Microsoft

11. srpna 2022

Prohlášení společnosti Microsoft Německo o dodržování ochrany osobních údajů v rámci Microsoft 365 a Microsoft Teams

Vyjádření orgánů veřejné moci, zejména některých orgánů pro ochranu osobních údajů, po určitou dobu možná vyvolávala dojem, že Microsoft 365 a Microsoft Teams pro podniky a veřejný sektor (zejména školství) nelze používat v souladu s ochranou osobních údajů nebo že samy o sobě nejsou v souladu s ochranou osobních údajů. Taková tvrzení nejsou správná, jak bychom rádi vysvětlili níže:

SPRÁVNĚ JE:	
1	Společnost Microsoft nabízí **perspektivní technologie se špičkovými standardy zabezpečení,** na které **se** Německo **může spolehnout** i v době krize. Naše technologie **posilují Německo**. Pouze důsledná digitalizace s využitím nejmodernějších technologií umožní Německu udržet si **prosperitu,** hájit své **hodnoty a** úspěšně plnit své společenské povinnosti (jako např. **vzdělávací mise**).
2	Společnost Microsoft je **důvěryhodným a zodpovědným partnerem**. [1] Naším **firemním cílem** je umožnit každému člověku a každé organizaci dosáhnout více. Naším **obchodním modelem** je **přispívat k úspěchu našich zákazníků** prostřednictvím produktivních technologií. **zákazníky**.
3	Všechny produkty a služby společnosti Microsoft lze používat v soukromém i veřejném sektoru (např. ve školách) **způsobem, který je v souladu s ochranou osobních údajů,** a **samy** jsou také **v souladu s ochranou osobních údajů**. Společnost Microsoft dodržuje požadavky platných zákonů o ochraně osobních údajů.
4	Společnost Microsoft poskytuje zákazníkům **smluvní záruky a technické prostředky pro** používání produktů a služeb společnosti Microsoft v souladu s ochranou osobních údajů, mimo jiné: ➢ smluvní závazky společnosti Microsoft: ➢ Údaje o zákaznících se nepoužívají k cizím účelům, například k reklamě; ➢ přijímá právní ochranná opatření proti nezákonným žádostem o předání ze strany orgánů nebo třetích stran; [2.] ➢ Případné třetí strany mají přístup k údajům klienta pouze v rozsahu stanoveném ve smlouvě; ➢ nezveřejňuje klíče platformy používané k šifrování údajů zákazníků a neumožňuje třetím stranám překonat šifrování; a ➢ nemá důvod se domnívat, že mu platné právní předpisy brání v plnění jeho povinností podle standardních smluvních doložek; a ➢ Možnosti technické ochrany údajů (např. šifrování, pseudonymizace, diferencovaná přístupová oprávnění a automatizace procesů důležitých pro bezpečnost) podle současného stavu techniky.
5	Společnost Microsoft již nyní ukládá data převážně regionálně v **datových centrech v EU**. Kromě toho - ačkoli k tomu neexistuje žádná zákonná povinnost - umožní **hranice EU pro údaje** společnosti Microsoft v budoucnu zákazníkům z veřejného sektoru se sídlem v EU a Umožnit firemním zákazníkům **zpracovávat a ukládat jejich údaje v rámci EU**. [3] [4]
6	**Společnost Microsoft je lídrem v oblasti kybernetické bezpečnosti** a zavedla řadu technických opatření na **ochranu dat zákazníků před kybernetickými útoky**. Patří mezi ně technologie pro odhalování a maření útoků a neoprávněného přístupu k datům. Společnost Microsoft bude v letech 2021 až 2025 investovat **20 miliard dolarů do kybernetické bezpečnosti.** **Investujte do kybernetické bezpečnosti**. [5]

[1] https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/08/RPC-Framework-2.pdf
[2] https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/
[3] https://news.microsoft.com/de-de/unsere-antwort-an-europa-microsoft-ermoeglicht-speicherung-und-verarbeitung-von-daten-

výhradně v-eu/
[4] https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/
[5] https://cloudblogs.microsoft.com/industry-blog/microsoft-in-business/security/2021/09/23/microsoft-expands-on-cybersecurity-závazky-pro-ú-vládní-agentury/

