Digitální a informační agentura

Dopad U.S. CLOUD Act a U.S. FISA Act na data v cloudu

V návaznosti na dotazy ohledně **dopadů vybrané judikatury platné v USA**, která se vztahuje i na **poskytovatele cloud computingu zapsané v katalogu cloud computingu**, a to ohledně **povinnosti vydat data**, jsme připravili stručný přehled k této problematice.

První část se zabývá obecným přehledem a navazuje shrnutí, jak reagují na vládní požadavky na zpřístupnění zákaznických dat, zejména podle U.S. CLOUD Act a FISA Act vybraní poskytovatelé cloud computingu, kteří mají sídlo v USA a zároveň mají zapsané nabídky v katalogu cloud computingu. Informace vychází z veřejně dostupných zdrojů.

Pozn. citace vyjádření jsou zde uvedena pro přehlednost modrou barvou, přeloženo z angličtiny.

1. Přehled vybrané legislativy USA

U.S. Department of Justice – CLOUD Act (Clarifying Lawful Overseas Use of Data) z r. 2018, oficiální výklad zde: Promoting Public Safety, Privacy, and the Rule of Law Around the World – The Purpose and Impact of the CLOUD Act (DOJ White Paper, duben 2019)[1], dále viz plný text[2].

CLOUD Act sám o sobě nevytváří nový typ příkazu – pouze rozšiřuje územní působnost existujících procesních nástrojů dle Stored Communications Act (SCA, 18 U.S.C. §§ 2701–2713). CLOUD Act se vztahuje na „providers of electronic communication service" (ECS) nebo „remote computing service" (RCS), kteří podléhají jurisdikci USA, bez ohledu na to, kde jsou data fyzicky uložena.

Prakticky to znamená, že CLOUD Act dopadá nejen na společnosti s hlavním sídlem v USA, ale také **na všechny zahraniční společnosti, které podléhají jurisdikci USA** – např. proto, že mají **pobočku nebo dceřinou společnost se sídlem v USA** nebo mají „**podstatnou operativní přítomnost" v USA,** tedy aktivně nabízejí svoje služby prostřednictvím distribučního kanálu. Povinnost zpřístupnit data se vztahuje na údaje, které má poskytovatel ve své držbě, správě nebo pod svou kontrolou (custody / control / possession). To znamená, že žádost o zpřístupnění dat ne-amerických osob lze uplatnit na jakéhokoliv poskytovatele cloud computingu podléhajícího jurisdikci USA, **který má v USA sídlo nebo pobočku** nebo který **aktivně nabízí svoje cloudové služby** v USA.

Postup při vydání příkazu pro získání obsahu elektronické komunikace podle SCA:

1. Vyšetřující orgán (FBI nebo jiná agentura) shromáždí důkazy a sepíše Affidavit
2. Department of Justice (DoJ), státní zástupce právně zkontroluje, zda je splněn standard pro žádost (probable cause), který je vyžadován pro přístup k obsahu komunikace
3. Federální soud nebo Magistrate judge vydá SCA Warrant dle Federal Rules of Criminal Procedure. Bez rozhodnutí soudce nelze vydat příkaz na **obsah komunikace**.

Možná obrana:

Poskytovatelé nemohou odmítnout příkaz jako takový, ale mohou se odvolat na **konflikt cizího práva**. CLOUD Act výslovně umožňuje poskytovateli podat návrh na zrušení nebo omezení příkazu, pokud by

[1] https://www.justice.gov/criminal/cloud-act-resources
[2] https://www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf

jeho splnění bylo v rozporu s právem cizího státu. Konkrétně, pokud se data týkají osob, které nepobývají v USA a nejsou tzv. United States person[3] (dále jen „ne-U.S. osoby"), a pokud existuje skutečný konflikt práva (např. GDPR), soud provede balancing test (tzv. comity analysis), a může zrušit daný požadavek (viz 18 U.S.C. § 2703(h) CLOUD Act). Příklady zpracování prováděného subjekty sídlících mimo EU podléhajícího GDPR, které mohou způsobit konflikt práva, naleznete např. v článku GDPR Article 27 Explained: EU Representative Requirement for Non-EU Controllers and Processors (With Practical Examples)

Dále může poskytovatel napadnout příkaz u soudu s tvrzením, že příkaz nespadá pod SCA (Stored Communications Act). SCA vymezuje, jaký typ dat, od jakých subjektů a za jakých podmínek může stát požadovat – primárně *electronic communications*, *stored communications*, *subscriber records*. **Nevztahuje se ale např. na interní firemní dokumenty, databáze**, která nejsou komunikací ani záznamem o účtu zákazníka, a také na **data vzniklá výhradně na straně zákazníka**.

Dále může poskytovatel podle čtvrtého dodatku Ústavy USA (upravující ochranu proti nepřiměřeným zásahům) argumentovat, že příkaz je **nepřiměřený** (unreasonable / overbroad), tzn. že je příkaz příliš široký a požaduje více dat, než je nutné, že není dostatečně konkrétní (ze kterých uživatelských účtů, za jaké období, jaký typ dat). Takto může poskytovatel **omezit jeho rozsah** a požadovat upřesnění účtu / datového typu, trvat na minimálním nezbytném rozsahu, předat jen metadata, odmítnout předat data mimo svou kontrolu nebo data šifrovaná pomocí customer-managed keys.

Pokud poskytovatel nevlastní dešifrovací klíče, pokud používá šifrování typu end-to-end na přenosové trase, nebo pokud má architekturu customer-managed keys (BYOK / HYOK), a tedy nemůže data poskytnout, protože k nim nemá přístup, pak toto DoJ akceptuje jako legitimní stav.

Pro srovnání je ještě vhodné uvést, že **extrateritoriální přístup orgánů činných v trestním řízení** k údajům vyšetřovaných osob **není specifikem USA**. I jiné země (Velká Británie[4], Kanada[5]) mají zákony či soudní precedenty, které jim umožňují získat přístup k údajům uloženým v jiných jurisdikcích. Podobně mezinárodní iniciativy, včetně připravované Úmluvy OSN proti kyberkriminalitě[6], směřují k posílení mechanismů mezinárodní spolupráce při získávání elektronických důkazů. Tento trend se výrazně projevuje také v právu EU. **Nařízení (EU) 2023/1543 o elektronických důkazech (tzv. e-Evidence),** použitelné od 18. srpna 2026, zavádí evropské vydávací a uchovávací příkazy (EPOC-European Production Orders a EPOC-PR – European Preservation Orders). Ty umožňují orgánům členských států vydávat **právně závazné příkazy přímo poskytovatelům služeb nabízejícím služby v EU**, a to **bez ohledu na fyzickou lokalitu uložených dat.** EPOC[7] umožňuje získat data přímo od poskytovatele v jiném státě EU a vydává jej soud, v případě nejméně citlivých dat státní zástupce. Tento mechanismus představuje významný posun oproti tradičním nástrojům mezinárodní justiční spolupráce (např. MLAT), neboť umožňuje přímou komunikaci mezi orgány a poskytovateli služeb a zásadně zkracuje dobu získávání elektronických důkazů.

