PROCONOM
Společně k digitalizaci stavebnictví.

**PROCONOM SOFTWARE, s. r. o.**
Soukenné náměstí 669/2a
Liberec 1
460 01 Liberec

V Liberci dne 10.03.2026

# Technická dokumentace Proconom

**Tento dokument shrnuje technické požadavky, architekturu, bezpečnostní opatření a akceptační kritéria systému Proconom. Je určen pro týmy zákazníka, kteří řeší návrh, nasazení, provoz a podporu systému v režimech On-Premise i Cloud (SaaS).**

## 1. Přehled nasazení

Proconom podporuje dvě provozní varianty:

- **On-Premise**: Aplikační část běží na infrastruktuře zákazníka (VM1), databázová část na samostatném SQL serveru (VM2).
- **Cloud (SaaS)**: Aplikační i datová vrstva jsou provozovány poskytovatelem; zákazník provozuje klienty (desktop, web, mobil) s připojením přes zabezpečený port **TCP 443 (HTTPS)**. V cloudovém režimu je využíván **Azure Front Door** pro směrování a zabezpečení provozu.

# 2. Systémová architektura

## 2.1. Datová vrstva (MS SQL)

- **RDBMS:** Microsoft SQL Server
- **Collation:** Czech_CI_AS
- **ORM:** Entity Framework (Microsoft)

## 2.2. Aplikační vrstva (microservices)

- Hlavní REST API v **.NET Core** (HTTPS, request/response) + **WebSocket (WS)** pro realtime komunikaci.
- **Background služby** v .NET Core pro periodické/neperiodické úlohy.
- Integrace třetích stran: Firebase, Autodesk Forge, služby Microsoft Azure, SendGrid (e-mail).

## 2.3. Prezentační vrstva

- **Desktop:** WPF (Windows).
- **Webový klient:** React + Typescript.
- **Mobilní aplikace:** Android/iOS (Flutter).

## 2.4. Princip CDE a AAAA

Společné datové prostředí (**CDE – Common Data Environment**) Proconom uplatňuje princip **AAAA**: **Authorization, Authentication, Accounting, Audit**.

## 2.5. Architektura cloudu

V prostředí **Azure** je nasazení systému Proconom realizováno pomocí následujících komponent:

- **App Service Plans** – hostují aplikační vrstvy (Web API, microservices).
- **Azure Front Door** – globální entry point pro směrování provozu, SSL terminaci a WAF.
- **Azure Functions** – pro asynchronní a event-driven úlohy.
- **Azure SQL Database** – databázová vrstva.
- **Storage Accounts** – ukládání dokumentů, blob storage, tables.
- **Cosmos DB** – část pomocné datové vrstvy.
- **Networking** – Virtual Network, NSG, privátní propojení mezi službami.
- **Integrace** – napojení na Microsoft Graph API, IoT Hub, OCR služby.

Architektura je navržena jako škálovatelná, s oddělením aplikační, datové a prezentační vrstvy. Front Door zajišťuje vysokou dostupnost a ochranu proti útokům.

# 3. Technické požadavky – On-Premise

## 3.1. VM1 – aplikační servery

**HW:**

- **CPU:** 4 vCPU (4 jádra)
- **RAM:** 16 GB
- **SSD pro OS:** ≥ 120 GB
- **Datový disk:** kapacita dle množství a velikosti dokumentů (dohodou).

**SW:**

- **OS:** Windows Server 2019 a novější

**Součinnost zákazníka:**

- Zajistit **RDP**.
- Předat **administrátorské přihlašovací údaje**.
- Zajistit **správu a zálohování** VM1 a VM2.
- Poskytnout údaje k **SMTP**.
- Vytvořit a sdělit **DNS záznamy** (privátní/veřejné).
- Vygenerovat a předat **SSL/TLS certifikáty**.

## 3.2. VM2 – databázový server

**HW:**

- **CPU:** 4 vCPU (4 jádra)
- **RAM:** 8 GB per SQL core
- **SSD:** ≥ 160 GB

**SW:**

- **OS:** Windows Server 2019 a novější
- **SQL Server:** 2019 Standard+
- **Autentizace:** dle infrastruktury zákazníka (SQL/Windows)

## 3.3. Síťové požadavky

Typické porty: HTTPS 443, MS SQL 1433, RDP 3389, SMTP (dle konfigurace).

**Poznámka:**
Některé funkcionality dostupné v cloudovém režimu (např. integrace s Azure službami, služby pro fulltextové vyhledávání, porovnání dokumentů, živou kooperaci nad úpravou dokumentů a 3D modely) nemusí být v režimu On-Premise dostupné nebo mohou vyžadovat alternativní řešení. Funkčnost těchto služeb závisí na infrastruktuře zákazníka a konfiguraci prostředí.

Provozní vlastnosti systému Proconom v režimu OnPremise, zejména výkon, odezva, stabilita a dostupnost, závisí na kvalitě a konfiguraci infrastruktury zákazníka (hardware, virtualizace, úložiště, síťová propojení, latence, firewall a bezpečnostní politiky).

Zákazník je odpovědný za správné dimenzování, zabezpečení a provoz vlastní infrastruktury, včetně pravidelných aktualizací, monitoringu výkonu, síťových parametrů a správy operačních systémů.

Proconom v režimu OnPremise **nemůže garantovat výkonnostní nebo provozní parametry prostředí**, které nejsou pod jeho přímou kontrolou, a nezodpovídá za incidenty způsobené nedostatečnou kapacitou, nevhodnou konfigurací nebo omezeními infrastruktury zákazníka.

