CVP-P-06 Provozní řád informačního systému

Bezpečnostní standard

Název	**Whitelist / Blacklist AI technologií**

Tento bezpečnostní standard je vydáván v souladu s čl. VII centrálního vnitřního předpisu CVP-P-14 Informační bezpečnost AI technologií. Technologie níže neuvedené musí být před jejich použitím posouzeny dle čl. VIII výše uvedeného předpisu. Schválený rozsah může být rozšířen do vyšší kategorie pouze po schválení konkrétního projektu manažerem kybernetické bezpečnosti.

Název technologie	Země původu	Prostředí původu	List	Schválený rozsah	Poznámka
Microsoft 365 Copilot – pracovní účet v tenantu	USA	Kooperativní	WhiteList	Rizikový	S výjimkou použití modelů Claude / Anthropic prostřednictvím Copilot (EU data residency)
Microsoft 365 Copilot – mimo pracovní účet v tenantu	USA	Kooperativní	WhiteList	Běžný	
Microsoft Security Copilot	USA	Kooperativní	WhiteList	Rizikový	
Microsoft AI stack	USA	Kooperativní	WhiteList	Běžný	Jednotlivé projekty a komponenty musí být schválené samostatně
Gemini	USA	Kooperativní	WhiteList	Běžný	Nutné nastavení EU Data Residency ve Workspace
ChatGPT	USA	Kooperativní	WhiteList	Běžný	
Canva AI	AU	Kooperativní	WhiteList	Veřejný	Není zajištěné uložení dat v EU a jejich nepřenositelnost
Claude / Anthropic	USA	Kooperativní	WhiteList	Běžný	Pouze provoz přes API, jinak není zajištěno EU Data residency
Codex	USA / IRL	Kooperativní	WhiteList	Běžný	Nutné zapnutí EU Data residency
Consensus	USA	Kooperativní	WhiteList	Veřejný	Neplacená verze nemá EU Data residency
Deep L	DE	Kooperativní	WhiteList	Veřejný	V neplacené verzi nelze vypnout učení
Descript	USA	Kooperativní	Whitelist	Veřejný	Nelze zajistit EU Data Residency
Edge TTS / Azure Speech	USA / EU dle Azure regionu	Kooperativní	WhiteList	Veřejný	
ElevenLab	USA	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
Elicit	USA	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency *Projít DPA

Gamma	USA	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
Genially AI	ES	Kooperativní	WhiteList	Běžný	
Grammarly	USA	Kooperativní	Whitelist	Veřejný	Ve free licenci nelze zajistit EU Data Residency a zákaz tréninku
HeyGen	USA	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
MindMeister	AT / DE	Kooperativní	WhiteList	Běžný	
Napkin AI	USA	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
Narakeet	UK / USA AWS	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
Notebook LM	USA / EU	Kooperativní	WhiteList	Běžný	Nutné nastavení EU Data Residency ve Workspace pro placené licence; free licence pouze veřejný režim
Opus.pro	USA	Kooperativní	WhiteList	Veřejný	Nepodařilo se najít spolehlivá data
Perplexity AI	USA	Kooperativní	WhiteList	Veřejný	U free služby nelze zajistit EU Data Residency
SciSpace	Indie	Neutrální	WhiteList	Veřejný	
Synthesia	UK	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
TurboScribe	USA	Kooperativní	WhiteList	Veřejný	Nelze zajistit EU Data Residency
VEED	UK	Kooperativní	WhiteList	Běžný	Pouze Enterprise platforma zajiš-ťuje EU Data Residency
Llama do verze 3.1 – lokální provoz	USA	Kooperativní	WhiteList	Běžný	
Mistral – lokální provoz	FR	Kooperativní	WhiteList	Běžný	Pouze verze pod Apache 2.0 license. Verze pod modifikovanou MIT licencí je nutné posoudit samostatně.
TinyLlama – lokální provoz	Singapore	Neutrální	WhiteList	Běžný	
Codestral – lokální provoz	FR	Kooperativní	WhiteList	Vědecký	
Gemma 4 – lokální provoz	USA	Kooperativní	WhiteList	Běžný	Pouze verze pod Apache License 2.0.
Whisper – lokální provoz	USA	Kooperativní	WhiteList	Běžný	

Zakázané AI technologie					
*	RU	Nepřátelské	BlackList	-	Yandex, GigaChat, Kandinsky, Alice AI, Cotype, MTS AI, …
*	CHN	Nepřátelské	BlackList	-	DeepSeek, Qwen, ERNIE, Tencent Hunyuan, Doubao, iFLYTEK Spark, SenseNova, Z.ai/ChatGLM, Kimi, MiniMax, …
Globe Explorer			BlackList		Nepodařilo se ověřit spolehlivá data k posouzení
Otter.ai	USA	Kooperativní	BlackList		Není možné EU Data Residency ani vypnutí režimu tréninku na zákaznických datech. Vzhledem k povaze zpracovávaných údajů (přepisy schůzek apod.) se nelze vyhnout PII a tedy je nutné blacklistovat.
Llama 3.2 a vyšší – lokální provoz	USA	Kooperativní	BlackList	-	Licenční omezení: https://www.llama.com/llama3_2/license/ „1.a Grant of Rights. You are granted a non-exclusive, worldwide, non-transferable and royalty-free limited license …“ https://www.llama.com/llama3_2/use-policy/ „…the rights granted under Section 1(a) of the Llama 3.2 Community License Agreement are not being granted to you if you are an individual domiciled in, or a company with a principal place of business in, the European Union.“
Codestral – lokální provoz	FR	Kooperativní	BlackList	Veřejný, Běžný, Rizikový	Licence neumožňuje použití v produkčním prostředí, viz. https://mistral.ai/static/licenses/MNPL-0.1.md
Stav ke dni		8. 6. 2026			