205	Kompromitace či ztráta záložních/archivních dat	Ano
1206	Nedostatečný/neaktuální/neodladěný antimalware	Ano
1207	Nedostatečně fungující vulnerability a patch management	Ano
1209	Výpadek podpůrných služeb v dodavatelském řetězci cloudového poskytovatele	Neaplikovatelné
1210	Nemožnost vlastní kontroly účinnosti bezpečnostních opatření u cloudového poskytovatele	Ano
1301	Zachytávání dat v sítích	Ano
1302	Skenování a testování bezpečnosti cloudové služby útočníkem	Ano
1303	Přerušení síťové komunikace	Ano
1401	Nedostatečné řízení rizik - analýza rizik	Ano
1402	Nedostatečná bezpečnost v procesech vývoje a podpory	Ano
1501	Netransparentní sub-processing	Neaplikovatelné

1502	Nedostatečné obchodní podmínky	Ano
1503	Nedostatečná integrace mezi IRM a SLA	Ano
1504	Nejasné rozdělení odpovědností za implementaci bezpečnostních opatření	Ano
1601	Nedostatečné řešení incidentů	Ano
1701	Nedostatečné DRP a BCP	Ano
1801	Chybějící bezpečnostní certifikace poskytovatele cloudu	Neaplikovatelné
1802	Riziko ztráty certifikace, nedostupnost dokumentace k prokázání certifikace	Neaplikovatelné
1803	Nesoulad s nadnárodními zákony	Ano
1804	Nesoulad v multijurisdikčních zákonech o datech	Neaplikovatelné
1805	Nesoulad se zákonem č. 101/2000 Sb. o ochraně osobních údajů	Ano
1806	Nesoulad se zákonem č. 181/2014 Sb. a souvisejícími vyhláškami o kybernetické bezpečnosti	Ano
1807	Nesoulad s požadavky normy ISO/IEC 27001/2013	Ano
1808	Nesoulad s doporučeními normy ISO/IEC 27017:2015	Ano
1809	Nesoulad s doporučeními normy ISO/IEC 27018:2014	Neaplikovatelné
1810	Nesoulad se zákonem č. 499/2004 Sb. o archivnictví	Ano
1811	Nesoulad s GDPR EU	Neaplikovatelné
1812	Riziko nedodržení zákonných požadavků, opuštění jurisdikčního prostředí na straně dodavatele	Neaplikovatelné
1813	Licenční riziko	Ano

Tabulka 8 Možnost pokrytí rizika opatřeními u zákazníka ze státní správy

Podrobnější popis opatření je uveden v příloze *Příloha A Identifikace a analýza legislativních požadavků* (zákonné požadavky) a v přiloženém excelovém souboru nazvaném *Cloud Risk Assessment.xlsx*, na záložce *Cloud Risk Register* a *Registr typových opatření*. Na záložce *Cloud Risk Register* je rovněž uvedeno přehodnocení pravděpodobnosti, dopadů a rizik po aplikaci bezpečnostních opatření.

5.2. Soulad s mezinárodními standardy

5.2.1. Cloudové prostředí Microsoft

Služby Azure a O365 splňují požadavky mnoha mezinárodně uznávaných norem a standardů, například ISO/IEC 27001, ISO/IEC 27018, SOC 1-2-3, NIST 800-171, UK G-Cloud, EU Model Clauses aj.

Aktuální seznam všech norem, jejichž požadavky splňují cloudové služby Microsoft, se nachází na adrese https://www.microsoft.com/en-us/trustcenter/Compliance.

5.2.2. Spisová služba GINIS

Spisová služba GINIS od společnosti GORDIC splňuje zákonné požadavky:

- Certifikát splnění požadavků zákona 499/2004 Sb., o archivnictví a spisové službě.
- Certifikát ověření shody produktu (IS GINIS) vůči požadavkům zákona č.181/2014 Sb., o kybernetické bezpečnosti.
- Certifikát vhodného dodavatele pro řešení v oblasti elektronického podepisování dokumentů v digitální podobě a v souladu s nařízením eIDAS.


Certifikát
č. IC-20120301

GINIS verze 3, v rozsahu zákazníkem vybrané funkcionality
Posouzení vůči požadavkům zák. č. 499/2004 Sb., v platném znění, a návazných předpisů

Objednatel:
GORDIC spol. s r. o., Erbenova 4, 586 01 Jihlava

Inspekce IT/IS v rozsahu zákazníkem definované funkcionality a etalonu provedená dle schváleného metodického pokynu IO-F-CLIETA.
Posuzovaná kritéria jsou uvedena v Inspekčním protokolu.

Hodnocení: Splňuje kritéria inspekce
Platný od 21. 3. 2012

podpis
ředitel A-TEST

datum 21. 3. 2012


Certifikát
č. IC-20160501

Produkt: Informační systém GINIS®, verze 3.76
ověření shody produktu vůči požadavkům zákona č. 181/2014 Sb.,
o kybernetické bezpečnosti

Objednatel:
GORDIC spol. s r.o., Erbenova 4, 586 01 Jihlava

Inspekce IT/IS v rozsahu zákazníkem definované funkcionality a etalonu provedená dle schváleného metodického pokynu IO-F-CLIETA.
Posuzovaná kritéria jsou uvedena v Inspekčním protokolu.

Hodnocení: Splňuje kritéria inspekce
Platný od 6. 5. 2016

podpis
hlavní metodik

datum 6. 5. 2016


Certifikovaný dodavatel
information and records management society

Tento certifikát potvrzuje, že

produkt GINIS

dodavatele

GORDIC spol. s r. o.

splnil všechna kvalifikační kritéria a požadavky a byl uznán produktovou certifikační komisí IRMS CRG za oprávněného užívat „CERTIFIKÁT VHODNÉHO DODAVATELE PRO ŘEŠENÍ V OBLASTI ELEKTRONICKÉHO PODEPISOVÁNÍ DOKUMENTŮ V DIGITÁLNÍ PODOBĚ" a v souladu s nařízením eIDAS.

Předložené vzorky dokumentů podepsané elektronickým podpisem vyhovují následujícím standardům:

- XAdES ETSI TS 103171
- CAdES ETSI TS 103173
- PAdES ETSI TS 103172
- PDF/A-2b: ISO 19005-2:2011

Tomáš Bezouška, president
Information and Records Management Society – Czech Republic Group, o.s.

Identifikační číslo certifikátu:
Datum certifikace:
Datum platnosti certifikátu od:
Datum platnosti certifikátu do:

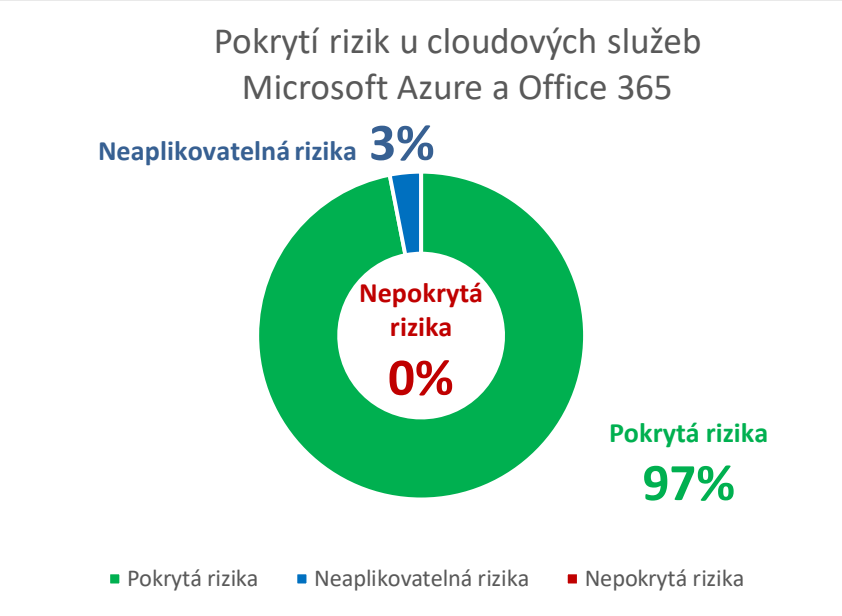
information and records management society
CZECH REPUBLIC GROUP

Vydáním tohoto certifikátu nepřebírá Information and Records Management Society – Czech Republic Group, o.s. žádnou jinou odpovědnost než ke klientovi, a to pouze v rozsahu uzavřeném platnou smlouvou.

5.3. Míra pokrytí rizik opatřeními

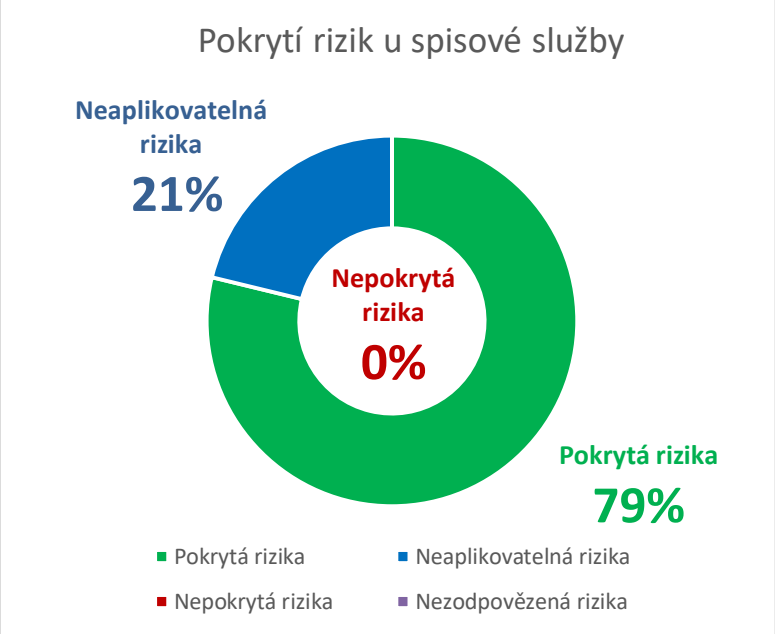
Na základě výsledků pokrytí rizik opatřeními lze konstatovat, že:

- Společnost Microsoft v rámci nabízených cloudových služeb Azure a Office 365 pokrývá 97 % identifikovaných rizik. Zbývající 3 % rizik jsou na poskytovatele cloudové služby neaplikovatelná.