[3] Tzn. nejsou občany USA, nemají zde trvalý pobyt ani sídlo a nejsou neregistrovaným sdružením, většina jehož členů jsou občany USA či osoby s trvalým pobytem v USA.
[4] UK (Overseas Production Orders) Crime Act 2019, prostřednictvím Overseas Production Orders
[5] Judikatury: R v. Love (2022 ABCA 269 - Facebook); Brecknell (2018 BCCA 5), OVH case 2024-2026
[6] www.unodc.org/unodc/en/cybercrime/convention/home.html
[7] Nařízení (EU) 2023/1543 čl. 5-7: EPOC, a čl. 11+: postup, notifikace, možnosti odmítnutí, pojistky

Povinnosti poskytovatelů služeb elektronických komunikací a dalších relevantních služeb v oblasti poskytování elektronických důkazů podle směrnice (EU) 2023/1544 o elektronických důkazech budou v českém právním řádu nově upraveny také zákonem o určování provozoven a jmenování zástupců některých poskytovatelů služeb za účelem shromažďování elektronických důkazů v trestním řízení. Návrh tohoto zákona, který transponuje směrnici do českého právního řádu, je v současnosti projednáván v Poslanecké sněmovně.

U.S. **Foreign Intelligence Surveillance Act, zkráceně FISA** (zejména FISA Section 702) dopadá výlučně na U.S. electronic communication service providers, které zavazuje ke spolupráci při cílení ne-U.S. osob nacházejících se v zahraničí. Jedná se o zpravodajský, nikoliv trestně-procesní režim, viz www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702, nebo přímo https://www.congress.gov/crs-product/R48592.

Příkazy vydává (formálně schvaluje) Foreign Intelligence Surveillance Court (FISC), což je zvláštní federální soud zřízený zákonem Foreign Intelligence Surveillance Act (FISA), též známý jako „FISA Court". Jeho soudci jsou federální soudci jmenovaní předsedou Nejvyššího soudu USA. Na základě roční certifikace programu pak Attorney General (generální prokurátor) a Director of National Intelligence (DNI) vydávají příkazy konkrétním U.S. poskytovatelům elektronických služeb, viz https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

V případě FISA je odvolání možné k instanci Foreign Intelligence Surveillance Court of Review (FISCR), rozhodnutí jsou neveřejná, a šance na úplné odmítnutí příkazu je velmi nízká. Velcí poskytovatelé cloudu (Microsoft, AWS) proto spíše interpretují rozsah příkazu velmi úzce, poskytují minimum dat a spoléhají se na end-to-end encryption zákaznických dat (tedy že nemohou předat dešifrovaná zákaznická data), využití customer-managed keys a celkově architekturu „no access by provider".

Dalším způsobem, jak žádat o data zákazníků cloudových služeb, jsou **National Security Letters** (NSL). Microsoft uvádí ve svých Q+A:

Dopisy o národní bezpečnosti (NSL) mohou vyžadovat zveřejnění základních údajů o předplatiteli, jako je jméno, adresa a délka předplatného zákazníka, který si předplatil některou z našich služeb. NSL, kodifikované podle 18 U.S. Code § 2709, nesmí být použity k požadavku na zpřístupnění obsahu komunikace nebo obsahu dat zákazníka. NSL lze použít pouze k žádosti o poskytnutí základních informací o zákaznících, které jsou relevantní pro národní bezpečnost USA, a nelze je použít pro trestní, civilní nebo správní vyšetřování. Vláda USA je povinna dvakrát ročně podávat Kongresu zprávu o tom, jak NSL používá, a Ministerstvo spravedlnosti provádí audit používání NSL FBI, aby zajistilo dodržování zákona.

2. Požadavky na poskytovatele a OVS dle současné regulace v ČR

Využívání cloud computingu orgány veřejné správy (dále jen „OVS") je v zák. č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „ZoISVS") a jeho prováděcích vyhláškách upraveno s přístupem založeným na riziku, s ohledem na zařazení informačních systémů veřejné správy (dále jen „ISVS") do bezpečnostních úrovní „nízká (1)" až „kritická (4)". Toto zařazení ISVS se odvozuje od analýzy možných dopadů ztráty důvěrnosti, integrity a dostupnosti služby nebo zpracovávaných dat.

- Pro cloudové služby zapisované do bezpečnostní úrovně (dále jen „BÚ“) „kritická (4)“ je v ZoISVS stanoven požadavek využití poskytovatele státního cloud computingu, který je mimo přímý vliv extrateritoriálních požadavků na vydání zákaznických dat.
- Služby zapisované do BÚ „vysoká (3)“ nebo nižší mohou dle ZoISVS nabízet komerční poskytovatelé po prokázání určitých kritérií způsobilosti, přičemž služby zapsané v BÚ 3, ukládající zákaznická data v prostředí cloudové služby, musí umožňovat použití vlastních šifrovacích klíčů pod správou OVS. Toto opatření fakticky znemožňuje zpřístupnění zákaznických dat poskytovatelem v dešifrované podobě, jak je uvedeno v předchozí kapitole.
- Poskytovatelé musí dle vyhl. č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „VoBK“) a vyhl. č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu (dále jen „VoBP“), pro služby ve všech BÚ dodržovat stanovené postupy, chránící OVS před neoprávněným nebo nadbytečným zpřístupněním jejich dat a specifických provozních údajů, a dále pro BÚ 3 musí poskytovatel navíc vyvinout veškeré možné zákonné úsilí, aby zabránil zpřístupnění informací OVS cizozemskému orgánu bez souhlasu daného OVS.
- Další bezpečnostní kritéria požadovaná dle VoBK uplatňují principy transparentnosti a povinnosti předání podkladů, které slouží úřadům pro jejich posouzení rizik, plynoucích z možného zpřístupnění zákaznických dat třetím státům. Jedná se zejména o tato kritéria:
    - výčet států, kde dochází k trvalému ukládání nebo i dočasnému zpracování zákaznických dat a specifických provozních údajů, zda jsou tyto informace přenášeny mimo oblast EU/ESVO[8] v otevřené, pseudonymizované nebo šifrované formě,
    - výčet států, z jejichž území dochází k výkonu správy a dohledu nad cloudovými službami,
    - v případě, že dochází k ukládání nebo zpracování informací OVS mimo oblast EU/ESVO, doložit rozsah těchto informací, předpokládanou dobu trvání, účel a místo takových zpracování,

  přičemž tyto informace (vlastnosti zapsaných služeb) jsou v souladu se ZoISVS publikovány v katalogu cloud computingu veřejné správy. Kromě toho jsou služby zapsané v BÚ 3, které z nějakých důvodů vyžadují dlouhodobé uložení informací OVS mimo oblast EU/ESVO, uvedeny v katalogu cloud computingu a na úřední desce NÚKIB[9] v seznamu výjimek.

