*Verze dokumentu: 3.0*
*Datum vydání: 5.5.2026*
*Autor: IT bezpečnostní tým*
*Schváleno: Miroslav Buček, vedoucí IT bezpečnosti*

# Bezpečnost a soulad s předpisy

Bezpečnost vašich dat je pro nás v Aiviro nejvyšší prioritou. Dodržujeme nejvyšší průmyslové standardy, abychom zajistili důvěrnost vašich dat. Pro Aiviro je zpracování klíčových obchodních dat pro podniky z celého světě denním chlebem. Jsme odhodláni dodržovat nejvyšší standardy zabezpečení, ochrany soukromí v souladu s předpisy při práci s daty zákazníků. K tomu jsme vyvinuli a zavedli komplexní sadu politik, postupů a kontrolních mechanismů, abychom zajistili odpovídající důvěrnost, integritu a dostupnost vašich dat, jak je popsáno níže.

## Oddělení pro bezpečnost, právní záležitosti a dodržování předpisů

Máme specializovaný tým pro bezpečnost, ochranu soukromí a dodržování předpisů, který spravuje naše bezpečnostní a soukromé programy. Navrhují a udržují naše obranné systémy, vyvíjejí procesy pro kontrolu bezpečnosti a neustále monitorují naše sítě, aby odhalili podezřelou aktivitu. Poskytují také odborné poradenství našemu technickému týmu.
Provádíme pravidelné interní audity. Dále Aiviro jmenuje pověřence pro ochranu osobních údajů a zavádí politiky zpracování, uchovávání a likvidace dat v souladu s GDPR. Pokud máte dotazy týkající se naší politiky ochrany soukromí nebo souladu s GDPR, kontaktujte našeho pověřence pro ochranu osobních údajů privacy@aiviro.com.

## Opatření na ochranu dat

Dodržujeme odpovídající technická a organizační opatření, vnitřní kontroly a bezpečnostní rutiny podle osvědčených postupů v průmyslu. Zohledňujeme vývoj technologií, abychom chránili vaše data před náhodnou ztrátou, zničením, změnou, neoprávněným zveřejněním nebo přístupem. Tato opatření zahrnují mimo jiné: zajištění spolehlivosti zaměstnanců s přístupem k vašim datům, omezený přístup, silnou autentizaci, školení personálu, pravidelné zálohování, postupy pro obnovu dat a řízení incidentů, technickou ochranu zařízení, kde jsou data uložena, a další.

## Soulad s předpisy

Aiviro dodržuje průmyslové standardy a pravidelně provádíme kontrolu aplikací, systémů a sítí, čímž zajišťujeme nepřetržitou ochranu vašich dat. Aktuálně se připravujeme na certifikaci ISO 27001.

## Zpracování a přenosy dat

Data shromážděná od vás mohou být přenesena, uložena a zpracována v Evropské unii. Naše podmínky a interní postupy zpracování dat pravidelně aktualizujeme, aby reflektovaly legislativní vývoj a zajistili soulad s nařízením Evropského parlamentu a rady EU 2016/679 GDPR a dalšími relevantními předpisy.

## Ekosystém dodavatelů

Každého dodavatele posuzujeme podle naší politiky řízení dodavatelů. Nové dodavatele přijímáme po důkladném posouzení rizik.

## Umístění datových center

Primárně zpracováváme data na serverech Google Cloud Platform (GCP), kde běží hlavní část naši infrastruktury, které dodržují nejvyšší bezpečnostní standardy a jsou pravidelně auditovány. Zároveň využíváme přídavné služby poskytované AWS nebo Azure podle potřeby a specifikací našich zákazníků. Využíváme vlastní datové zóny, žádná data nejsou dále sdílená, to platí i pro OpenAI GTP modely.
Evropská datová centra:

- Google GCP: europe-central2 (Warsaw, Poland) (certifikace)
- AWS region: eu-central-1 (Evropa – Frankfurt), europe-west1 (certifikace)
- Azure region: West Europe (Evropa – Belgie) (certifikace)

Naše architektura je založená na hybridním modelu. Veškeré datové záznamy a jejich metadata zůstávají u zákazníka, v rámci jeho infrastruktury. Do cloud jsou odesílána pouze nezbytně nutná data, jen na nezbytně nutnou dobu pro zpracování a analýzu v cloudu. Tato data se však v cloudu neukládají, jsou pouze zpracována a následně odstraněna. Všechny naše služby běží v stateless režimu, tedy žádný stav aplikace není uchováván mezi jednotlivými požadavky. Každý požadavek je zpracován jako nezávislá jednotka, která nevyžaduje uchování dat o předchozích operacích.