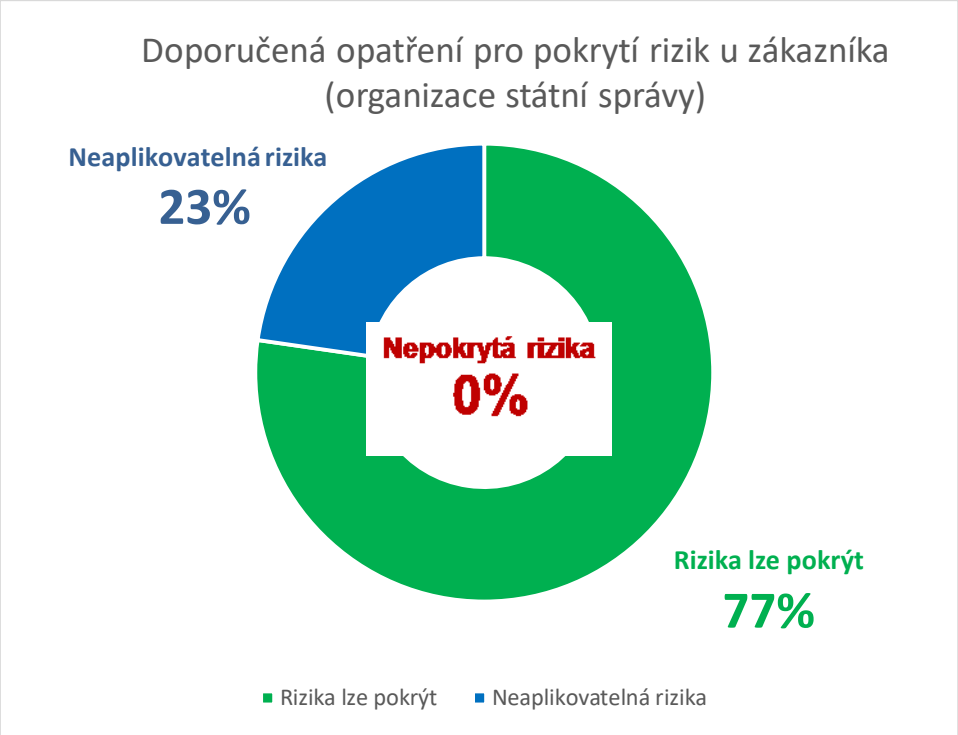
Graf 4 Pokrytí rizik u cloudových služeb Microsoft Azure a Office 365

- Společnost Gordic u spisové služby Ginis pokrývá 79 % identifikovaných rizik, 21 % rizik je neaplikovatelných.



Graf 5 Pokrytí rizik u spisové služby

- Organizace státní správy může pokrýt 77 % identifikovaných rizik, 23 % je neaplikovatelných.



Graf 6 Možnosti pokrytí rizik u organizace státní správy

6. Použité zdroje

Kapitola popisuje použité zdroje v rámci tohoto dokumentu.

Níže uvedený výčet dokumentace je registrem, který mimo jiné odkazuje na dokumenty, kde jsou uvedeny popisy konkrétních opatření. Uvedená dokumentace je přiložena jako volná příloha tohoto dokumentu. Některé z dokumentů jsou přístupné pouze pro zákazníky cloudových služeb společnosti Microsoft na základě platných NDA, a proto v případě distribuce této zprávy mimo prostředí organizaci státní správy nejsou dokumenty připojeny.

ID	Název dokumentu	Stručný popis dokumentu
00	00_AR GINIS v AZURE.pdf	Analýza rizik provozu spisové služby v Microsoft Azure
01	01_Cloud Computing Security Risk Assessment.pdf	Dokument od The European Network and Information Security Agency (ENISA) nazvaný: Cloud Computing - Benefit, risks and recommendations for information security. Dílčí zdroj pro registr rizik, aktiv a zranitelností.
02	02_Azure ISO Statement of Applicability SOA 2015 clickwraper protected.pdf	SoA pro 27001, Azure (2015)
03	03_Azure_ISO 27001 Report Aug 2015_clickwraped-protected.pdf	Assessment Report pro 27001, Azure (2015)
04	04_MCIO ISO Audit Report -clickwraped-protected FY15.pdf	Assessment Report pro 27001, Microsoft Cloud Infrastrukture Operation (MCIO) (2015)
05	05_MCIO ISO Statement of Applicability SOA 2015 clickwraped-protected.pdf	SoA pro 27001, MCIO (2015)
06	06_Microsoft Online Services Controls Aligned to ISO 27001_2013 and ISO 27018_2014 FAQ (2015).pdf	Mapuje soulad s ISO 27001 a ISO 27018, Microsoft Online Services (2015)
07	07_Microsoft-Office365-CCM-v3.0.1-2015-12-18.pdf	Mapuje požadavky Cloud Control Matrix od CSA na O365
08	08_Office 365 ISMS Statement of Applicability Security and Privacy 2015.xlsx	SoA pro 27001 a 27018 (2015)
09	09_Office 365 ISO 27001 and ISO 27018 Audit Assessment Report 2015.pdf	Assessment Report pro 27001 a 27018, Office 365 (2015)
10	10_Tenant Isolation in Office 365.pdf	Popis izolace dat uživatelů v O365
11	11_Cloud Exit Strategie zakaznika 160901.pdf	Exit strategie zákazníka pro cloudové prostření
12	12_OnlineSvcsConsolidatedSLA(WW)(Czech)(April2016)(cr).docx	Smlouva o úrovni služeb pro online služby
13	13_Shared responsibilities for cloud computing.pdf	Odpovědnosti zákazníka při používání cloudových služeb MS
14	14_Data Encryption Technologies in Office 365.pdf	Šifrování v O365
15	15_Security in Office 365 Whitepaper.docx	Bezpečnost v O365
16	16_Strategie ICT a bezpečnosti informací.docx	Strategie ICT a bezpečnosti inforamcí zákazníka
17	17_MicrosoftProductTerms(WW)(Czech)(May2016)(cr).docx	Licenční podmínky, které uvádějí seznam univerzálních licenčních podmínek a podmínek licenčního modelu vztahujících se na softwarové produkty.

ID	Název dokumentu	Stručný popis dokumentu
18	18_ISO 27001_2013 and ISO 27018_2014 Aligned FAQ (2016).pdf	Mapuje soulad s ISO 27001 a ISO 27018, Microsoft Online Services (2016)
19	19_StandardResponsetoRequestforInformationMicrosoftAzureOct2015.docx	Popisuje zabezpečení MS Azure
20	20_MicrosoftOnlineServicesTerms(Czech)(November2016)(cr).docx	Podmínky pro služby online MS (OST)
21	21_Prováděcí smlouva Enterprise.pdf	Smlouva Enterprise mezi zákazníkem a MS
22	22_Prováděcí smlouva 2014_016.pdf	Prováděcí smlouva na pořizování licencí MS (2014)
23	23_Microsoft_Cloud_Services_Risk_Management_in_European_Health.pdf	Průvodce bezpečností a ochranou osobních údajů v cloudových službách ve zdravotnictví.
24	24_Microsoft_Enterprise_Cloud_Red_Teaming.pdf	Strategie penetračního testování cloudové infrastruktury, služeb a aplikací Microsoft.
25	25_Prohlaseni-aplikovatelnosti-Gordic.pdf	Prohlášení o aplikovatelnosti společnosti Gordic
26	26_Microsoft Cloud_Information_Security_Management_System (17p. Feb 2014).pdf	ISMS pro cloudovou infrastruktutu MS. Řízení rizik
27	27_NDA_only_ISAE 3000 Microsoft CZ cloud risk management v102 CZ.PDF	Soulad metodologie posuzování rizik služby Microsoft Online Services (MOSRAM) se zákonem 181/2014 Sb.
28	28_Office 365 Residual Risk Report 2014 (MS Confidential).docx	Zbytková rizika Office 365 (2014)
29	29_Windows Azure Subcontractors.pdf	Seznam subdovatelů, kteří jsou oprávněni zpracovávat uživatelská data
30	30_GINADM01.pdf	Administrační příručka pro IS Ginis
31	31_Prohlaseni-aplikovatelnosti-2015-Gordic.pdf	Prohlášení o palikovatelnosti Gordic (2015)
32	32_S.ICZa.s.-Protecting_Data_in_MS_Cloud_202_Final.pdf	Studie se zabývá ochranou dat v prostředí online služeb společnosti Microsoft (ochranou dat v cloudových službách) z pohledu požadavků Zákona č. 181/2014 Sb., o kybernetické bezpečnosti a navazující vyhlášky č. 316/2014 Sb.
33	33_MicrosoftAzureDataProtection_Aug2014.pdf	Protecting Data in Microsoft Azure
34	34_Windows Azure Network Security Whitepaper - FINAL.docx	Síťová bezpečnost Windows Azure
35	35_ISAE 3000 Microsoft CZ cloud risk management v102 CZ (NDA info).pdf	Zpráva poskytující přiměřenou jistotu o metodologii posuzování rizik Microsoft Online Services na základě požadavků, vyplývajících z Paragrafu 5/2(b) Zákona o kybernetické bezpečnosti č.181/2014 sb., Paragrafu 4 a 7 vyhlášky o kybernetické bezpečnosti č.316/2014 sb.
36	36_Microsoft Azure ISO 27017 Certificate.pdf	Certifikát o souladu s ISO/IEC 27017:2015
37	37_Azure ISO 27018 Certificate PII 648972 Year 2016.pdf	Certifikát o souladu s ISO/IEC 27018:2014
38	38_Azure ISO 27001_27018 Statement of Applicability Year 2016.pdf	Prohlášení o aplikovatelnosti (SoA) pro MS Azure v rámci ISO/IEC 27001:2013