- OVS pak musí dle VoBP, posoudit rizika zpřístupnění dat cizozemským orgánům podle deklarovaných míst zpracování a smí využívat pouze takové služby cloud computingu, u kterých vyhodnotil rizika pro bezpečnost informací jako přijatelná.

Z výše uvedeného vyplývá, že současná úprava ZoISVS a jeho vyhlášek vytváří ucelený rámec pro právní ukotvení tzv. „eGovernment cloudu (eGC)“ s přístupem založeným na riziku a s adekvátním odstupňováním bezpečnostních požadavků pro využívání služeb poskytovatele státního cloud computingu vs. komerčních poskytovatelů, které vychází z hodnocení dopadů a zařazení ISVS a cloudových služeb do bezpečnostních úrovní „nízká (1)“ až „kritická (4)“.

[8] Evropské sdružení volného obchodu (ESVO)
[9] https://nukib.gov.cz/cs/uredni-deska/cloud-computing/

3. Microsoft Corporation

Microsoft shrnuje svůj přístup k ochraně zákaznických dat a vyřizování požadavků orgánů veřejné moci ve vyjádření veřejně dostupném na stránce Microsoft Corporate Responsibility[10] (přeloženo z angličtiny).

Microsoft dodržuje stejné principy pro všechny žádosti OVS o poskytnutí zákaznických dat.

- Microsoft přezkoumává všechny právní požadavky, aby zajistil, že žádost je platná a v souladu s platnou a účinnou právní úpravou. K žádosti o jiná než obsahová data je vyžadováno předvolání (subpoena) nebo obdobný procesní nástroj a pro obsahová data je vyžadován soudní příkaz (warrant) nebo jeho obdobný procesní nástroj.
- Microsoft zpřístupňuje zákaznická data pouze tehdy, pokud je k tomu právně povinen.
- Microsoft žádnému OVS neposkytuje přímý ani neomezený přístup k zákaznickým datům.
- Microsoft žádnému OVS neposkytuje své šifrovací klíče ani možnost prolomit své šifrování.

Žádosti o zpřístupnění zákaznických dat nebo metadat o elektronické komunikaci lze obecně rozdělit do několika kategorií:

- Žádosti o spotřebitelská (consumer) data – podle CLOUD Act
- Žádosti o firemní data (včetně data veřejné správy) - podle CLOUD Act
- Žádosti podle FISA Act – ve věci národní bezpečnosti

Microsoft zveřejňuje na zmíněné stránce (Corporate Responsibility[11]) počty žádostí vždy za 6měsíční období. Poslední zveřejněné období je 2. pol. 2025.

Zdaleka nejvíce obdržených žádostí se týká „consumer data“ – nejspíše proto, že v případě těchto uživatelských účtů orgány činné v trestním řízení (dále jen „OČTŘ“) obvykle neznají skutečnou identitu uživatelů (podezřelých) a mají k dispozici jen emailovou adresu. Za 2. pol. 2025 Microsoft uvádí téměř **28.000** žádostí, ale z toho se pouze **190** žádostí týkalo dat „podnikových zákazníků“ (tzv. enterprise customers – v komerční oblasti, v oblasti veřejné správy či v oblasti vzdělávání, kteří zakoupili předplatné některé z jeho cloudových služeb pro více než 50 uživatelů). V případech „podnikových zákazníků“ OČTŘ zná identitu organizace, kterou lze zjistit podle domény v emailových adresách nebo pak pomocí platební metody (bankovní účet platby nebo kreditní karta), a proto se obrací na poskytovatele zejména v případech, kdy se statutární zástupci organizace mohou sami podílet na trestné činnosti, a předáním žádosti na statutární orgán by OČTŘ riskoval smazání dat a zahlazení stop.

K těmto 190 žádostem o data podnikových zákazníků Microsoft dále uvádí:

- V 96 případech (51 %) byly žádosti zamítnuty, staženy, nebyla k dispozici žádná data nebo byly vyšetřovací orgány úspěšně odkázány na zákazníka.
- **V 94 případech (49 %) byl Microsoft povinen vyhovět:**

[10] www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data
[11] www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data

    - V 45 případech jsme museli zpřístupnit obsah zákaznických dat.
        - Z toho 31 případů bylo spojeno s požadavky vyšetřovacích orgánů v USA.
    - Ve 49 případech jsme museli zveřejnit jiná než obsahová data (například základní informace o zákaznících a jejich IP adresy).
- Žádné z těchto zpřístupnění se netýkalo obsahových dat v Microsoft Azure patřících podnikovému zákazníkovi z komerční oblasti, oblasti vzdělávání či veřejné správy.
- Žádné z těchto zpřístupnění se netýkalo dat v Microsoft Dynamics 365.

Zpřístupnění dat přeshraničních firemních zákazníků (se sídlem mimo USA):

- Z těchto 190 žádostí:
    - Microsoft poskytl americkým OČTŘ obsahová data týkající se tří podnikových zákazníků se sídlem mimo USA, jejichž data byla uložena mimo USA.
    - Jeden z těchto tří zákazníků se nacházel v EU/ESVO.

V případě žádostí o vydání dat ze spotřebitelských (consumer) účtů zveřejňuje Microsoft každých 6 měsíců celosvětovou statistiku, kde je pro žádosti z každé země uveden celkový počet žádostí z dané země, dále podíl a počet případů, ve kterých byla poskytnuta obsahová data zákazníka, podíl a počet případů, ve kterých byla poskytnuta jiná než obsahová data (např. metadata o uživateli a jeho komunikaci); dále je zde uveden podíl a počet případů, kdy žádná data nebyla nalezena, a nakonec podíl případů, kdy byla žádost odmítnuta z důvodu nesplnění požadovaných náležitostí[12].