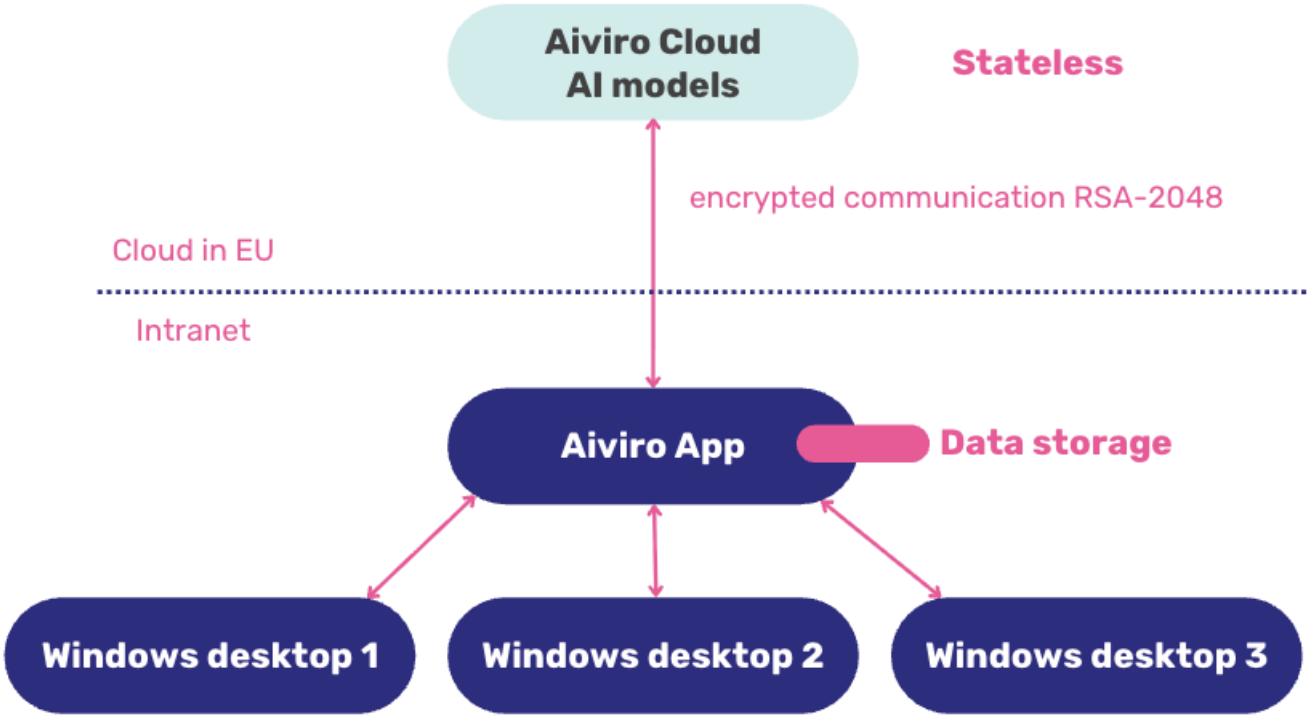


Diagram znázorňuje bezpečnostní architekturu systému Aiviro, který zajišťuje šifrovanou komunikaci (RSA-2048) mezi cloudovými službami v EU (Google OCR, Azure) a interními firemními prostředky (Aiviro Manager, log storage, Windows desktopy)

## Šifrování komunikace

Komunikace mezi lokální částí systému Aiviro a cloudovými službami (API systému na adrese **`api.aiviro.com`**) probíhá výhradně přes zabezpečený protokol HTTPS s využitím TLS 1.3.