ID	Název dokumentu	Stručný popis dokumentu
39	39_Azure ISO 27001_27018 Assessment Report Year 2016.pdf	Zpráva z auditu pro MS Azure v rámci ISO/IEC 27001 a 27018
40	40_Azure ISO 27001 Certificate IS 577753 Year 2016.pdf	Certifikát o souladu MS Azure s ISO/IEC 27001:2013
41	41_Cílový koncept SO 160509.pdf	Popis aktuálního stavu interní infrastruktury státní organizace

Příloha A. Identifikace a analýza legislativních požadavků

V rámci této kapitoly bylo analyzováno, 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 a dokumentů v rámci spisové služby v cloudovém prostředí. Tato kapitola neobsahuje úplný výčet legislativních požadavků, které se na využití cloud computingu pro zajištění cloudové služby vztahují, ale analyzuje vybraná důležitá ustanovení týkající se ochrany osobních údajů se zaměřením na obsah smlouvy o zpracování osobních údajů mezi zákazníkem z veřejného sektoru a společnosti Microsoft a požadavků stanovených obecně na zajišťování spisové služby.

U každého požadavku je následně uvedeno, zda a jakým způsobem je daný požadavek v cloudovém prostředí Microsoft Azure pokryt podle Podmínek pro služby online platných k 1. listopadu 2016 (dále jen „**PSO**"), které stanoví podmínky pro užívání služeb online, včetně Microsoft Azure. Smluvní vztah mezi společností Microsoft a zákazníky není stanoven pouze v PSO, ale také v dalších dokumentech uzavírané zákazníkem při nákupu služby Microsoft Azure; 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 stanoví pouze vybrané legislativní požadavky implementované v PSO, nikoliv však v dalších částech smluvní dokumentace. 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 Azure schopná splnit tyto legislativní požadavky.

Nad rámec posouzení 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.

1.1 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 o ochraně osobních údajů této situaci přizpůsoben. Požadavky uvedené v této kapitole nemusí být v současnosti zcela pokryty, neboť GDPR dosud není platnou legislativou.

Vzhledem k tomu, že GDPR nabyde 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 některým 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 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").

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
Článek 28, odst. 1 GDPR	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 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 „Microsoft Azure Core" odpovídají standardům ISO 27001, ISO 27002, ISO 270018 a dalším).
Článek 28, odst. 2 GDPR	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.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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 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: **Error! Reference source not found.**
Článek 28, odst. 3 GDPR	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 zpracovatelem (společností Microsoft). **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 (…)
		(…) v nichž je stanoven předmět a doba trvání zpracování (…)	**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. *Použití zákaznických dat (str. 7)*

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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.
		(...) 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. 7)* 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. 7)* 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)*

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			„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 „zákaznická data“ zahrnuje pouze zákaznická data, která jsou poskytována prostřednictvím těchto služeb online.
		(…) kategorie subjektů údajů (…)	**Vyhodnocení:** v souladu s GDPR PSO výslovně neuvádí, zda jsou v rámci online služeb zpracovávány např. citlivé údaje vztahující se k politickému přesvědčení, náboženství či filosofii jednotlivých lidí, které se mezi údaji zpracovávanými v rámci spisové služby jistě objevují, 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.
		(…) povinnosti a práva správce (…)	**Vyhodnocení:** v souladu s GDPR Jednotlivá práva a povinnosti smluvní stran jsou uvedené napříč PSO a jsou dostatečně specifická.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
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.
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:**

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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 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.
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 zpracování 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

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			zablokovat zákaznická data, nebo (2) provádět takové opravy, odstranění nebo blokování jménem zákazníka.
Článek 28, odst. 3, písm. g)		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. V případě, že si zákazníci sami data neextrahují, Microsoft nabízí službu „Azure Import/Export", v rámci které Microsoft zajistí transfer velkých objemů dat z a do služby Azure za pomocí harddisků. Microsoft tak nabízí službu „vrácení" dat svým zákazníkům. V případě, že si zákazník data sám neextrahuje nebo nevyužije služby „Import/Export" 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)* 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	**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

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
		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.	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 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	**Vyhodnocení:** V současnosti neexistují schválené kodexy chování, 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
		osvědčení uděleného správci či zpracovateli podle článků 42 a 43. 7. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku 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 rizik, 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. *Zabezpečení – Obecné postupy (str. 11)*

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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.
Článek 32, odst. 1, písm. a)	Zabezpečení zpracování	a) pseudonymizace a šifrování osobních údajů;	**Vyhodnocení:** částečně v souladu s GDPR, k doplnění nástroji na aplikační úrovni Společnost Microsoft umožňuje zákazníkům šifrovat data uložená v různých formách v prostředí Microsoft Azure. Data uložená v blobovém uložišti Azure mohou být šifrována nativní službou „Azure Storage Service Encryption". Disky virtuálních serverů mohou využívat službu „Azure Disk Enryption", která umožňuje zašifrovat disky prostřednictvím nástroje BitLocker v případě OS Windows, případně nástrojem DM-Crypt v případě OS Linux. Pokud jsou data uložená v Azure SQL databázi, je možné pro šifrování využít nativní službu „Transparent Data Encryption (TDE)". Služby „Azure Disk Encryption" a „Transparent Data Encryption" využívají pro správu a údržbu šifrovacích klíčů službu „Azure Key Vault". Tato cloudová podoba Hardware security modulu (HSM) zajišťuje zákazníkům exkluzívní kontrolu nad přístupem k šifrovacím klíčům. Pro službu „Azure Storage Encryption" bude tato funkčnost plánovaná v brzké budoucnosti také dostupná. Dále, jak stanoví PSO, Společnost Microsoft vždy šifruje údaje při přenosech prostřednictvím veřejných sítí. Posouzení, která data by měla být šifrována a pseudonymizovaná, se musí provádět s ohledem na typ zpracovávaných údajů. Konkrétně v kontextu údajů spisové služby nelze vyloučit, že by měly být šifrovány či pseudonymizovány vždy. Takové šifrování je ovšem potřeba zajistit na aplikační úrovni služeb Azure. **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.
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.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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:
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 který 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 obnovení dat zadat ručně.
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. 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. *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.
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,	**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. **Relevantní ustanovení PSO:**

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
		uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.	*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.
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 relevantní pro oblast veřejné správy či konkrétně spisové služby 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. 7)* 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 *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.

1.2 Zákon č. 101/2000 Sb., o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů upravuje podmínky zpracování osobních údajů vztahující se na subjekty státní správy. Vzhledem k tomu, že spisová služba bude zpravidla zahrnovat dokumenty obsahující osobní údaje, uplatní se na ni i požadavky tohot zákona. Níže analyzujeme splnění těchto zákonných požadavků na zpracování osobních údaů při využití Microsoft online služby Azure. Tento zákon definuje následující požadavky na poskytovatele cloudových služeb v roli zpracovatele osobních údajů.

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. 7)* 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. 7)*

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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 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

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			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, 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.
§ 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 pro zajištění souladu se zákonem. V případě zpracování dokumentace spisové služby je však na zákazníkovi, aby vybral ta technická opatření, která odpovídají povaze údajů jím generovaných. Typ orgánu veřejné moci a zejména typ jím zpracovávaných osobních údajů bude mít vliv na přijatá opatření. **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)*

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			Před zpracováním zákaznických dat nebo spuštěním služeb online společnost Microsoft provedla posouzení rizik.
§ 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.
	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.
	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. 13)* 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. 13)* Společnost Microsoft uchovává záznam o oprávnění zabezpečení osob, které mají přístup k zákaznickým datům.

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
			- 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.
	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.
§ 27, odst. 2-3	Předání údajů do třetích zemí	2) Do třetích zemí mohou být osobní údaje předány, pokud zákaz	**Vyhodnocení**: v souladu se zákonem **Relevantní ustanovení PSO:**

ID požadavku	Stručný popis	Podrobnější popis (znění právního předpisu)	Popis pokrytí
		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,	*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.