Z tohoto reportu vyplývá, že vyšetřovací orgány v **USA iniciovaly 5 587 žádostí**, dále např. **Německo iniciovalo 4 094 žádostí**, **Francie 1 841 žádostí**, a **Česko 20 žádostí**. V případě českých OČTŘ Microsoft ve 14 případech poskytl jiná než obsahová data, v žádném případě neposkytl obsahová data zákazníka, ve 3 případech nebyla nalezena žádná relevantní data a 3 žádostem nevyhověl pro nesplnění formálních náležitostí.

Screenshot žádostí v oblasti vyšetřování trestných činů (viz report – link výše):

[12] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/Microsoft-LERR-2025-H1

Law Enforcement Requests Report 2025

Requests received for all Microsoft Services from July to December 2025

	Total Requests		Some Customer Data Disclosed				No Customer Data Disclosed			
	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests	Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)	
	#	#	%	#	%	#	%	#	%	#
TOTAL	**27 412**	**63 107**	**5,14%**	**1 410**	**61,30%**	**16 803**	**12,96%**	**3552**	**20,60%**	**5647**
Argentina	154	171	0,00%	-	55,84%	86	16,88%	26	27,27%	42
Australia	774	1 141	1,16%	9	72,61%	562	16,02%	124	10,21%	79
Austria	490	857	0,00%	-	85,31%	418	11,84%	58	2,86%	14
Belgium	408	568	0,00%	-	78,19%	319	15,44%	63	6,37%	26
Brazil	3 110	9 995	13,25%	412	27,20%	846	4,86%	151	54,69%	1 701
Bulgaria	1	1	0,00%	-	100,00%	1	0,00%	-	0,00%	-
Canada	282	405	0,00%	-	62,77%	177	9,57%	27	27,66%	78
Chile	14	33	0,00%	-	28,57%	4	7,14%	1	64,29%	9
China	3	4	0,00%	-	0,00%	-	0,00%	-	100,00%	3
Colombia	36	51	0,00%	-	27,78%	10	11,11%	4	61,11%	22
Costa Rica	16	17	0,00%	-	81,25%	13	12,50%	2	6,25%	1
Croatia	10	11	0,00%	-	80,00%	8	20,00%	2	0,00%	-
Czech Republic	20	29	0,00%	-	70,00%	14	15,00%	3	15,00%	3
Denmark	18	36	0,00%	-	72,22%	13	0,00%	-	27,78%	5
Dominican Republic	3	3	0,00%	-	33,33%	1	33,33%	1	33,33%	1
Ecuador	6	8	0,00%	-	33,33%	2	33,33%	2	33,33%	2
El Salvador	2	2	0,00%	-	0,00%	-	50,00%	1	50,00%	1
Estonia	2	2	0,00%	-	50,00%	1	0,00%	-	50,00%	1
Finland	101	229	0,00%	-	84,16%	85	9,90%	10	5,94%	6
France	1 841	2 675	0,00%	-	59,80%	1 101	19,83%	365	20,37%	375
Germany	4 094	6 868	0,00%	-	58,89%	2 411	10,45%	428	30,65%	1 255
Greece	71	71	0,00%	-	42,25%	30	15,49%	11	42,25%	30
Hungary	39	77	0,00%	-	58,97%	23	12,82%	5	28,21%	11
Iceland	2	-	0,00%	-	0,00%	-	0,00%	-	100,00%	2
India	1 953	3 485	0,00%	-	65,80%	1 285	14,08%	275	20,12%	393
Ireland	139	250	54,68%	76	16,55%	23	6,47%	9	22,30%	31
Israel	9	10	0,00%	-	55,56%	5	0,00%	-	44,44%	4
Italy	277	1 213	0,00%	-	34,30%	95	24,19%	67	41,52%	115

Screenshot žádostí podle FISA Act a pomocí National Security Letters:

U.S. National Security Orders Report

	Reporting Period	Orders seeking disclosure of content	Accounts impacted by orders seeking content	Orders seeking disclosure of only non-content	Accounts impacted by non-content orders
Foreign Intelligence Surveillance Act (FISA) Orders	Jan - June 2021	0 - 499	15,500 - 15,999	0 - 499	0 - 499
	July - Dec 2021	0 - 499	21,000 - 21,499	0 - 499	0 - 499
	Jan - June 2022	0 - 499	21,500 - 21,999	0 - 499	0 - 499
	Jul - Dec 2022	0 - 499	20,500 - 20,999	0 - 499	0 - 499
	Jan - June 2023	0 - 499	24,000 - 24,499	0 - 499	0 - 499
	Jul - Dec 2023	0 - 499	22,000 - 22,499	0 - 499	0 - 499
	Jan - Jun 2024	0 - 499	26,000 - 26,499	0 - 499	0 - 499
	Jul - Dec 2024	0 - 499	26,000 - 26,499	0 - 499	0 - 499
	Jan - Jun 2025	0 - 499	33,500 - 33,999	0 - 499	0 - 499
National Security Letters (NSL)	Jan - June 2021	N/A	N/A	0 - 499	500 - 999
	July - Dec 2021	N/A	N/A	0 - 499	500 - 999
	Jan - June 2022	N/A	N/A	0 - 499	500 - 999
	July - Dec 2022	N/A	N/A	0 - 499	0 - 499
	Jan - June 2023	N/A	N/A	0 - 499	0 - 499
	Jul - Dec 2023	N/A	N/A	0 - 499	0 - 499
	Jan - Jun 2024	N/A	N/A	0 - 499	0 - 499
	Jul - Dec 2024	N/A	N/A	0 - 499	0 - 499
	Jan - Jun 2025	N/A	N/A	0 - 499	0 - 499

Microsoft k tomu uvádí ve svých Q+A[13]:

Proč neuvádíte podrobnější informace o příkazech národní bezpečnosti (FISA orders), například o umístění zákazníka (nebo zákazníků) dotčených požadavky nebo o konkrétních typech či přesném počtu FISA příkazů, které jste obdrželi?

Právní předpisy Spojených států nám neumožňují zveřejňovat podrobnější informace týkající se právních požadavků souvisejících s národní bezpečností, včetně příkazů FISA a NSL. Microsoft s touto úpravou nesouhlasí a je přesvědčen, že vyšší míra transparentnosti je klíčová pro udržení důvěry v právní stát. Microsoft má dlouhou a úspěšnou historii prosazování větší transparentnosti jak u soudů, tak v Kongresu. Jsme odhodláni spolupracovat se zákonodárci na dalším rozšiřování našich možností poskytovat veřejnosti smysluplnější informace.