Aktuálně používaná šifrovací sada je **`TLS_CHACHA20_POLY1305_SHA256`**. Jde o moderní AEAD šifru, která zajišťuje vysokou úroveň důvěrnosti i integritu přenášených dat. Výměna klíčů probíhá pomocí algoritmu ECDH nad křivkou X25519, čímž je plně zajištěna podpora Perfect Forward Secrecy (PFS). Případná budoucí kompromitace privátního klíče serveru tedy neumožní zpětné dešifrování dříve zachycené komunikace.

Serverový certifikát používá veřejný klíč RSA o délce 2048 bitů (RSA-2048 se v tomto případě vztahuje k veřejnému klíči serverového certifikátu pro ověření identity, nikoliv k samostatnému šifrování celé

komunikace). Certifikát je vydán důvěryhodnou certifikační autoritou Google Trust Services prostřednictvím zprostředkujícího certifikátu WR3.

## Ukládání hesel a tajemství

Hesla, přístupové údaje a další citlivá tajemství (secrets) se v cloudu Aiviro **neukládají**. Jsou bezpečně uchovávána výhradně lokálně v infrastruktuře zákazníka, a to pomocí šifrovaných úložišť nativně podporovaných konkrétním operačním systémem.

Jelikož je Aiviro multiplatformní řešení, pro ukládání secrets využívá standardní bezpečnostní mechanismy dané platformy (Windows, macOS a Linux). Cloudová část systému Aiviro nemá k uloženým heslům přímý přístup a hesla nejsou nikdy přenášena ani ukládána mimo zabezpečené prostředí zákazníka.

## Logování

Systém Aiviro neukládá žádné textové ani obrazové logy do svého cloudu. Veškeré provozní, technické a diagnostické logy zůstávají lokálně v infrastruktuře zákazníka.

Logy standardně neobsahují žádná citlivá data (do logů nejsou nikdy ukládána hesla, autentizační tokeny ani jiná tajemství). V případě potřeby navíc systém umožňuje citlivé hodnoty v logovaných obrázkových datech maskovat. Doba uchování těchto záznamů je plně konfigurovatelná a řídí se výhradně nastavením konkrétní instalace a interními bezpečnostními požadavky zákazníka.

## Auditování

Aiviro poskytuje a eviduje kompletní historii běhů automatizací pro účely auditu. Auditní záznamy obsahují detailní informace o každém spuštění scénáře – zejména čas zahájení a ukončení, celkový výsledek běhu, záznam o případné chybě a jasnou identifikaci komponenty či uživatele, který daný běh inicioval.

Zatímco detailní provozní logy jsou uchovávány pouze po nastavenou retenční dobu (a po jejím uplynutí mohou být automaticky odstraněny dle pravidel dané instalace), základní historie běhů může zůstat zachována dlouhodobě pro auditní a analytické účely.

Změny konfigurací scénářů jsou navíc verzovány a bezpečně ukládány v systému Git. Tento přístup zaručuje absolutní transparentnost: vždy je možné zpětně dohledat kompletní historii změn, autora dané úpravy, přesný čas uložení a konkrétní rozdíly mezi jednotlivými verzemi konfigurace.

## Příprava na certifikaci ISO 27001

V souladu s naší strategií neustálého zvyšování bezpečnosti a transparentnosti aktuálně procházíme procesem přípravy na certifikaci **ISO 27001**. Tento mezinárodně uznávaný standard potvrzuje, že náš systém řízení bezpečnosti informací (ISMS) splňuje nejnáročnější požadavky na ochranu aktiv, řízení rizik a kontinuitu provozu. Implementace tohoto rámce nám umožňuje systematicky dohlížet na integritu a důvěrnost klientských dat, čímž upevňujeme pozici Aiviro jako důvěryhodného partnera pro zpracování kritických obchodních procesů v digitálním prostředí.



**AIVIRO** s.r.o., Purkyňova 670/142, 612 00 Brno-Medlánky | privacy@aiviro.com