1.3 Zákon č. 499/2004 Sb., o archivnictví a spisové službě

Požadavek zákona	Požadavek vyhlášky	Popis	Popis pokrytí požadavku ve vztahu k online službám společnosti Microsoft, konkrétně službě Microsoft Azure	Popis pokrytí požadavku ve vztahu k aplikaci GINIS
Požadavky zákona č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů	***Vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby***	Níže jsou specifikovány požadavky zákona č. 499/2004 Sb., o archivnictví a spisové službě, a vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, relevantní ke zpracování informací v digitální podobě v prostředí IS Gordic	Níže je krátké shrnutí, jak jsou legislativní požadavky splněny ve vztahu k produktům a smluvním podmínkám společnosti Microsoft pro online služby dle aktuálního znění **Podmínek pro služby online (dále jen „PSO")** účinných ke dni 1. 12. 2016 (https://www.microsoft.com/en-us/licensing/product-licensing/products.aspx#OST)	Níže je krátké shrnutí, jak jsou legislativní požadavky splněny ve vztahu k aplikaci Gordic GINIS
Uchování dokumentů v digitální podobě § 3 odst. 5		V případě dokumentů v digitální podobě se jejich uchováváním rozumí rovněž zajištění **věrohodnosti původu** dokumentů, **neporušitelnosti jejich obsahu** a čitelnosti, **tvorba a správa metadat** náležejících k těmto dokumentům v souladu s tímto zákonem a **připojení údajů prokazujících existenci dokumentu v čase**. Tyto vlastnosti musí být zachovány do doby provedení výběru archiválií.	**Vyhodnocení:** v souladu se zákonem pokud bude doplněno nástroji na aplikační úrovni. 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. Na základě toho se domníváme, že zákazník společnosti Microsoft (povinná osoba dle zákona) naplní povinnosti požadavku na neporušitelnost obsahu a čitelnosti dokumentů z pohledu jejich zabezpečení. Neporušitelnost je dále zajištěna způsobem zálohování, kdy společnost Microsoft garantuje dle PSO uchovávání několika kopií, ze kterých lze dokument obnovit. Ve vztahu k požadavkům na (i) zajištění věrohodnosti původu, (ii) tvorbu a správu metadat a (iii) připojení údajů prokazujících existenci v čase je potřeba doplnit funkcionality a nástroje na aplikační úrovni. **Relevantní ustanovení PSO:** *Zabezpečení (str. 8)* Prioritou společnosti Microsoft je napomáhat při ochraně bezpečnosti informací zákazníka. Společnost Microsoft	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace

			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 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 „Microsoft Azure Core“ odpovídají standardům ISO 27001, ISO 27002, ISO 270018 a dalším). *Sdělení a správa operací (str. 11)* - Společnost Microsoft uchovává průběžně a minimálně jednou týdně (pokud během tohoto období nebyla aktualizována žádná zákaznická data) několik kopií zákaznických dat, ze který 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.	
Mlčenlivost zaměstnanců § 14 odst. 1		Zaměstnanci správních úřadů na úseku archivnictví a výkonu spisové služby, zaměstnanci archivů a jejich zřizovatelé jsou povinni zachovávat mlčenlivost o všech skutečnostech, které se dozvěděli při výkonu činností podle tohoto zákona. Této povinnosti mohou být zproštěni příslušným správním úřadem na úseku archivnictví a	**Vyhodnocení**: v souladu se zákonem Tato povinnost se nevztahuje na zaměstnance společnosti Microsoft jako dodavatele úložiště. Nicméně za předpokladu, že (i) by společnost Microsoft byla v postavení archivu či zřizovatele archivu ve smyslu zákona nebo (ii) by na společnost Microsoft byla tato povinnost smluvně přenesena jednou z povinných osob,	Tato povinnost se nevztahuje na programové vybavení. Jedná se o organizační opatření, které původce upraví ve Spisovém řádu. Nicméně přístupy a změny informací zaznamenáváme

		výkonu spisové služby; zproštění musí být písemné s uvedením rozsahu a účelu. Povinnost mlčenlivosti stanovená zvláštními právními předpisy tím není dotčena.	povinnost mlčenlivosti pracovníků podle § 14 zákona by se vztahovala také na společnost Microsoft. **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. *Organizace zabezpečení informací (str. 11)* Pracovníci společnosti Microsoft s přístupem k zákaznickým datům jsou vázáni závazky důvěrnosti. *Standardní smluvní doložky – Dodatek 2 (str. 33)* Pracovníci musí zachovávat důvěrnost zákaznických dat a tato povinnost platí i po ukončení jejich závazků.	neměnným způsobem do transakčního protokolu. Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
Mlčenlivost zaměstnanců § 14 odst. 2		Je-li zřizovatelem archivu právnická osoba, vztahuje se povinnost zachovávat mlčenlivost podle odstavce 1 na fyzické osoby, které se vzhledem ke svému zaměstnání, funkci nebo obdobnému postavení v této právnické osobě s chráněnými údaji seznámily.	**Vyhodnocení**: v souladu se zákonem Viz posouzení § 14 odst. 1.	Tato povinnost se nevztahuje na programové vybavení. Jedná se o organizační opatření, které původce upraví ve Spisovém řádu. Nicméně přístupy a změny informací zaznamenáváme neměnným způsobem do transakčního protokolu. Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace
Mlčenlivost zaměstnanců § 14 odst. 3		Povinnost zachovávat mlčenlivost trvá i po skončení služebního poměru, pracovněprávního nebo jiného obdobného vztahu.	**Vyhodnocení**: v souladu se zákonem Viz posouzení § 14 odst. 1 a 2.	Tato povinnost se nevztahuje na programové vybavení. Jedná se o organizační

				opatření, které původce upraví ve Spisovém řádu.
Identifikátory dokumentu v digitální podobě § 15 odst. 1		Dokumenty vybrané jako archiválie a určené do péče archivu předá původce nebo vlastník dokumentu na základě protokolu o provedeném skartačním řízení nebo protokolu o provedeném výběru archiválií mimo skartační řízení určenému archivu. O předání se sepíše úřední záznam, jehož součástí je soupis předávaných dokumentů; u každého dokumentu v digitální podobě se uvedou údaje nutné pro jeho vyhledávání. Prováděcí právní předpis stanoví náležitosti soupisu předávaných dokumentů v digitální podobě.	**Vyhodnocení**: na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
Povinnosti vlastníka nebo držitele archiválie § 25 odst 1 b)		Vlastník nebo držitel archiválie je povinen b) vytvořit z dokumentu v digitální podobě vybraného jako archiválie jeho repliku v datovém formátu stanoveném prováděcím právním přepisem a předat ji neprodleně po provedeném výběru archiválií Národnímu archivu nebo digitálnímu archivu k uložení,	**Vyhodnocení**: na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Systém zajišťuje předání digitální podoby dokumentu a metadat do příslušného Archivu v souladu s přílohou Národního standardu (NSESS).
Vyřizování a podepisování dokumentů § 65 odst. 1		Při vyřizování dokumentů se všechny dokumenty týkající se téže věci spojí ve spis. Dokumenty v analogové podobě se vzájemně spojí fyzicky, dokumenty v digitální podobě se vzájemně spojí prostřednictvím metadat, vzájemné spojení dokumentu v analogové podobě a dokumentu v digitální podobě se činí pomocí odkazů.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajisti nástroji aplikace. Spojení s dokumenty v analogové podobě je třeba zajistit na uživatelské úrovni.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
Zvláštní ustanovení o dokumentech v		Převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak a změnu datového formátu dokumentu v digitální podobě provádí určený původce	**Vyhodnocení**: Převod dokumentů mohou provádět pouze tzv. určení původci, tedy kraje, obce, městské části apod. Tuto činnost dle zákona nemůže provádět Microsoft; požadavky dle § 69a zákona se na něj tedy	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Evidenci

digitální podobě § 69a odst 1		postupem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu převádění nebo změny formátu.	neuplatní. Je třeba zajistit na uživatelské úrovni, případně v samostatné aplikaci.	dokumentů (analogových i digitálních) zajistí původce v systému GINIS (provozovanému u sebe nebo jako službu). Soulad fyzického stavu a evidenčních údajů v elektronickém nástroji je zodpovědností původce. Ke splnění povinnosti je možné využít systém GINIS, nebo samostatnou aplikaci a zaevidování výsledného dokumentu v GINIS. Jedná se o organizační opatření, které původce upraví ve Spisovém řádu.
Zvláštní ustanovení o dokumentech v digitální podobě § 69a odst. 2		Připojení údajů, které vznikly při přípravě dokumentu k uchování podle § 3 odst. 5 nebo při převedení či změně datového formátu dokumentu podle odstavce 1 a které jsou pro uchování dokumentu nebo převedení nebo změnu datového formátu dokumentu nezbytné, se nepovažuje za nezajištění neporušitelnosti obsahu dokumentu.	**Vyhodnocení**: Viz posouzení § 69a odst. 1	Dtto
Zvláštní ustanovení o dokumentech v digitální podobě § 69a odst. 3		Před převedením dokumentu v digitální podobě na dokument v analogové podobě nebo změnou datového formátu dokumentu v digitální podobě ověří určený původce platnost elektronického podpisu, elektronické pečetě nebo elektronického časového razítka, je-li jimi dokument v digitální podobě opatřen, a platnost certifikátů, jsou-li na nich založeny. Údaje o výsledku ověření a datum převedení dokumentu v digitální podobě na dokument v analogové podobě nebo datum změny	**Vyhodnocení**: Viz posouzení § 69a odst. 1	Dtto