Co by Microsoft udělal, kdyby obdržel požadavek orgánů USA na vydání dat zahraničního subjektu veřejného sektoru?

Microsoft uplatňuje stejné principy vůči všem požadavkům OVS na vydání dat. Jsme přesvědčeni, že vlády by nikdy neměly stavět globální technologické poskytovatele do středu sběru zpravodajských informací mezi jednotlivými státy. Microsoft by se bránil proti jakémukoli požadavku na zpřístupnění dat zahraničního subjektu veřejného sektoru bez ohledu na to, která vláda by takový požadavek vznesla.

Mají i jiné země než USA podobné pravomoci v oblasti národní bezpečnosti, a jak by Microsoft reagoval, kdyby na jejich základě obdržel vládní požadavek na zpřístupnění dat?

Řada států disponuje zákonnými pravomocemi, které umožňují jejich OVS požadovat od soukromých společností poskytnutí určitých informací v souvislosti s ochranou národní bezpečnosti. Pokud Microsoft takový požadavek obdrží, uplatní stejné principy jako při posouzení jakýchkoli jiných požadavků OVS na zpřístupnění dat. Tyto případy jsou rovněž zahrnuty do této Zprávě o požadavcích OVS na poskytnutí dat (Government Requests Report).

Smluvní záruky, poskytované smluvní entitou Microsoft Ireland Operations Ltd. pro zákazníky v EU:

Smluvní záruky a rozsah služeb jsou popsány zejména v aktuálních **Podmínkách pro produkty Microsoft** (Product and Services Terms)[14].

Viz část **Core Online Services – *Hlavní služby online*** (na které se vztahují všechny smluvní závazky, umístěna cca v polovině webové stránky)[15].

Závazek umístění je uveden v podkapitole ***Umístění pro uchování neaktivních zákaznických dat pro hlavní služby online***.

[13] http://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data#tab-national-security-orders-report
[14] www.microsoft.com/licensing/terms/cs-CZ/product/PrivacyandSecurityTerms/MPSA
[15] https://www.microsoft.com/licensing/terms/cs-CZ/product/PrivacyandSecurityTerms/MPSA#Hlavnísložbyonline

Zde lze nalézt výčet Microsoft „regionů“, ke kterým se vztahuje závazek uchování neaktivních zákaznických dat v určitých hlavních geografických oblastech. Pro Českou republiku je relevantní geografickou oblastí Evropská unie.

Další relevantní sekcí je **EU Data Boundary – *Služby Datové hranice EU***[16], která kromě umístění neaktivních zákaznických dat upravuje také podmínky **zpracování zákaznických dat v rámci EU**. Do režimu EU Data Boundary již byla zahrnuta většina služeb Microsoft Azure (IaaS/PaaS), **s výjimkou služeb označených jako „non-regional“**, jejichž funkcionalita není vázána na konkrétní Azure region. Microsoft současně průběžně rozšiřuje okruh služeb zahrnutých do EU Data Boundary a u některých služeb dříve označovaných jako non-regional předpokládá jejich budoucí zařazení do tohoto režimu. Dostupnost jednotlivých služeb v konkrétních Azure regionech je k dispozici v interaktivním seznamu[17]. V textu jsou uvedeny i určité výjimky z garance místa zpracování v EU, jako např. vzdálený přístup pracovníků technické podpory, pokud je třeba pro řešení technických problémů zákazníka.

Ochrana osobních údajů je upravena v dodatku **Data Protection Addendum**[18], zejména v **Příloze C – Dodatek o dalších ochranných opatřeních**, který obsahuje ustanovení týkající se obrany proti právně závazným požadavkům na zpřístupnění osobních údajů, která byla zmiňována již výše – citace:

1. Obrana proti právně závazným požadavkům na zpřístupnění osobních údajů. V případě, že společnost Microsoft obdrží od jakékoli třetí strany příkaz k nucenému zpřístupnění jakýchkoli osobních údajů zpracovávaných podle tohoto dodatku DPA, společnost Microsoft je povinna:

a. vyvinout veškeré možné úsilí k přesměrování požadavku třetí strany přímo na zákazníka;
b. bezodkladně informovat zákazníka, nezakazují-li to účinné právní předpisy, kterými je žadatel vázán; v případě, že je takové informování zákazníka zakázáno, zavazuje se společnost Microsoft využít veškeré zákonné prostředky k tomu, aby se takový zákaz v daném případě neuplatnil a zákazníkovi tak bylo možno co nejdříve sdělit co nejvíce informací; a
c. využít veškeré zákonné prostředky k obraně proti takovým závazným požadavkům založené na případných právních nedostatcích či vadách vyplývajících z právních předpisů, o které se žadatel opírá, či případném rozporu s příslušnými právními předpisy Evropské unie nebo příslušného členského státu.

Pokud po provedení kroků popsaných v bodech a. až c. výše bude společnost Microsoft nebo některá z jejích afilací stále nucena zpřístupnit osobní údaje, zpřístupní společnost Microsoft pouze minimální množství těchto údajů nezbytné pro splnění příkazu k nucenému zpřístupnění.

Dále je v bodě 2. Přílohy C DPA zakotven závazek k odškodnění subjektů údajů za hmotnou nebo nehmotnou újmu v případě zpřístupnění na příkaz vládního orgánu (za určitých podmínek).

Příloha D – Námitky proti příkazu nebo závazné právní povinnosti, kterými se pozastavují online služby stanovuje nové závazky pro definovaný pojem **„chráněný zákazník ze státní správy“ z EU/EEA**.

1. V případě, že společnost Microsoft bude doručen příkaz nebo se na ni jinak bude vztahovat závazná právní povinnost ze strany jakékoli vlády, agentury, komise nebo kvazivládního orgánu, který vyžaduje, aby společnost Microsoft zcela nebo zčásti pozastavila nebo ukončila poskytování online služeb (mimo

[16] https://www.microsoft.com/licensing/terms/cs-CZ/product/PrivacyandSecurityTerms/MPSA#SlužbyDatovéhraniceEU
[17] https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/table
[18] www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

jiné včetně poskytování služeb Microsoft Azure, služeb Microsoft Dynamics 365 nebo služeb Office 365) chráněnému zákazníkovi ze státní správy, bude společnost Microsoft svým jménem a jménem svých přidružených společností:

a. používat dostupné prostředky k zajištění dobrovolného stažení, odvolání nebo zrušení takového příkazu; a
b. využívat veškeré zákonné prostředky k obraně proti takovým příkazům před soudy v zemi, jejíž vláda vydala takový příkaz, založené na případných právních nedostatcích či vadách vyplývajících z právních předpisů, o které se žadatel opírá, či případném rozporu s příslušnými právními předpisy Evropské unie nebo států uvedených výše.

