d365Legal

Dynamics 365 for Legal CRM — Microsoft Marketplace app

Technical and security architecture overview

Microsoft Marketplace: https://marketplace.microsoft.com/en-us/product/d365globalptyltd1665883818849.d365_legal?tab=Overview

Learn Portal: https://learn.d365.global/Tutorials/D365Guides/D365LegalGuides/D365LegalUserGuide



High-level security overview

ARCHITECTURE AT A GLANCE

Microsoft Entra ID

Identity, sign-in and conditional access

Power Platform / Dataverse

Data storage, security roles, auditing

d365Legal solution

Managed solution, plug-ins, PCF controls

Firm tenant

All data and app runtime stay in the tenant

Design principles

- The app runs entirely inside the firms own Microsoft 365 tenant
- No client matter data is copied to a vendor-hosted service
- Security inherits from Microsoft Entra ID and Dataverse, not custom code
- Least privilege by default, enforced by role-based security
- Defence in depth across identity, application, data and network layers

Security provided

WHAT THE PLATFORM AND THE APP DELIVER

Enterprise identity

Single sign-on through Microsoft Entra ID with MFA and conditional access.

Granular authorisation

Dataverse security roles, business units and teams scope every record.

Encrypted data

Encryption in transit and at rest, with tenant-region data residency.

Auditable activity

Platform auditing records data reads, changes and access attempts.

Governed lifecycle

Managed solution deployment with environment-level administrator control.

Continuous assurance

Marketplace certification and Microsoft cloud compliance inheritance.

Identity and authentication

MICROSOFT ENTRA ID AS THE SINGLE SOURCE OF TRUTH

- All users authenticate against Microsoft Entra ID — d365Legal never stores or validates passwords
- Single sign-on across Dynamics 365, Microsoft 365 and the d365Legal interfaces
- Multi-factor authentication and passwordless sign-in enforced by tenant policy
- Conditional access controls device compliance, location, risk level and session lifetime
- Service-to-service calls use OAuth 2.0 with Entra application registrations and managed identities
- Guest and external counsel access handled through Entra B2B collaboration, not shared accounts



Identity is the primary security perimeter — no credential handling in application code.

Authorisation and access control

LEAST PRIVILEGE, ENFORCED BY THE PLATFORM

Security roles

Privileges granted per table and per action — create, read, write, delete, append, share.

Business units

Matters, clients and documents scoped by practice group, office or entity.

Teams and ownership

Owner, access and Entra group teams give matter-level collaboration without over-sharing.

Ethical walls

Record sharing and field-level rules isolate conflicted matters and confidential clients.

Field-level security

Sensitive fields such as fees, rates and settlement values restricted independently.

Administrative separation

System administrator, customiser and business user duties kept distinct.

API and backend security

EVERY CALL AUTHENTICATED, AUTHORISED AND LOGGED

Client

Model-driven app, custom page or integration

»

Entra ID

OAuth 2.0 token issued, scopes validated

»

Dataverse Web API

TLS 1.2+, throttling and API limits applied

»

Data layer

Role checks re-evaluated per record, audit written

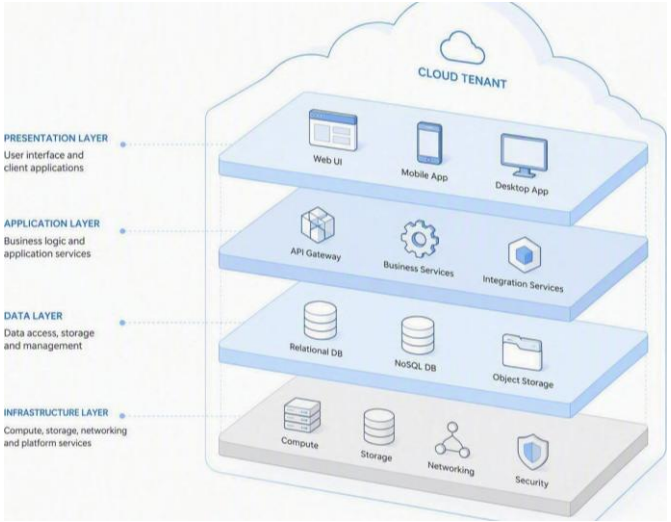
Request path: client to Entra ID to Dataverse Web API to the data layer.

- No anonymous or key-only endpoints — bearer tokens are mandatory for every request
- Server-side business logic runs as sandboxed plug-ins with no elevated tenant privileges
- Integrations use dedicated service principals with narrowly scoped application permissions
- Secrets and connection credentials held in Azure Key Vault or environment variables, never in code

Application security

HOSTED IN THE FIRMS TENANT

- d365Legal is delivered as a managed solution installed into the firms own environment
- No vendor-hosted middleware, database or shared multi-tenant service processes customer data
- The vendor has no standing access; support access is firm-granted, time-bound and revocable
- Environment separation for development, test and production with controlled solution promotion
- Client-side components (PCF controls, custom pages) run within the platform's sandbox model
- Updates are published to the Marketplace and applied by the customer on their own schedule



Firm retains full ownership and administrative control of the environment and its data.

Data protection

CONFIDENTIALITY THROUGH THE MATTER LIFECYCLE

Encryption

TLS 1.2+ in transit; transparent data encryption at rest, with firm-managed keys optional.

Data residency

Data stored in the firms chosen geography, aligned to local practice rules.

Document handling

Matter documents held in SharePoint with inherited permissions and versioning.

Backup and recovery

Platform backups and point-in-time restore, with defined recovery objectives.

Retention and deletion

Retention policies and legal hold support disposal obligations for closed matters.

Information protection

Microsoft Purview sensitivity labels and DLP applied to legal content.

Compliance and governance

ASSURANCE INHERITED AND ASSURANCE ADDED

Inherited from the Microsoft cloud

- ISO/IEC 27001, 27017 and 27018 certified platform services
- SOC 1, SOC 2 Type II attestation reports available to the firm
- GDPR and regional privacy commitments through the Data Protection Addendum
- Physical, network and hypervisor security operated by Microsoft

Governed by the firm

- Marketplace certification review before the app is published
- Auditing and Microsoft Purview audit logs for access review
- Change control through solution versioning and environment promotion
- Administrative policies: DLP, tenant isolation and environment security groups

Shared responsibility: Microsoft secures the cloud, the firm governs the tenant, d365Legal secures the application layer.

Security for firm authentication

CLIENT AND EXTERNAL PARTY ACCESS

Client portal identities

External clients authenticate via Entra External ID with self-service sign-up controls.

Federation

Support for federated sign-in from a client's own identity provider where required.

Scoped visibility

Portal users see only their own matters, documents and invoices — enforced server-side.

Session protection

Short-lived tokens, idle timeout, revocation on offboarding and sign-in risk detection.

Onboarding controls

Invitation-based access with approval workflow and periodic access recertification.

Monitoring

Sign-in logs and anomalous access alerts surfaced to tenant administrators.

Summary

THE SECURITY POSITION IN FIVE POINTS

1. Client data never leaves the firms tenant — the vendor holds no copy and no standing access.
2. Identity is handled entirely by Microsoft Entra ID, with MFA and conditional access under firm policy.
3. Authorisation is enforced by Dataverse roles, business units, teams and field-level security.
4. Data is encrypted in transit and at rest, resident in the chosen region, and covered by retention controls.
5. Compliance is inherited from Microsoft's certified platform and reinforced by Marketplace certification.