		datového formátu dokumentu v digitální podobě určený původce zaznamená a uchová je spolu s dokumentem vzniklým převedením nebo změnou datového formátu.		
Zvláštní ustanovení o dokumentech v digitální podobě § 69a odst. 4		Dokument vzniklý převedením nebo změnou datového formátu opatří určený původce doložkou. Doložku dokumentu v analogové podobě podepíše osoba odpovědná za převedení dokumentu. Doložku dokumentu v digitální podobě podepíše osoba odpovědná za převedení nebo změnu datového formátu kvalifikovaným elektronickým podpisem nebo určený původce zapečetí kvalifikovanou elektronickou pečetí a dále doložku opatří kvalifikovaným elektronickým časovým razítkem. Takový dokument má stejné právní účinky jako ověřená kopie dokumentu, jehož převedením nebo změnou datového formátu vznikl. Údaje týkající se převedení nebo změny datového formátu stanoví prováděcí právní předpis.	**Vyhodnocení**: Viz posouzení § 69a odst. 1	**Dtto**
	Příjem dokumentů v digitální podobě § 2 odst. 2	Veřejnoprávní původce vybaví podatelnu zařízením umožňujícím příjem datových zpráv1) doručovaných na elektronické adresy podatelny zveřejněné podle odstavce 3 písm. c), doručovaných na přenosných technických nosičích dat zveřejněných podle odstavce 3 písm. g), doručovaných prostřednictvím datové schránky podle odstavce 3 písm. d), má-li ji veřejnoprávní původce zřízenu a zpřístupněnu, a doručovaných jinými prostředky elektronické komunikace2), pokud je veřejnoprávní původce připouští. Pokud veřejnoprávní původce vykonává spisovou službu v elektronické podobě v	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		elektronickém systému spisové služby, je příjem datových zpráv součástí elektronického systému spisové služby nebo na něj má automatizovanou vazbu; to neplatí pro veřejnoprávního původce, u něhož to neumožňuje zvláštní povaha jeho působnosti.		
	Příjem dokumentů v digitální podobě § 3 odst. 1	Veřejnoprávní původce zaznamená datum doručení dokumentu. V případě dokumentu v digitální podobě s výjimkou dokumentu v digitální podobě doručeného na přenosném technickém nosiči dat veřejnoprávní původce zaznamená rovněž čas doručení dokumentu s přesností na sekundy.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Příjem dokumentů v digitální podobě § 4 odst. 1	*Veřejnoprávní původce zjistí, zda je doručený dokument v analogové podobě úplný a čitelný. Veřejnoprávní původce zjistí, zda je doručený dokument v digitální podobě včetně datové zprávy, v níž je obsažen, úplný, lze jej zobrazit uživatelsky vnímatelným způsobem, neobsahuje škodlivý kód, je v datovém formátu, ve kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, a je uložen na přenosném technickém nosiči dat, na kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, je-li k doručení dokumentu užito přenosného technického nosiče dat.*	**Vyhodnocení**: v souladu s vyhláškou, pokud bude doplněno nástroji na aplikační úrovni. V rámci PSO se Microsoft zavazuje používat prostředky proti neoprávněnému přístupu škodlivého software. Na úrovni Azure však PSO nepokrývají požadavky na kontrolu doručených dokumentů co do (i) úplnosti, (ii) zobrazení či (iii) správného formátu. **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* Škodlivý software. Společnost Microsoft používá prostředky proti malwaru, které brání neoprávněnému přístupu škodlivého softwaru k zákaznickým datům, včetně škodlivého softwaru pocházejícího z veřejných sítí.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

	Příjem dokumentů v digitální podobě § 4 odst. 2	Pokud veřejnoprávní původce zjistí, že doručený dokument v analogové podobě je neúplný nebo nečitelný, a je schopen určit odesílatele tohoto dokumentu a kontaktní údaje odesílatele, vyrozumí odesílatele o zjištěné vadě dokumentu a stanoví další postup pro její odstranění. Nepodaří-li se veřejnoprávnímu původci vadu doručeného dokumentu ve spolupráci s jeho odesílatelem odstranit, veřejnoprávní původce dokument dále nezpracovává. Není-li veřejnoprávní původce schopen určit odesílatele doručeného dokumentu, který je neúplný nebo nečitelný, a kontaktní údaje odesílatele, dokument dále nezpracovává.	**Vyhodnocení**: Microsoft Azure neumí zpracovávat dokumenty v analogové podobě. Neuplatní se.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. GINIS slouží i jako nástroj k evidenci metadat o dokumentech v analogové podobě.
	Příjem dokumentů v digitální podobě § 4 odst. 3	Veřejnoprávní původce postupuje podle odstavce 2 obdobně, pokud zjistí, že doručený dokument v digitální podobě včetně datové zprávy, v níž je obsažen, je neúplný, nelze jej zobrazit uživatelsky vnímatelným způsobem, obsahuje škodlivý kód, není v datovém formátu, ve kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, nebo není uložen na přenosném technickém nosiči dat, na kterém veřejnoprávní původce přijímá dokumenty v digitální podobě, je-li k doručení dokumentu užito přenosného technického nosiče dat.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Příjem dokumentů v digitální podobě § 4 odst. 4	Veřejnoprávní původce zjistí, zda je doručený dokument v digitální podobě včetně datové zprávy, v níž je obsažen, podepsán uznávaným elektronickým podpisem20) nebo označen uznávanou elektronickou značkou21), popřípadě opatřen kvalifikovaným časovým razítkem22).	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

	Příjem dokumentů v digitální podobě § 4 odst. 5	Veřejnoprávní původce ověří platnost uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, a kvalifikovaného časového razítka23).	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Příjem dokumentů v digitální podobě § 4 odst. 6	Pokud veřejnoprávní původce vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby, zaznamená údaje o výsledcích zjištění podle odstavce 1 věty druhé a odstavců 4 a 5 v elektronickém systému spisové služby. Pokud veřejnoprávní původce vykonává spisovou službu v listinné podobě, zaznamená tyto údaje způsobem stanoveným ve spisovém řádu na dokument v analogové podobě vzniklý převedením doručeného dokumentu v digitální podobě, jehož se provedená zjištění týkají.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Příjem dokumentů v digitální podobě § 4 odst. 7	Zaznamenanými údaji o výsledku zjištění podle odstavců 4 a 5 jsou alespoň a) název nebo obchodní firma akreditovaného poskytovatele certifikačních služeb, b) údaj o době, na kterou byl certifikát vydán, popřípadě, pokud jsou známy, datum a čas jeho zneplatnění, c) jméno, popřípadě jména, a příjmení, název nebo obchodní firma držitele certifikátu a d) výsledek, datum a čas ověření platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, uznávané elektronické značky a kvalifikovaného systémového certifikátu, na	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		kterém je uznávaná elektronická značka založena, a kvalifikovaného časového razítka, náležitosti kvalifikovaného časového razítka a číslo seznamu zneplatněných certifikátů, vůči kterému byla platnost certifikátů ověřována, bylo-li seznamu zneplatněných certifikátů k ověření užito.		
	Příjem dokumentů v digitální podobě § 4 odst. 8	Pokud je veřejnoprávní původce schopen z dokumentu v digitální podobě včetně datové zprávy, v níž je obsažen, doručeného na elektronickou adresu podatelny podle § 2 odst. 3 písm. c) zjistit adresu elektronické pošty odesílatele, potvrdí na základě výsledků zjištění podle odstavců 1, 4 a 5 odesílateli na tuto adresu, že dokument byl doručen a splňuje podmínky stanovené touto vyhláškou a veřejnoprávním původcem pro přijímání dokumentů. Součástí zprávy o potvrzení doručení je alespoň a) datum a čas doručení dokumentu s uvedením hodiny a minuty, popřípadě sekundy a b) charakteristika datové zprávy, v níž byl dokument obsažen, umožňující její identifikaci.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

	Příjem dokumentů v analogové podobě § 6 odst. 1	Pokud veřejnoprávní původce vykonává spisovou službu v listinné podobě, převede doručený dokument v digitální podobě autorizovanou konverzí dokumentů nebo jiným způsobem převedení podle § 69a zákona do dokumentu v analogové podobě. **Veřejnoprávní původce uloží doručený dokument v digitální podobě včetně datové zprávy, v níž je obsažen, ve tvaru, ve kterém mu byl doručen, a uchová jej po dobu nejméně 3 let ode dne doručení, pokud obsah dokumentu není spojen s výkonem práv a povinností, pro jejichž uplatnění stanoví jiný právní předpis dobu delší**; v takovém případě původce uchová doručený dokument po dobu stanovenou jiným právním předpisem pro uplatnění práv a povinností ke skutečnostem obsaženým v tomto dokumentu. Veřejnoprávní původce opatří otiskem podacího razítka, popřípadě jiným technologickým prostředkem obdobného určení jako podací razítko dokument v analogové podobě vzniklý převedením doručeného dokumentu v digitální podobě.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace. Požadavek konverze dokumentů dle § 69a zákona lze splnit pouze za využití určených původců dokumentů; tuto činnost v souladu s § 69a zákona není Microsoft oprávněn provádět a platforma Azure tuto činnost neprovádí. PSO stanoví, že zákazník společnosti Microsoft bude mít možnost přistoupit k datům po celou dobu platnosti smluvního vztahu. Microsoft tedy bude data zpracovávat po dobu platnosti smlouvy. **Relevantní ustanovení PSO:** *Uchování dat (str. 4)* Kdykoli během doby platnosti odběru zákazníka bude mít zákazník možnost přistupovat k zákaznickým datům uloženým v každé ze služeb online a tato data získávat.	Nerelevantní požadavek, je pouze pro původce se spisovou službou vedenou v listinné podobě.