Společnost Microsoft bude v případě potřeby usilovat o trvalá a předběžná opatření, aby zajistila nepřetržité a nepřerušované poskytování příslušných online služeb až do úplného a konečného soudního rozhodnutí týkajícího se zákonného úsilí o napadení příkazu nebo jiné závazné právní povinnosti uvedené výše.

4. Amazon Web Services Inc. (AWS)

Postoj AWS Corporate Legal / Corporate Affairs k vládním žádostem

AWS uvádí, že žádné vládě neposkytuje přímý ani automatický přístup k datům zákazníků a zákaznický obsah zpřístupňuje pouze na základě platného právního příkazu (valid legal process)[19].

AWS zároveň zdůrazňuje, že CLOUD Act nevytvořil pro vládu USA „neomezený" nebo „automatický" přístup k datům v cloudu a že jde primárně o vyjasnění územní působnosti již existujících nástrojů podle Stored Communications Act (SCA). **Podle AWS platí, že pro zpřístupnění obsahu (content) musí být splněny přísné požadavky**, typicky soudní příkaz (warrant), a AWS odmítá nebo zužuje požadavky, které jsou nepřiměřené (overbroad) nebo právně vadné[20].

AWS od roku 2020 reportuje, že **žádná žádost nevedla ke zpřístupnění obsahu dat podnikových nebo vládních zákazníků uložených mimo území USA americké vládě** (enterprise/government content stored outside the U.S.), viz výše uvedené reference.

V oblasti národní bezpečnosti AWS uvádí, že některé požadavky mohou přicházet formou National Security Letters (NSL) nebo příkazů podle Foreign Intelligence Surveillance Act (FISA), přičemž přesné počty lze zveřejňovat jen v zákonem povolených intervalech (reporting ranges)[21].

Zveřejňování počtů vládních žádostí

AWS publikuje pololetní „Information Request Report", který rozlišuje typy žádostí (subpoena, search warrant, other court orders) a uvádí i oddělenou část pro národní bezpečnost (NSL/FISA) včetně pravidel reportování v početních intervalech.

[19] https://aws.amazon.com/compliance/cloud-act/
[20] https://aws.amazon.com/blogs/security/five-facts-about-how-the-cloud-act-actually-works/
[21] https://d1.awsstatic.com/Security/pdfs/Amazon_AWS_Information_Request_Report_H2_2024.pdf

Report rovněž vysvětluje rozdíl mezi „non-content" informacemi (např. údaje o předplatiteli) a „content" informacemi (obsah zákaznických dat zpracovaných/uložených v AWS) a uvádí, v kolika případech došlo k plné nebo částečné reakci vs. odmítnutí.

Smluvní a technické záruky AWS pro zákazníky v EU

Základní smluvní rámec tvoří AWS Customer Agreement[22] a navazující AWS Service Terms[23] (včetně odkazovaných politik a dokumentace).

Pro zpracování osobních údajů AWS zpřístupňuje AWS GDPR Data Processing Addendum (DPA) [24], který je zahrnut do smluvních podmínek a obsahuje závazky vůči vládním požadavkům (přesměrování žádosti na zákazníka, notifikace zákazníka, zpřístupnění minimálně možných dat).

AWS zdůrazňuje technickou architekturu, která omezuje přístup i na straně poskytovatele – zejména u Nitro System[25], který je navržen bez mechanismu pro „operator access" (bez možnosti přihlášení na hosty, čtení paměti instancí či přístupu k šifrovaným EBS (Elastic Block Store) svazkům).

AWS dále umožňuje zákazníkům používat zákaznicky spravované klíče (customer managed keys) v AWS Key Management Service (KMS), což posiluje kontrolu zákazníka nad životním cyklem a použitím šifrovacích klíčů[26].

AWS na svém GDPR Center zdůrazňuje, že zákazníci mají kontrolu nad tím, kde budou jejich data uložena (volba regionu) a mají k dispozici šifrování „in transit" i „at rest" včetně možnosti správy vlastních klíčů[27].

5. Oracle Corporation

Postoj Oracle Corporate Legal / Corporate Affairs k vládním žádostem

Oracle ve svém dokumentu US CLOUD Act FAQ uvádí, že CLOUD Act nezměnil způsob, jakým Oracle reaguje na žádosti orgánů činných v trestním řízení, a že zákazníci volí region uložení a spravují obsah dat ve svých cloudových tenantech[28]. Pokud se používá termín **Oracle Cloud Infrastructure (OCI)**, jedná se o divizi Oracle Corp (není to samostatná dceřiná společnost), avšak s oddělenou infrastrukturou pro poskytování cloudových služeb vůči zbytku společnosti Oracle.

Oracle dále popisuje interní proces, kdy jsou **veškeré žádosti o zpřístupnění dat povinně předávány příslušným právníkům** a Oracle je **vyhodnocuje případ od případu z hlediska závaznosti a platnosti dle aplikovatelného práva**. Zákazníci mají přímý přístup ke svým datům v cloudovém tenantu, a proto je podle Oracle zákazník zpravidla v lepší pozici reagovat na právní požadavek; pokud však Oracle obdrží žádost přímo, zavazuje se (pokud to právo umožní) zákazníka promptně informovat a napadat

[22] https://aws.amazon.com/agreement/
[23] https://aws.amazon.com/service-terms/
[24] https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf
[25] https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/no-aws-operator-access.html
[26] https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html
[27] https://aws.amazon.com/compliance/gdpr-center/
[28] https://www.oracle.com/contracts/docs/us_cloud_act_faq.pdf

nezávazné nebo neplatné požadavky[29]. Oracle zde výslovně uvádí, že některé právní režimy (včetně U.S. CLOUD Act) poskytují poskytovatelům více možností, jak požadavky napadat, a že Oracle poskytne pouze minimální množství informací na základě rozumné interpretace požadavku.

Zveřejňování počtů vládních žádostí

Oracle publikuje pololetní „Law Enforcement Requests Report", který shrnuje typy požadavků a agregované statistiky za konkrétní reportované období[30].

V reportu Oracle uvádí členění žádostí (např. administrative subpoenas, grand jury subpoenas, preservation requests, search warrants) a přehled, v kolika případech poskytl plnou/částečnou odpověď vs. odmítl reagovat nebo vyhodnocoval další postup[31].