7	Společnost Microsoft podstupuje nejméně jednou ročně **audit mezinárodně uznávanými nezávislými auditory**. Na základě **normy ISO/IEC 27001** tito auditoři kontrolují, zda společnost Microsoft zajišťuje zásady a postupy pro zabezpečení, ochranu dat, kontinuitu a shodu s předpisy. Společnost Microsoft rovněž splňuje požadavky **katalogu požadavků na cloud computing (C5)**6 vydaného společností BSI a je držitelem řady dalších příslušných certifikátů a osvědčení, například **normy ISO/IEC 27018** pro **ochranu dat v cloudu** a **normy ISO/IEC 27701 pro ochranu dat v cloudu.** **Řízení rizik**. [7] [8]
NÁSLEDUJÍCÍ TVRZENÍ JSOU NESPRÁVNÁ:	
1	***"Cloud je nezabezpečený."***
	Správné je spíše: ➢ Použití cloudu vede ke **zvýšení bezpečnosti a dostupnosti dat ve** srovnání s lokálními řešeními. Současná válka na Ukrajině ukazuje, že země s cloudovou strategií jsou **kybernetickými útoky zasaženy méně.** [9] ➢ Předpisy o technologické ochraně údajů (např. čl. 32 GDPR) vyžadují, aby se ochrana neustále přizpůsobovala technickým podmínkám a aby se další vývoj. Cloudová řešení průběžně odrážejí **aktuální požadavky na zabezpečení.**
2	***"Vláda USA čte všechno."***
	Správné je spíše: ➢ Zájem amerických orgánů například o **údaje ze školní výuky v** Německu **nelze myslet vážně.** ➢ Dokazuje to rozsáhlá analýza veřejně dostupných dokumentů amerických vládních agentur o používání **§ 702 zákona o dohledu nad zahraničním zpravodajstvím (FISA) v praxi[10] :** ➢ **Neexistují žádné důkazy o tom,** že by vláda USA využívala § 702 zákona FISA k tomu, aby (i) provádět průmyslovou špionáž nebo sledovat hospodářské zájmy USA nebo ii) zaměřovat se na vlády v Evropském hospodářském prostoru a ➢ Vláda USA používá § 702 zákona FISA v podstatě ke shromažďování informací pro vyšetřování **závažných hrozeb pro národní bezpečnost,** jako je terorismus, kybernetické útoky a šíření zbraní. ➢ Společnost Microsoft **několikrát úspěšně zažalovala vládu USA, aby** ochránila práva svých zákazníků na ochranu soukromí. [11] Společnost Microsoft se i nadále zasazuje o ochranu dat zákazníků. [12] ➢ Z "Transparency Reporting" společnosti Microsoft vyplývá, že jen ve **velmi málo případech** byla data společnosti umístěná mimo USA nucena být předána americkým orgánům činným v trestním řízení. [13] ➢ Plošné doporučení jednotlivých orgánů využívat pouze poskytovatele z EU také nebere v úvahu, že poskytovatelé se sídlem v EU mohou rovněž podléhat americkým zákonům o dohledu, např. kvůli přítomnosti v USA nebo minimálnímu kontaktu s nimi. Orgány nesmí uplatňovat **dvojí metr** a podléhají **zásadě objektivity**.
3	***"Předávání údajů do třetích zemí, například do USA, není povoleno."***

[6] https://docs.microsoft.com/de-de/compliance/regulatory/offering-c5-germany
[7] https://news.microsoft.com/de-de/im-daten-dschungel-zertifizierungen-der-microsoft-cloud/
[8] https://docs.microsoft.com/de-de/compliance/regulatory/offering-home
[9] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
[10] https://www.microsoft.com/en-us/trust-center/privacy (klikněte na "Zjistěte více o dodržování požadavků EU na přenos").
[11] 2014: https://blogs.microsoft.com/on-the-issues/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data/#sm.00059ylyl10cvctusyt1n87pf9egh; a https://blogs.microsoft.com/on-the-issues/2014/05/22/new-success-in-protecting-customer-rights-unsealed-today; 2016: https://blogs.microsoft.com/eupolicy/2016/09/05/our-search-warrant-case-microsofts-commitment-to-protecting-your-privacy; 2017: https://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn
[12] https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/
[13] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report a https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report.