# 4. Minimální požadavky na klienty

- Mobilní aplikace: Podporované (dostávající bezpečnostní aktualizace) verze Android a iOS.
- Webový klient: prohlížeče založené na Chromium (např. poslední verze Chrome, Edge), Firefox, Safari.

Desktop

- Klientská zařízení: CPU ≥ 2 jádra, RAM ≥ 8 GB, disk ≥ 10 GB.
- OS: **Windows 11 a novější**.
- Síť: **TCP 443 (HTTPS)**.

**Poznámka:** Minimální požadavky na CPU a RAM závisí na typu práce. Pro běžné použití postačí uvedené konfigurace, avšak při práci s velkými 3D modely nebo náročnými vizualizacemi může být nutné navýšit výkon (CPU, RAM, případně GPU) podle velikosti a složitosti modelu.

Přehled klientských aplikací: https://www.proconom.cz/pro-klienty-software-proconom

# 5. Zabezpečení systému

- Společnost Proconom Software s.r.o. je certifikovaná:
  - ČSN EN ISO/IEC 27001:2023 – systém managementu informační bezpečnosti,
  - ČSN EN ISO/IEC 27017:2017 – bezpečnost informací pro cloudové služby,
  - ČSN EN ISO/IEC 27018:2019 – ochrana osobně identifikovatelných informací (PII) ve veřejných cloudech,
  - ČSN EN ISO 9001:2016 – systém managementu kvality – QMS.
- Společnost Proconom Software s.r.o. je zapsána v oficiálním seznamu poskytovatelů služeb Cloud Computing.
- Zabezpečení systému Proconom je navrhováno a provozováno v souladu s požadavky směrnice Evropského parlamentu a Rady (EU) 2022/2555 (NIS2) a souvisejícím právním rámcem České republiky v oblasti kybernetické bezpečnosti. Bezpečnostní opatření systému vycházejí z principů řízení rizik, ochrany dostupnosti, integrity a důvěrnosti informací a jsou průběžně rozvíjena v návaznosti na vývoj legislativních a regulatorních požadavků.
- Auditní logy.
- V souladu s nařízením Evropského parlamentu a Rady (EU) 2022/2065 o digitálních službách (DSA) je v rámci systému Proconom CDE zaveden mechanismus umožňující oznámení podezření na obsah uložený uživateli, který může být v rozporu s platnými právními předpisy nebo smluvními podmínkami služby. Tento mechanismus slouží k přijímání podnětů týkajících se obsahu poskytovaného příjemci služby a je součástí opatření zajišťujících transparentní a odpovědný provoz hostingové služby ve smyslu nařízení DSA. https://proconom.atlassian.net/servicedesk/customer/portal/2
- Za obsah nahraný do systému odpovídá zákazník jako poskytovatel příspěvků uživatelů.
- Bezpečnostní aktualizace jsou vydávány v pravidelných intervalech.

## 5.1. Zabezpečení v cloudu

- Data v členských zemích EU.
- Azure bezpečnostní standardy (https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure).
- Data jsou šifrována při přenosu (TLS/SSL) i při uložení (Azure Storage Encryption https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption, Transparent Data Encryption pro SQL).
- Soubory a data ve Storage account jsou replikována GRS, což zajišťuje durabilitu minimálně 99.99999999999999 %.
- Datové databáze jsou zálohovány a umožňují point-in-time restore 35 dní. Long-time-restore (týdenní/měsíční) zálohy jsou dostupné až 3 roky.

## 5.2. Penetrační testy

Poslední penetrační test externím subjektem (listopad 2025) neidentifikoval žádné kritické ani vysoké zranitelnosti. Všechny nalezené nedostatky byly konfiguračního charakteru (např. HTTP hlavičky, HSTS, CORS) a byly vyhodnoceny jako nízké nebo informační.

**Závěr:** Na základě provedeného testu nehrozí bezprostřední riziko kompromitace systému ani úniku dat. Architektura a implementace splňují základní bezpečnostní standardy. Doporučená opatření směřují k dalšímu zvýšení odolnosti, nikoliv k řešení kritických chyb. Systém je v souladu s doporučeními OWASP Top 10 a OWASP API Security Top 10 – kritické zranitelnosti nebyly nalezeny.

# 6. Monitoring, audit a systémové záznamy

Vnitřní monitoring (např. AppInsights, Azure a serverové logy) není běžně přístupný a není určen jako auditní nebo forenzní log. Administrátor systému má přístup k auditním logům requestů na API. Na vyžádání dodáme export. Záznamy jsou automatické a obsahují minimálně tyto informace a činnosti:

- Endpoint, HTTP metodu a status kód, typ requestu a response, identifikace uživatele a databáze, datum a čas, IP adresu.
- Přihlášení a odhlášení všech uživatelů (včetně administrátorů či privilegovaných účtů)
- Činnosti provedené administrátory (přidělení/odebrání oprávnění, založení/smazání uživatele, přidělení/odebrání role, reset hesla, povýšení oprávnění)
- Činnosti prováděné uživateli (úpravy, vkládání a mazání dat, nahrání, stažení nebo prohlížení záznamu, vložení poznámky, revize, změna stavu)

# 7. Přílohy a odkazy

Seznam balíčků třetích stran

- https://www.cde.proconom.cz/packages

OpenApi standard dokumentace hlavního REST API

- https://api.proconom.cz/swagger/index.html

Manuály

https://manual.proconom.cz/

Dokumentace API pro externí synchronizaci

https://api.proconom.cz/manualy/Dokumentace API pro externí synchronizaci.pdf