Smluvní a technické záruky Oracle pro zákazníky v EU

Oracle publikuje smluvní dokumenty pro cloudové služby na portálu Oracle Contracts; typicky jde o Oracle Cloud Services Agreement (CSA) a navazující dokumenty a specifikace služeb[32].

Pro zpracování osobních údajů Oracle poskytuje Data Processing Agreement for Oracle Services (DPA), který je výslovně aplikovatelný na zpracování osobních údajů a stanoví role a povinnosti (Oracle jako zpracovatel osobních údajů) a obecné účely zpracování v rámci poskytovaných služeb[33].

Oracle zároveň v dokumentu Legal Access Requests odkazuje na to, že **konkrétní závazky ochrany zákazníků** (safeguards) při právních požadavcích jsou ukotveny v DPA (a dále v Binding Corporate Rules dle GDPR).

Oracle uvádí k Oracle Cloud Infrastructure (OCI), že Key Management Service podporuje možnosti BYOK (import vlastních klíčů) i HYOK (externí správa klíčů zákazníkem mimo OCI), a to pro posílení požadavků na bezpečnost a compliance[34].

Oracle popisuje, že u External Key Management Service jsou klíče vytvářeny a spravovány v externím key management systému mimo OCI; klíčový materiál není do OCI importován a OCI pracuje pouze s referencemi, přičemž kryptografické operace probíhají přes integraci s externím systémem[35].

Na produktové úrovni Oracle prezentuje OCI Vault / Key Management jako zákaznicky spravované šifrování, které umožňuje zákazníkovi udržet kontrolu nad šifrovacími klíči v HSM (včetně variant single-tenant/dedicated a external KMS)[36].

[29] https://www.oracle.com/a/ocom/docs/oracle-legal-access-requests.pdf
[30] https://www.oracle.com/legal/law-enforcement-requests-report/
[31] https://www.oracle.com/a/ocom/docs/law-enforcement-requests-sept-2024.pdf
[32] https://www.oracle.com/contracts/cloud-services/
[33] https://www.oracle.com/contracts/docs/data-processing-agreement-oracle-services-081425.pdf
[34] https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm
[35] https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Tasks/external_key_management.htm
[36] https://www.oracle.com/security/cloud-security/key-management/

Oracle v souvislosti s pojmem „data sovereignty“ a přístupovými žádostmi uvádí, že součástí jeho přístupu je důkladné právní posouzení žádostí, transparentní reporting a schopnost napadat neplatné nebo nevymahatelné požadavky, a to i v případě Oracle EU Sovereign Cloud[37].

6. Google LLC (USA)

Postoj Google Legal / Corporate Affairs k vládním žádostem

Google Cloud zastává zásadní postoj: zákazníci vlastní svá data a mají plnou kontrolu nad přístupem k nim. Google velmi vážně dbá na bezpečnost a soukromí svých zákazníků a vyvinul transparentní proces pro zpracování jakýchkoliv vládních žádostí o informace, který odpovídá mezinárodním osvědčeným postupům.

Veškeré informace níže vychází z oficiálního dokumentu **Government Requests for Cloud Customer Data**[38]. Verze na webu (únor 2022) je zdrojovou informací pro tento článek k datu 24.7.2026.

Pokud Google obdrží požadavek od vládního úřadu nebo soudu (včetně požadavků na základě U.S. CLOUD Act nebo FISA), postupuje systematicky podle pevně stanoveného čtyřkrokového procesu:

1. Přesměrování
2. Přezkum validity
3. Upozornění
4. Právní odpor

Přesměrování na zákazníka (Redirection): Pokud Google obdrží žádost vládního orgánu o přístup k zákaznickým datům v cloudu, informuje tento orgán, že musí požadavek uplatnit **přímo u dotčeného zákazníka** (organizace). Tento postup je plně v souladu s oficiální politikou vlády USA i se smluvními závazky Google Cloud.

Důsledný přezkum právní validity (Evaluation of Legal Validity): Pokud vládní orgán přesto nutí Google na žádost odpovědět, specializovaný a vyškolený tým právníků Google Cloud pečlivě přezkoumá, zda je požadavek legální, přiměřený a splňuje veškeré formální i věcné náležitosti. Google se aktivně staví proti (odmítá, omezuje nebo upravuje) jakýmkoliv požadavkům, které vyhodnotí jako příliš široké, nepřiměřené, neslučitelné s platnými zákony nebo jinak nezákonné.

Upozornění zákazníka a transparentnost (Customer Notice): Google **předem upozorní zákazníka** na to, že jeho data mají být zpřístupněna, aby zákazník mohl uplatnit vlastní právní ochranu. Výjimkou jsou pouze situace, kdy je toto upozornění výslovně zakázáno zákonem (např. soudní příkaz k mlčenlivosti), mohlo by mařit vyšetřování, nebo v případě bezprostředního ohrožení

[37] https://blogs.oracle.com/cloud-infrastructure/oracle-sovereign-cloud-solutions-data-access
[38] https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf

života či vážné újmy na zdraví. V případě, že je upozornění dočasně zakázáno, je politikou Google informovat zákazníka okamžitě poté, co tento zákaz pomine (např. po vypršení platnosti soudního příkazu k mlčenlivosti).

Podpora zákazníka při právním odporu (Customer Challenges): Google v maximální míře povolené zákonem spolupracuje se zákazníkem na jeho obraně proti vládnímu požadavku. Pokud zákazník podá formální odpor u příslušného soudu a poskytne Google kopii tohoto odporu, Google **data nevydá a podrží je v úschově (escrow)** po celou dobu trvání soudního řízení, je-li to právně přípustné.