	Příjem dokumentů v digitální podobě § 6 odst. 2	Pokud veřejnoprávní původce vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby, zpravidla převede doručený dokument v analogové podobě autorizovanou konverzí dokumentů nebo jiným způsobem převedení podle § 69a zákona do dokumentu v digitální podobě. Veřejnoprávní původce uchová doručený dokument v analogové podobě po dobu uchování dokumentu v digitální podobě vzniklého převedením doručeného dokumentu v analogové podobě jiným způsobem převedení podle § 69a zákona; pokud je převedení dokumentu provedeno autorizovanou konverzí dokumentů, původce uchová doručený dokument v analogové podobě po dobu nejméně 3 let s výjimkou případu, kdy je jeho obsah spojen s výkonem práv a povinností, pro jejichž uplatnění stanoví jiný právní předpis dobu delší25); v takovém případě původce uchová dokument po dobu stanovenou jiným právním předpisem pro uplatnění práv a povinností ke skutečnostem obsaženým v dokumentu.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace. Požadavek konverze dokumentů dle § 69a zákona lze splnit pouze za využití určených původců dokumentů; tuto činnost v souladu s § 69a zákona není Microsoft oprávněn provádět a platforma Azure tuto činnost neprovádí.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Evidenci dokumentů (analogových i digitálních) zajistí původce v systému GINIS (provozovanému u sebe nebo jako službu). Soulad fyzického stavu a evidenčních údajů v elektronickém nástroji je zodpovědností původce. Ke splnění povinnosti je možné využít systém GINIS, nebo samostatnou aplikaci a zaevidování výsledného dokumentu v GINIS. Jedná se o organizační opatření, které původce upraví ve Spisovém řádu.
	Označování dokumentů § 7 odst. 1	Jednoznačný identifikátor obsahuje zejména označení veřejnoprávního původce, popřípadě zkratku označení veřejnoprávního původce, a alfanumerický kód. Je-li jako jednoznačný identifikátor užit otisk podacího razítka, popřípadě jiný technologický prostředek obdobného určení jako podací razítko, nemusí obsahovat alfanumerický kód. Jednoznačný identifikátor musí být neoddělitelně spojen s dokumentem, který označuje.	**Vyhodnocení**: Toto ustanovení neukládá žádnou povinnost, pouze požadavky na identifikátor. Pokud se pro danou činnost bude vyžadovat opatření dokumentu identifikátorem, lze tento požadavek implementovat na aplikační úrovni Microsoft Azure.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Označování dokumentů § 7 odst. 3	Veřejnoprávní původce opatří doručený dokument v digitální podobě a dokument v digitální podobě vyhotovený veřejnoprávním	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace	Tento požadavek je splněn standardní funkčností aplikace

		původcem jednoznačným identifikátorem, který je s dokumentem spojen prostředky elektronického systému spisové služby.		GINIS dle provozní dokumentace.
	Označování dokumentů § 7 odst. 4	Veřejnoprávní původce zachová při převedení dokumentu v analogové podobě do dokumentu v digitální podobě podle § 6 odst. 2, při změně datového formátu dokumentu v digitální podobě nebo při převedení dokumentu v digitální podobě do dokumentu v analogové podobě s výjimkou převedení podle § 6 odst. 1 označení převáděného dokumentu i pro dokument vzniklý převedením.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Evidence dokumentů § 8 odst. 1	Veřejnoprávní původce eviduje dokumenty v základní evidenční pomůcce. Základní evidenční pomůckou spisové služby vykonávané v elektronické podobě v elektronickém systému spisové služby je elektronický systém spisové služby.	Toto ustanovení neukládá žádnou povinnost na evidenční pomůcku, resp. na elektronický systém.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Jedná se o standardní funkci.
	Evidence dokumentů § 8 odst. 2	Stanoví-li tak jiný právní předpis10) nebo veřejnoprávní původce ve spisovém řádu, veřejnoprávní původce eviduje dokumenty stanovené jiným právním předpisem nebo spisovým řádem v samostatné evidenční pomůcce, kterou je samostatná evidence dokumentů; dokumenty evidované v samostatné evidenci dokumentů veřejnoprávní původce neeviduje v základní evidenční pomůcce. Samostatná evidence dokumentů vedená v elektronické podobě musí být v souladu s požadavky stanovenými národním standardem.	**Vyhodnocení:** Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace. Z ustanovení zákona není zřejmé, co se myslí „samostatnou evidencí" a do jaké míry musí být samostatná od základní evidenční pomůcky. Konkrétně není jasné, zda musí být tento požadavek na úrovni Azure zajištěn např. uložením dat na jiné disky. Předpokládáme, že se jedná o evidenci na aplikační úrovni, kdy rozdíl mezi „evidenční pomůckou" a „samostatnou evidencí" je řešen v rámci aplikace a nejedná se o požadavek na uložení dat v rozdílných úložištích.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Evidence dokumentů § 8 odst. 5	Veřejnoprávní původce zabezpečí evidenční pomůcku proti odcizení, ztrátě, pozměňování, neoprávněnému nebo nahodilému přístupu, zničení nebo	**Vyhodnocení**: v souladu s vyhláškou do té míry, do které se požadavek uplatní na Microsoft Azure. Microsoft implementoval technická a organizační opatření podle níže uvedených ISO standardů a mnohá další	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		neoprávněnému zpracování údajů, jakož i proti jinému zneužití.	opatření, která jsou specifikována v PSO v části „Podmínky zpracování dat – Zabezpečení" na str. 11 – 12. Na základě toho se domníváme, že veřejnoprávní původce naplní povinnosti tohoto požadavku, pokud se rozhodne pro Microsoft jakožto zpracovatele osobních údajů. **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 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 „Microsoft Azure Core" odpovídají standardům ISO 27001, ISO 27002, ISO 270018 a dalším).	
	Evidence dokumentů § 8 odst. 6	Veřejnoprávní původce provede zápis v evidenční pomůcce srozumitelně a přehledně a v evidenční pomůcce vedené v listinné podobě také čitelně a způsobem zaručujícím trvanlivost zápisu. Je-li evidenční pomůcka vedena v listinné podobě, veřejnoprávní	**Vyhodnocení**: K zajištění toho, aby byly veškeré změny v údajích čitelné, je potřeba zavést opatření na aplikační úrovni. Konkrétně služba Azure Storage Services umožňuje detailní logování úspěšných a neúspěšných požadavků na Storage Account, včetně záznamu operací čtení zápisu a mazání.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Přístupy a změny informací jsou v GINIS zaznamenávány neměnným

		původce škrtne chybný zápis způsobem zaručujícím čitelnost zápisu i po provedení škrtu a v případě potřeby jej doplní správným zápisem; **u provedené opravy veřejnoprávní původce zabezpečí uvedení data opravy, jména, popřípadě jmen, příjmení a podpisu fyzické osoby, která opravu provedla.**	**Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* 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. *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.	způsobem do transakčního protokolu dle NSESS. Logování na úrovni Azure je prvek zvyšující důvěryhodnost systému.
	Evidence dokumentů § 9 odst. 2	Dojde-li ke ztrátě nebo zničení dokumentu v analogové podobě, k nevratnému poškození nebo ke zničení dokumentu v digitální podobě anebo nelze-li dokument v digitální podobě zobrazit uživatelsky vnímatelným způsobem, poznamená veřejnoprávní původce tuto skutečnost do evidenční pomůcky včetně čísla jednacího dokumentu nebo evidenčního čísla dokumentu ze samostatné evidenční pomůcky, kterým byla ztráta, poškození nebo zničení řešena.	**Vyhodnocení**: K zajištění toho, aby byly veškeré změny v údajích čitelné, je potřeba zavést opatření na aplikační úrovni. Konkrétně služba Azure Storage Services umožňuje detailní logování úspěšných a neúspěšných požadavků na Storage Account, včetně záznamu operací čtení zápisu a mazání. **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* 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. *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.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Tento bod neříká „jak zabezpečit systém proti ztrátě", ale když dojde ke ztrátě, co má úředník v systému zaznamenat.

