Frequently Asked Questions

TEXAS OCA SECURITY & DATA POLICY

➔ ***How is data encrypted in transit and at rest?***

All data is protected using end-to-end encryption. eCourtDate enforces HTTPS for all connections in transit and uses AES-256 encryption for data at rest. The platform operates in compliance with FIPS 140-2 and 140-3 standards, ensuring government-grade encryption across all systems.

➔ ***Does eCourtDate retain any of the transmitted data, or is it used solely for message delivery and then purged?***

eCourtDate does not permanently store personally identifiable information (PII) on its portals or dashboards. Message and delivery data are used solely for operational purposes and securely cached during processing. Archived PII is automatically purged after approximately 90 days, and agencies can permanently remove data at any time using the built-in Reset Data tool.

➔ ***What is the data retention policy for reminder-related information?***

Other than data that is automatically shared with the Statewide Data Dashboard or Portal, courts may customize their own data retention preferences.

eCourtDate offers full lifecycle customization including:

- Automated data archival
- Automated data purge
- One time data archive and purge tools

Once data is purged from your tenant, it is permanently deleted in the database. eCourtDate does maintain hourly and daily backups. Once the backup period expires (7 - 14 days), then the data is not retrievable.

➔ ***How is access to data managed and monitored?***

Access to all systems is controlled through strict role-based permissions with create, read, update, and delete (CRUD) access levels. Multifactor authentication (MFA) is required for administrative users. Every access event is logged using immutable, read-only audit trails, and activity is continuously monitored through AWS CloudTrail and related security services.

➔ ***Is your product compliant with any recognized security or privacy standards?***

Yes. We use AWS's FIPS 140-2/140-3 compliant cryptographic services, ensuring that all data encryption, decryption, and key management processes adhere to federal and state standards.

Our platform is hosted in AWS GovCloud (US), a secure environment specifically designed for U.S. government workloads. This ensures that all data is processed and stored using FIPS-compliant endpoints, providing an additional layer of protection for sensitive information. AWS GovCloud (US) is compliant with FedRAMP High, the DOJ's Criminal Justice Information Services (CJIS) security policy, U.S. International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5, FIPS 140-2, IRS-1075, and others.

➔ ***What measures are in place to detect and respond to unauthorized access or potential data breaches?***

eCourtDate uses continuous monitoring, vulnerability scanning (OWASP/CWE standards), and automated intrusion detection tools. The system includes CloudFlare firewall protection, DDoS mitigation, and real-time email alerts for any abnormal or unauthorized activity.

➔ ***Is there a data use or sharing agreement in place defining how court-provided data may be used?***

Statewide Portal

Courts using eCourtDate for cases and court dates can share data with the Texas Courts Statewide Portal. This allows attorneys and interested parties to subscribe for notifications.

No personal data is included. Only the following data fields:

Case Number	*Event Reference*	*Event Type*
Case Type	*Event Date*	*Event Status*
Case Status	*Event Time*	
Case Attorney Bar Number	*Event Location*	

There is no additional cost or integration effort. Courts can opt out.

Statewide Data Dashboard

A statewide dashboard tracks aggregate data about messaging and events performance.

This is required as part of the legislative bill to track outcomes. All data is aggregate and does not include any personal or case specific records.

Courts cannot opt out of the Data Dashboard if funded by OCA.

Support and Carrier Compliance

eCourtDate support is required to monitor messaging for carrier compliance. If a carrier flags messaging for spam, eCourtDate may validate that messages are compliant. No personal data is used although message content may be reviewed.

➔ ***How does eCourtDate handle user authentication and account security?***

All user access is protected through single sign-on (SSO) or multifactor authentication (MFA). Session tokens are short-lived and automatically expire after

a defined period of inactivity. Passwords are stored using encryption with salted hashing and never transmitted in plaintext.

➔ ***Are logs auditable by the court or OCA?***

Yes. Courts and OCA administrators can request full access to immutable audit logs, which track all login attempts, data access events, and system changes. Logs are retained according to FedRAMP retention requirements.

➔ ***What is eCourtDate's incident response protocol?***

The company maintains a 24/7 incident response plan aligned with NIST 800-61 standards. Any confirmed data breach or security incident triggers immediate isolation, investigation, and notification procedures in compliance with state and federal laws.

➔ ***How is system availability and disaster recovery handled?***

eCourtDate uses active-active redundancy across multiple AWS GovCloud availability zones. Disaster recovery tests are conducted semi-annually, and recovery time objectives (RTOs) are under 1 hour for critical systems.