Zveřejňování počtů vládních žádostí

Google se dlouhodobě hlásí k naprosté otevřenosti a jako první cloudový poskytovatel na světě začal pravidelně zveřejňovat statistiky o vládních žádostech. Tento přehled slouží jako veřejný a nezávisle ověřitelný registr. Všechny historické i aktuální statistiky jsou veřejně dostupné na oficiálním portálu:

- **Hlavní rozcestník:** Google Transparency Report[39]
- **Specifická sekce pro firemní zákazníky:** Zpráva o požadavcích na firemní cloud (Enterprise Cloud requests)[40]

Jak zpráva funguje a co obsahuje:

- **Pololetní aktualizace:** Data jsou kompletně aktualizované každých šest měsíců za uplynulé období.
- **Jasná definice podnikového (Enterprise) zákazníka:** Zpráva striktně odděluje běžné spotřebitelské účty od firemních a vládních subjektů. Pod pojmem *Enterprise Cloud Customer* se ve statistikách rozumí:
  - Účty Google Cloud Platform (GCP) fakturované na základě offline fakturace.
  - Domény Google Workspace (včetně Workspace for Education) s placenými službami a více než 50 licencemi (seats).
- **Co z historických statistik vyplývá:**
  - Počet požadavků cílících na firemní cloudové zákazníky představuje **naprosté minimum** (zpravidla pod **0,4 %** ze všech obdržených žádostí celosvětově - H12025).
  - Statistiky prokazují, že pro zákazníky služby **Google Cloud Platform (GCP) nebyla v řadě reportovaných období vydána vůbec žádná data** v reakci na vládní požadavky.
  - Žádosti týkající se národní bezpečnosti USA (podle FISA a NSL) jsou rovněž vykazovány samostatně v mezích stanovených zákonem (v povolených početních intervalech).

Smluvní a technické záruky pro zákazníky v EU

Smluvní záruky: Google Cloud poskytuje robustní smluvní záruky (v rámci *Data Processing Addendum – DPA* a standardních smluvních doložek), které chrání zákazníky z EU před nezákonnými vládními zásahy:

[39] https://transparencyreport.google.com/
[40] https://transparencyreport.google.com/user-data/enterprise

- **Závazek k právní obraně:** Google se smluvně zavazuje využít veškeré dostupné zákonné prostředky k napadení jakéhokoli vládního požadavku na přístup k datům, pokud existuje rozpor s právem EU nebo členského státu.
- **Minimalizace poskytovaných dat:** Pokud je po vyčerpání všech právních prostředků Google přesto nucen data vydat, poskytne vždy pouze **naprosté minimum informací** nezbytné pro splnění daného právního příkazu.
- **Závazek lokalizace dat (Data Residency):** Google Cloud umožňuje zákazníkům zvolit si konkrétní region pro ukládání dat (data at rest) výhradně v rámci EU.

Technické záruky: Google Cloud staví na principu, že nejlepší ochranou před vládními požadavkami jsou **vyspělé kryptografické a přístupové mechanismy**, které technicky znemožňují poskytovateli (Google) číst zákaznická data bez explicitního souhlasu:

- **Šifrování jako standard:** Všechna zákaznická data jsou ve výchozím nastavení šifrována jak při přenosu (in transit), tak při uložení (at rest).
- **Externí správa klíčů (Cloud EKM & BYOK/HYOK):** Zákazníci mohou spravovat své šifrovací klíče zcela mimo infrastrukturu Google Cloud (např. ve svém vlastním on-premise prostředí nebo u nezávislého partnera).
- **Key Access Justifications (KAJ):** Tato unikátní technologie poskytuje zákazníkovi podrobné zdůvodnění pokaždé, když je vyžadován šifrovací klíč pro dešifrování dat (včetně případných požadavků ze strany inženýrů Google nebo vládních nařízení). Zákazník může na základě KAJ **aktivně zamítnout dešifrování dat**, což znamená, že Google fyzicky nemůže data v dešifrované podobě vládnímu orgánu poskytnout.
- **Access Approval (Schvalování přístupu):** Umožňuje zákazníkům explicitně schvalovat či zamítat jakýkoliv administrativní přístup personálu Google k jejich datům či konfiguracím. Každý takový pokus je navíc transparentně logován (*Access Transparency*).
- **Assured Workloads:** Nástroj umožňující automaticky vynutit a kontrolovat dodržování přísných bezpečnostních politik, jako je geografické omezení zpracování dat v EU a omezení personální správy pouze na občany EU.

7. Strategie a nabídky globálních poskytovatelů pro posílení suverenity dat až po izolované implementace v prostředí zákazníka nebo státního cloudu

Poskytovatel	Strategie pro EU Sovereign Cloud	Možnost provozu v izolovaném privátním / státním cloudu
Microsoft	Microsoft nabízí **Microsoft Sovereign Cloud** jako kombinaci Sovereign Public Cloud, Sovereign Private Cloud a National Partner Clouds, která má zajistit evropskou kontrolu nad daty, přístupy a AI službami při zachování plné funkcionality Azure a Microsoft 365. [microsoft.com], [blogs.microsoft.com]	Microsoft současně umožňuje provoz části cloudových služeb v izolovaném prostředí prostřednictvím **Azure Local (dříve Azure Stack HCI)** a souvisejících technologií, které jsou základem i pro nabídku Sovereign Private Cloud. [microsoft.com], [blogs.microsoft.com]
AWS	AWS buduje **AWS European Sovereign Cloud** jako samostatný cloud provozovaný výhradně v EU evropskými entitami a evropským personálem bez provozních závislostí mimo EU. [aws.eu], [aws.amazon.com]	AWS nabízí on-prem varianty zejména prostřednictvím **AWS Outposts**, případně Dedicated Local Zones, které umožňují provoz vybraných AWS služeb v datacentrech zákazníka nebo národního operátora, avšak jejich integrace s AWS cloudem je obecně těsnější než u plně izolovaných řešení. [aws.amazon.com], [aws.eu]
Oracle	Oracle prezentuje **EU Sovereign Cloud** jako plnohodnotný OCI cloud provozovaný samostatnými právními entitami v EU, se samostatnou správou, podporou a kontrolou přístupu omezenou na EU. [oracle.eu], [docs.oracle.com]	Oracle umožňuje nasazení cloudových služeb do prostředí zákazníka prostřednictvím **OCI Dedicated Region** a dalších variant OCI nasazených v zákaznickém datacentru, což je vhodné i pro státní nebo národně provozované cloudy. [oracle.eu], [docs.oracle.com]
Google	Google uvádí **Google Sovereign Cloud** založený na kombinaci suverénních kontrol, regionálních operátorů (např. Thales/S3NS či T-Systems) a různých úrovní provozní nezávislosti podle požadavků zákazníka. [cloud.google.com], [cloud.google.com]	Google nabízí provoz vybraných cloudových a AI služeb mimo veřejný cloud prostřednictvím **Google Distributed Cloud**, a to jak v připojeném, tak plně air-gapped režimu určeném pro obranu a kritickou infrastrukturu. [cloud.google.com]

Pro případné využití výše uvedených nabídek je třeba vyhodnotit, zda podléhají definici a rozsahu regulace cloud computingu dle ZoISVS, a pokud ano, zda jsou v rozsahu již zapsaných nabídek v katalogu cloud computingu veřejné správy v ČR.