	Správné je spíše: ➢ **GDPR povoluje předávání údajů do třetích zemí, včetně USA,** za použití vhodných ochranných opatření (např. standardních smluvních doložek 2021/914 a dalších opatření). ➢ Je třeba provést analýzu rizik ve světle judikatury ESD ve věci Schrems II a v případě potřeby zavést dodatečná opatření. ➢ Společnost Microsoft nabízí **další, právně uznávané mechanismy ochrany pro** předávání údajů do třetích zemí, například dodatečné smluvní doložky. ➢ V souvislosti s mezinárodním předáváním údajů není ze zákona nutné vyloučit všechna teoretická zbytková rizika, jako je například regulační přístup ve třetí zemi. [14] Požadavek na **"přístup s nulovým rizikem"** je **nepřiměřený** a není v souladu ani s GDPR, ani s úpravou standardních smluvních doložek15 , judikaturou Schrems II a doporučeními Výboru pro Evropský sbor pro ochranu osobních údajů pro opatření týkající se předávání údajů do třetích zemí16.
4	***"Diagnostické údaje jsou zbytečné a škodlivé."***
	Správné je spíše: ➢ **Diagnostické údaje jsou nezbytné pro bezpečný a stabilní provoz produktů a služeb**. Naši zákazníci oprávněně očekávají, že budou moci používat naše výrobky a služby bezpečně a v souladu se smlouvou. K tomu přispívá i zodpovědné využívání diagnostických údajů. ➢ Zákazníci používají mnoho různých technických infrastruktur. Zpracování diagnostických údajů je proto velmi užitečné pro **snížení náchylnosti k chybám a pravděpodobnosti bezpečnostních rizik**. ➢ Diagnostické údaje jsou často nesprávně chápány a **zaměňovány s funkčními údaji**, z. např. proto, že příslušné (nesprávné) klasifikace neberou v úvahu skutečnost, že pro smluvně sjednanou, a tedy i zákazníkem oprávněně očekávanou stabilitu a bezpečnost příslušné aplikace (a tedy pro její řádné fungování) je nutné určité musí být shromážděny údaje, aby bylo možné provést požadovanou akci uživatele.
5	***"Společnost Microsoft monitoruje uživatele svých produktů a služeb."***
	Správné je spíše: ➢ Technické spojení mezi uživateli a společností Microsoft (např. prostřednictvím serverů a datových center) je v mnoha případech **povinným předpokladem pro smluvně zavázané poskytování služeb.** Nic z toho nelze považovat za špehování zákazníků. ➢ Cloudové služby fungují pouze tehdy, pokud jsou přenášeny akce uživatele, aby mohla být provedena příslušná reakce aplikace (např. překlad). **Na stránkách** **je technicky srovnatelný se zpracováním v lokálních řešeních.**
6	***"Službu může používat pouze ten, kdo plně rozumí jejímu technickému fungování."***

[14] Srov. Stefan Brink a další: "Na druhou stranu ESD zachází příliš daleko, když například považuje za vražedné kritérium pro globální výměnu údajů pouze abstraktní a hypotetickou možnost přístupu mimoevropských bezpečnostních orgánů bez konkrétního a reálného rizika pro osobní údaje Evropanů." (https://www.faz.net/aktuell/wirtschaft/digitec/so-war-die- dsgvo-ne-obecne-co-se-stane-kdyz-je-pouzijete-18179521.html; zveřejněno 18.07.2022)
[15] Viz také zejména poznámka pod čarou č. 12 Standardních smluvních doložek EU 2021/914.
[16] Viz doporučení 01/2020 Evropského sboru pro ochranu osobních údajů o opatřeních, která doplňují Nástroje pro předávání k zajištění úrovně ochrany osobních údajů podle práva Unie, bod 47.

	Správné je spíše: ➢ Analýza každého jednotlivého zpracování služby správcem/uživatelem **není podle zákona o ochraně osobních údajů nutná ani vyžadovaná** a jde daleko nad rámec povinností odpovědnosti podle čl. 5 odst. 2 GDPR. Rozhodujícím faktorem je, že správce má k dispozici informace nezbytné pro splnění svých povinností týkajících se odpovědnosti. ➢ Postavení takové překážky by znamenalo konec mnoha technologií hyperškálování v prostředí cloudu, které mají přirozenou mezeru ve znalostech mezi poskytovatelem technologie a uživatelem. Požadovat to by bylo **nerealistické a protitechnologické.** Odpovídající požadavky lze jen stěží splnit v jakékoli oblasti života, která je významně ovlivněna technologií. ➢ Uznává se, že čistě **technické provedení** může být do určité míry určeno samotným zpracovatelem. [17]

[17] Viz např. Evropský sbor pro ochranu osobních údajů ve svých "Pokynech 07/2020 k pojmům správce a zpracovatel v GDPR", bod 40: "*Základní prostředky" jsou tradičně a ze své podstaty vyhrazeny správci. Zatímco nepodstatné prostředky může určit i procesor, podstatné prostředky určí řídicí jednotka. [...] "Nepodstatné prostředky" se týkají praktičtějších aspektů implementace, jako je volba konkrétního typu hardwaru nebo softwaru nebo podrobných bezpečnostních opatření, jejichž výběr může být ponechán na zpracovateli.* ").