	Evidence dokumentů § 10 odst. 1	Veřejnoprávní původce vede o dokumentu v podacím deníku tyto údaje: a) pořadové číslo dokumentu, pod nímž je evidován v podacím deníku, b) datum doručení dokumentu veřejnoprávnímu původci, a stanoví-li jiný právní předpis povinnost zaznamenat čas doručení dokumentu, rovněž čas jeho doručení, nebo datum vytvoření dokumentu veřejnoprávním původcem; datem vytvoření dokumentu veřejnoprávním původcem se rozumí datum jeho zaevidování v podacím deníku, c) údaje o odesílateli v rozsahu údajů stanoveném pro vedení údajů o odesílateli dokumentu ve jmenném rejstříku; jde-li o dokument vytvořený veřejnoprávním původcem, uvede se slovo „Vlastní“, d) identifikace dokumentu z evidence dokumentů odesílatele, je-li jí dokument označen, e) údaje o kvantitě dokumentu v rozsahu 1. počet listů, jde-li o dokument v listinné podobě, 2. počet listů nebo počet svazků příloh v listinné podobě, 3. počet a druh příloh v nelistinné podobě včetně příloh v digitální podobě; u dokumentu v digitální podobě se počet a druh příloh uvádí pouze v případě, že je povaha dokumentu umožňuje určit, f) stručný obsah dokumentu, g) označení organizační součásti veřejnoprávního původce, které byl dokument přidělen k vyřízení; pokud je veřejnoprávním původcem určena k vyřízení dokumentu fyzická osoba, uvede veřejnoprávní původce současně její jméno, popřípadě jména, a příjmení,	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		h) údaje o vyřízení dokumentu v rozsahu 1. způsob vyřízení, 2. identifikace adresáta v rozsahu údajů stanovených pro vedení údajů o adresátovi dokumentu ve jmenném rejstříku, 3. datum odeslání, 4. počet a druh odeslaných příloh; u dokumentu v digitální podobě se počet a druh příloh uvádí pouze v případě, že je povaha dokumentu umožňuje určit, a i) spisový znak a skartační režim, který vyplývá z přiděleného skartačního znaku, skartační lhůty, popřípadě z roku zařazení dokumentu do skartačního řízení a jiné skutečnosti, kterou veřejnoprávní původce stanoví jako spouštěcí událost.		
	Evidence dokumentů § 10 odst. 2	Veřejnoprávní původce vede o dokumentu v elektronickém systému spisové služby údaje stanovené v odstavci 1 a dále a) jednoznačný identifikátor dokumentu, b) informaci o tom, zda jde o dokument v digitální podobě nebo dokument v analogové podobě, c) informaci o tom, zda byl dokument zařazen do výběru archiválií a zda byl dokument vybrán jako archiválie, a d) identifikátor, který dokumentu v digitální podobě, který byl vybrán jako archiválie, přidělil Národní archiv nebo digitální archiv.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Evidence dokumentů § 10 odst. 3	Veřejnoprávní původce vede o dokumentu v samostatné evidenci dokumentů vedené v elektronické podobě alespoň údaje stanovené v odstavci 1 písm. b), c), f) a i) a v odstavci 2.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Neaplikovatelné: Požadavek na evidenci dokumentů mimo systém spisové služby.
	Evidence dokumentů § 10 odst. 4	Pořadová čísla v evidenční pomůcce tvoří číselnou řadu, která začíná číslem 1 a je složena z celých kladných čísel nepřetržitě po sobě jdoucích. V základní evidenční pomůcce	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		je číselná řada vedena od prvního kalendářního dne časového období, které veřejnoprávní původce stanoví pro vedení číselné řady (dále jen „určené časové období"), a to před zahájením určeného časového období.		
	Evidence dokumentů § 10 odst. 6	Elektronický systém spisové služby neumožní, aby byl proveden zápis dalšího dokumentu s pořadovým číslem zápisu dokumentu v elektronickém systému spisové služby, které již bylo přiděleno v rámci tohoto určeného časového období, nebo aby po ukončení určeného časového období byl proveden zápis dokumentu nebo spisu, jehož evidence náleží do následujícího určeného časového období.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace. Z ustanovení PSO vyplývá, že každý přístup k údajům v Azure je opatřen jedinečným ID. Zákonný požadavek je tedy částečně pokryt přímo v rámci aplikace Azure, na základě smluvních ustanovení v PSO. Pro zajištění souladu s požadavkem na pořadové číslo a na zápis v jednotlivých časových obdobích je ovšem potřeba upravit podmínky a funkcionality na aplikační úrovni. **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* 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.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Číslo jednací a evidenční číslo ze samostatné evidence dokumentů § 11 odst. 1	Dokument zaevidovaný v elektronickém systému spisové služby nebo v podacím deníku označuje veřejnoprávní původce číslem jednacím. Číslo jednací obsahuje označení nebo zkratku označení veřejnoprávního původce, pořadové číslo zápisu dokumentu v základní evidenční pomůcce a označení určeného časového období, kterým je zpravidla kalendářní rok, popřípadě označení nebo zkratku označení organizační součásti veřejnoprávního původce nebo jiné znaky charakterizující	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		skutečnosti související s dokumentem. Eviduje-li veřejnoprávní původce dokument ve sběrném archu podle § 12 odst. 3, uvede v čísle jednacím za pořadovým číslem zápisu dokumentu v základní evidenční pomůcce pomlčku nebo lomítko a pořadové číslo zápisu dokumentu ve sběrném archu.		
	Číslo jednací a evidenční číslo ze samostatné evidence dokumentů § 11 odst. 2	Veřejnoprávní původce přidělí dokumentu evidovanému v samostatné evidenci dokumentů evidenční číslo ze samostatné evidence dokumentů; strukturu evidenčního čísla stanoví veřejnoprávní původce ve spisovém řádu. Evidenční číslo ze samostatné evidence dokumentů musí splňovat minimálně podmínky stanovené pro jednoznačný identifikátor.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Neaplikovatelné: Požadavek na evidenci dokumentů mimo systém spisové služby.
	Číslo jednací a evidenční číslo ze samostatné evidence dokumentů § 11 odst. 3	Pokud veřejnoprávní původce k jednomu doručenému dokumentu vyhotovuje jeden vyřizující dokument, může ho připojit k doručenému dokumentu a označit ho stejným číslem jednacím nebo stejným evidenčním číslem ze samostatné evidence dokumentů jako doručený dokument.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

	Tvorba spisu § 12 odst. 4	Veřejnoprávní původce vede v elektronickém systému spisové služby nebo v samostatné evidenci dokumentů vedené v elektronické podobě údaje o spisu v rozsahu a) jednoznačný identifikátor spisu, b) stručný obsah spisu, c) spisová značka spisu, d) datum založení spisu, e) datum uzavření spisu, f) spisový znak spisu, g) skartační režim spisu, h) údaje o uložení spisu, kterými jsou počet uložených listů dokumentů v listinné podobě tvořících spis, popřípadě svazků příloh v listinné podobě dokumentů tvořících spis, i) informace o tom, zda spis obsahuje dokumenty v analogové podobě a jejich fyzické umístění, j) informaci o tom, zda byl spis zařazen do výběru archiválií a zda byl spis vybrán jako archiválie, a k) identifikátor, který spisu obsahujícímu dokumenty v digitální podobě, který byl vybrán jako archiválie, přidělil Národní archiv nebo digitální archiv.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Tvorba spisu § 12 odst. 6	Vyžaduje-li to jiný právní předpis11) nebo to z jiných důvodů považuje veřejnoprávní původce za účelné, označí spis spisovou značkou, pod níž je také evidován. Spisovou značkou je a) v případě tvorby spisu spojováním dokumentů číslo jednací nebo evidenční číslo ze samostatné evidence dokumentů prvního nebo posledního evidovaného dokumentu, b) v případě tvorby spisu pomocí sběrného archu číslo jednací nebo evidenční číslo ze samostatné evidence dokumentů iniciačního dokumentu bez pořadového čísla zápisu	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		tohoto dokumentu ve sběrném archu, nebo c) jiné označení.		
	Rozdělování a oběh dokumentů § 13 odst. 2	Veřejnoprávní původce zajistí oběh dokumentů a spisů způsobem umožňujícím sledovat veškeré úkony s dokumenty a spisy, identifikovat fyzické osoby, které úkon provedly, a určit datum, kdy byly úkony provedeny.	**Vyhodnocení**: v souladu s vyhláškou **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* 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.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Podrobnosti zpracování a struktura spisového a skartačního plánu § 15 odst. 6	Veřejnoprávní původce, který vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby, zpracovává spisový a skartační plán v elektronické podobě ve struktuře určené pro zaslání podle schématu XML pro export a import spisového a skartačního plánu stanoveného národním standardem.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Odesílání dokumentů § 18 odst. 3	Vykonává-li veřejnoprávní původce spisovou službu v elektronické podobě v elektronickém systému spisové služby, je odesílání datových zpráv součástí elektronického systému spisové služby, pokud není zprostředkováno automatizovanou vazbou na tento systém; to neplatí pro veřejnoprávního původce, u něhož to neumožňuje zvláštní povaha jeho působnosti.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Odesílání dokumentů § 18 odst. 4	Veřejnoprávní původce zajistí před odesláním datové zprávy kontrolu případného výskytu škodlivého kódu.	**Vyhodnocení**: v souladu s vyhláškou	Tento požadavek je splněn standardní funkčností aplikace

			V rámci PSO se Microsoft zavazuje používat prostředky proti neoprávněnému přístupu škodlivého software. **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* Škodlivý software. Společnost Microsoft používá prostředky proti malwaru, které brání neoprávněnému přístupu škodlivého softwaru k zákaznickým datům, včetně škodlivého softwaru pocházejícího z veřejných sítí.	GINIS dle provozní dokumentace. Realizace formou volání externího antivirového programu.
	Ukládání dokumentů § 19 odst. 2	Veřejnoprávní původce před uložením kontroluje uzavřený spis a vyřízený dokument, jsou-li úplné, zda jsou v evidenční pomůcce správně zpracovány všechny povinné údaje a zda jsou dodrženy podmínky uzavření spisu. Předmětem kontroly je zejména a) označení doručeného dokumentu v analogové podobě podacím razítkem a úplnost jeho vyplnění, b) označení dokumentu v analogové podobě jednoznačným identifikátorem zajišťujícím identifikaci a nezaměnitelnost tohoto dokumentu v elektronickém systému spisové služby původce, je-li dokument v analogové podobě v tomto systému evidován nebo zpracováván, c) kompletnost spisu obsahujícího dokumenty v analogové podobě v rozsahu dokumentů uvedených v soupisu dokumentů podle § 12 odst. 2 nebo ve sběrném archu podle § 12 odst. 3, d) počet listů dokumentu v listinné podobě, počet listinných příloh dokumentu a počet listů těchto příloh, popřípadě počet svazků listinných příloh dokumentu; u příloh v nelistinné podobě jejich počet a druh, e) celkový počet listů, popřípadě počet svazků listinných příloh podle písmene d)	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Pro analogové dokumenty se může jednat o organizační opatření, které původce upraví ve Spisovém řádu (kontrola podacího razítka atp.).

