



How Case Information Is Kept Secure

A plain-English overview for counsel · Arbitration & mediation case-management system

ADRassistant runs its scheduling, case files, invoicing, and communications entirely on **Microsoft's cloud** — the same **Microsoft 365** and **Microsoft Azure** platform relied on by law firms, courts, hospitals, and government agencies. Your clients' materials are not kept on a personal laptop or handed to an outside service. This page explains, in everyday terms, how that system protects the information you entrust to us.

1 The information lives inside Microsoft's cloud

Case documents, party and counsel contact details, and scheduling data are stored in Microsoft 365 (OneDrive and SharePoint) and Microsoft Azure, housed in Microsoft's professionally secured data centers in the United States. Microsoft maintains these systems to recognized industry standards and undergoes independent security audits and certifications (for example, SOC 2 and ISO 27001).

2 Everything is encrypted — in transit and at rest

Information is encrypted (scrambled so it cannot be read) both while it travels over the internet and while it sits stored on Microsoft's servers. Intercepted data would be unreadable without Microsoft's keys.

3 Only authorized people and programs can get in

Access requires a verified Microsoft sign-in from your firm. The automated part of the system proves its identity to Microsoft using a built-in, passwordless *managed identity*, so no passwords sit in the code for anyone to steal. The few sensitive keys the system does use are locked in a Microsoft *Key Vault* — a dedicated digital safe — and sensitive internal approvals require a one-time code sent by text message (two-factor authentication).

4 Case folders are shared through private, personalized links

When you are granted access to a case folder, it is through a secure link tied to *your specific email address* — not an open link that anyone could forward and use. The first time you open it, Microsoft confirms your identity with a one-time code emailed to you. If counsel changes, access updates automatically: new people are added and anyone removed loses access. When the case closes, access is turned off.

5 No outside middlemen

The system connects directly to Microsoft's services through Microsoft's official, permission-limited interface (the Microsoft Graph). Case data is not routed through third-party automation services; it stays within **ADRassistant's** own Microsoft environment. This purpose-built system replaced an earlier setup that had relied on an outside automation vendor to make the system more secure.

6 Backups, version history, and recovery

Microsoft keeps redundant copies and a full version history of documents, with a recycle bin, so files can be recovered if something is accidentally changed or deleted.

7 Activity logging and tamper protection

System activity is logged for review, and every automated entry point is guarded against forged or “spoofed” requests — each instruction is verified as genuinely coming from an authorized source before it is acted on.

Questions about how client information is handled? Contact us at www.adrassistant.com/#contact. This overview is provided for general information about our safeguards and does not modify any confidentiality order, engagement terms, or the parties' agreements.