		spisu u dokumentů v analogové podobě, f) převedení dokumentu v digitální podobě do výstupního datového formátu, g) uvedení spisového znaku a skartačního režimu u všech dokumentů a spisů, h) zápis v evidenční pomůcce a jeho úplnost, a to podle druhu evidence, ve které je dokument evidován, i) uložení dokumentů a spisů v obalech, které zaručují jejich neporušitelnost a zachování jejich čitelnosti, j) uložení dokumentů v digitální podobě zpracovávaných před vyřízením na přenosných technických nosičích dat v elektronickém systému spisové služby nebo jejich převedení podle § 6 odst. 1 a opatření doložkou podle § 24.		
	Ukládání dokumentů § 19 odst. 3	Pokud veřejnoprávní původce vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby, je evidence uložených dokumentů a spisů jeho součástí.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Ukládání dokumentů § 19 odst. 4	Spisovna vede evidenci o zapůjčování a nahlížení do dokumentů a spisů. Pokud veřejnoprávní původce vykonává spisovou službu v elektronické podobě v elektronickém systému spisové služby, vede evidenci v tomto systému. Veřejnoprávní původce stanoví postup při zapůjčování a nahlížení do dokumentů a spisů a podrobnosti vedení evidence ve spisovém řádu.	**Vyhodnocení**: v souladu s vyhláškou **Relevantní ustanovení PSO:** *Sdělení a správa operací (str. 11)* 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. *Protokolování událostí (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.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

			Řízení přístupu (str. 12) Zásady přístupu. Společnost Microsoft uchovává záznam o oprávnění zabezpečení osob, které mají přístup k zákaznickým datům. Oprávnění k přístupu - Společnost Microsoft uchovává a aktualizuje záznam pracovníků oprávněných k přístupu k systémům společnosti Microsoft, které obsahují zákaznická data. - Společnost Microsoft deaktivuje pověření pro ověření, která nebyla používána po dobu maximálně šesti měsíců. - Společnost Microsoft identifikuje pracovníky, kteří mohou udělovat, měnit nebo rušit autorizovaný přístup k datům a prostředkům. - Společnost Microsoft zajistí, že pokud k systémům obsahujícím zákaznická data přistupuje více než jedna osoba, budou mít tyto osoby oddělená ID a přihlašovací údaje.	
	Postup při vyřazování dokumentů a podrobnosti skartačního řízení ***§ 20 odst. 5***	Veřejnoprávní původce sestaví z elektronického systému spisové služby nebo ze samostatné evidence dokumentů vedené v elektronické podobě seznam dokumentů určených k posouzení ve skartačním řízení. Tento seznam je tvořen podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem a obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Postup při vyřazování dokumentů a podrobnosti skartačního řízení ***§ 21 odst. 4***	Veřejnoprávní původce předá příslušnému archivu do péče dokumenty a spisy v analogové podobě a úřední razítka vybrané jako archiválie; jedná-li se o dokumenty v analogové podobě evidované v elektronickém systému spisové služby, veřejnoprávní původce předá rovněž metadata k nim náležející. V případě, že jsou	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		jako archiválie vybrány dokumenty nebo spisy v digitální podobě, veřejnoprávní původce předá příslušnému archivu jejich repliky a k nim náležející metadata. Tyto repliky a metadata veřejnoprávní původce předá příslušnému archivu zpracované podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem a schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem.		
	Postup při vyřazování dokumentů a podrobnosti skartačního řízení ***§ 21 odst. 7***	Součástí úředního záznamu je soupis předávaných dokumentů, spisů a úředních razítek vybraných jako archiválie zpracovaný veřejnoprávním původcem v rozsahu údajů stanovených v § 20 odst. 4 s výjimkou uvedení skartačního znaku a skartační lhůty. Jestliže jsou dokumenty evidované v elektronickém systému spisové služby nebo v samostatné evidenci dokumentů vedené v elektronické podobě, veřejnoprávní původce předá dokumenty, spisy a úřední razítka vybrané jako archiválie na základě seznamu vytvořeného archivem podle schématu XML pro zasílání údajů o rozhodnutí ve skartačním řízení a potvrzení přejímky s identifikátory digitálního archivu původci stanoveného národním standardem. Příslušný archiv sepíše úřední záznam po předání dokumentů a spisů v analogové podobě a úředních razítek vybraných jako archiválie do příslušného archivu a po potvrzení úspěšného přenosu dokumentů a spisů v digitální podobě vybraných jako archiválie do digitálního archivu.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace. Soupis jiných entit (např. úředních razítek, pečetí atp.) musí vyhotovit zodpovědná osoba.

	Postup při vyřazování dokumentů a podrobnosti skartačního řízení § 21 odst. 8	V případě dokumentů v digitální podobě veřejnoprávní původce provede jejich zničení smazáním z elektronického systému spisové služby a dalších úložišť. Obdobně veřejnoprávní původce postupuje při zničení dokumentů v digitální podobě, které byly vybrány jako archiválie a jejichž repliky předal veřejnoprávní původce do digitálního archivu.	**Vyhodnocení:** v souladu s vyhláškou **Relevantní ustanovení PSO:** *Uchování dat (str. 4)* Po uplynutí 90denního období uchování společnost Microsoft účet zákazníka deaktivuje a odstraní zákaznická data. *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. *Likvidace komponent (str. 11)* Společnost Microsoft používá standardní procesy odvětví k odstranění zákaznických dat, když již nejsou potřeba	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 1	Výstupním datovým formátem dokumentů v digitální podobě se rozumí a) datový formát výstupu z elektronického systému spisové služby, b) datový formát dokumentu ukládaného ve spisovně, která je součástí elektronického systému spisové služby, c) datový formát pro předávání do digitálního archivu.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 2	Výstupním datovým formátem statických textových dokumentů a statických kombinovaných textových a obrazových dokumentů je datový formát Portable Document Format for the Long-term Archiving (PDF/A, ISO 19005).	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek (kontrola validity výstupních datových formátů) je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 3	Výstupním datovým formátem statických obrazových dokumentů je a) datový formát Portable Network Graphics (PNG, ISO/IEC 15948), b) datový formát Tagged Image File Format (TIF/TIFF, revize 6 – nekomprimovaný),	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek (kontrola validity výstupních datových formátů) je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

		c) datový formát Joint Photographic Experts Group File Interchange Format (JPEG/JFIF, ISO/IEC 10918).		
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 4	Výstupním datovým formátem dynamických obrazových dokumentů je a) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 2 (MPEG-2, ISO/IEC 13818), b) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu Moving Picture Experts Group Phase 1 (MPEG-1, ISO/IEC 11172), c) datový formát Graphics Interchange Format (GIF).	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek (kontrola validity výstupních datových formátů) je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 5	Výstupním datovým formátem zvukových dokumentů je a) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu MPEG-1 Audio Layer II nebo MPEG-2 Audio Layer II (MP2), b) datový formát umožňující uložení komprimovaných dat kódovaných podle standardu MPEG-1 Audio Layer III nebo MPEG-2 Audio Layer III (MP3), c) datový formát Waveform audio format (WAV), modulace Pulse-code modulation (PCM).	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek (kontrola validity výstupních datových formátů) je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 6	Výstupním datovým formátem pro databáze je datový formát Extensible Markup Language Document (XML), kde součástí předávaného dokumentu v datovém formátu XML je popis jeho struktury pomocí schématu XML nebo Document Type Definition (DTD), o kterém veřejnoprávní původce vede dokumentaci.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek (kontrola validity výstupních datových formátů) je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.

	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 7	Výstupním datovým formátem metadat, jimiž jsou opatřovány dokumenty v elektronickém systému spisové služby, je datový formát Extensible Markup Language Document (XML) podle schématu XML pro výměnu dokumentů a jejich metadat mezi elektronickým systémem spisové služby stanoveného národním standardem nebo datový formát Extensible Markup Language Document (XML) podle schématu XML pro vytvoření datového balíčku SIP stanoveného národním standardem, který obsahuje metadata podle schématu XML pro zaznamenání popisných metadat uvnitř datového balíčku SIP stanoveného národním standardem.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek (kontrola validity výstupních datových formátů) je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Výstupní datové formáty dokumentů v digitální podobě § 23 odst. 8	Veřejnoprávní původce může pro výstup z elektronického systému spisové služby podle odstavce 1 písm. a) současně použít také jiný datový formát.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace.
	Údaje týkající se převedení nebo změny datového formátu dokumentu § 24 odst. 1	Údaje týkající se převedení dokumentu v analogové podobě do dokumentu v digitální podobě jsou a) název nebo obchodní firma veřejnoprávního původce, který převedení provedl, b) počet listů, z nichž se skládá převáděný dokument, c) informace o existenci vodoznaku, reliéfního tisku nebo embossingu, suché pečetě nebo reliéfní ražby, optického variabilního prvku, jiného zajišťovacího prvku, plastického písma nebo otisku plastického razítka, d) datum vyhotovení ověřovací doložky, e) jméno, popřípadě jména, a příjmení fyzické osoby, která převedení provedla.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace, za předpokladu realizace pomocí prostředků GINIS nebo integrovanými v GINIS.

	Údaje týkající se převedení nebo změny datového formátu dokumentu § 24 odst. 2	Údaje týkající se převedení dokumentu v digitální podobě do dokumentu v analogové podobě jsou a) název nebo obchodní firma veřejnoprávního původce, který převedení provedl, b) informace o existenci zajišťovacího prvku, c) datum vyhotovení ověřovací doložky, d) jméno, popřípadě jména, a příjmení fyzické osoby, která převedení provedla.	**Vyhodnocení**: Na platformě Azure lze požadavek implementovat na aplikační úrovni. Pro zajištění souladu je však potřeba zajistit nástroji aplikace.	Tento požadavek je splněn standardní funkčností aplikace GINIS dle provozní dokumentace, za předpokladu realizace pomocí prostředků GINIS nebo integrovanými v GINIS.