Everlaw

Security and Compliance at Everlaw

As a provider of cutting-edge software for customers with highly confidential data, we recognize how important security is to protecting information. Everlaw's core philosophy is to build for the long term. We understand that the security of our product and the compliance culture of our business are instrumental in maintaining the trust our customers place in us, and we are committed to protecting that information. That is why we have a full-time VP of Security and Compliance who reports directly to our Founder and CEO.

Everlaw's compliance program is holistic. It demonstrates our commitment to ethics and our company values, as well as compliance with our security and confidentiality commitments to customers and applicable laws and regulations. The framework for compliance at Everlaw has seven elements and is based on both the United States Sentencing Commission Guidelines Manual, Section 8, on an Effective Compliance and Ethics Program, and the U.S. Attorneys' Manual, Section 9-28.800 on Corporate Compliance Programs:

1. Everlaw Code of Conduct, Policies and Procedures
2. Oversight by our CEO and Board, and accountability resting with our VP of Security and Compliance
3. Education, formal training, and regular communication and awareness activities
4. Human resources security practices and appropriate and defined delegation of authority
5. Enforcement, discipline and incentives
6. Risk assessment, monitoring, and third-party audits
7. Continuous improvement

Internal Governance
Our compliance program at Everlaw establishes a formal system of internal control. This includes, for example, regular meetings of our Risk Committee and Security Management Team, which are led by our VP of Security and Compliance, and include our CEO and leaders of each team at Everlaw. The Security and Compliance, Internal Operations, and Finance teams perform formal reviews of all vendors and suppliers prior to contract execution. Everlaw employees complete security and compliance onboarding training upon hiring, annual face-to-face security and privacy awareness training, in addition to annual policy and compliance and information security and privacy computer-based training modules. Our system of internal control requires annual third-party audits to test the operational effectiveness of our program and practices.

Independent Auditing and Testing
At Everlaw, we choose to undergo rigorous security and privacy testing by independent third party auditors. In 2017, Everlaw completed a third-party HIPAA Compliance Assessment that evaluated compliance with the HIPAA Administrative, Physical and Technical Safeguards. In 2018, Everlaw completed an independent GDPR Compliance Readiness Assessment. In addition, since 2016, Everlaw has completed an annual SOC 2 Type II certification, which includes vulnerability scanning and penetration testing. In 2018, Everlaw added the Privacy criteria to the SOC 2 audit scope, which already included the Security, Availability and Confidentiality criteria.

For a company to receive SOC 2 Type II certification, it must have sufficient policies and controls operating to protect customers' data, and it must provide detailed evidence and pass independent testing of operational effectiveness through the audit testing procedures. This examination of our entire security and compliance infrastructure, rather than solely relying on the credentials of our cloud service provider, illustrates Everlaw's ongoing commitment to create and maintain stringent security controls. We are happy to provide a copy of the SOC 2 audit report to customers or

prospective customers upon request, and after executing a confidentiality agreement.

Our Policies and Practices

Below are some of our key security, privacy and compliance policies and practices, although it is not an exhaustive list. We hope that our continuing commitment to security, as well as our transparency regarding policies and practices, set your mind at ease. If you have any questions, don't hesitate to contact us at security@everlaw.com.

Internal Operations

All of our employees are required to undergo background checks and sign our nondisclosure and confidentiality agreement upon hiring. We also require employees to affirm their acknowledgement and agreement to follow Everlaw's Code of Conduct, Employee Handbook and all Policies and Procedures on an annual basis. The Everlaw Human Resources team works closely with the Security and Compliance team on all employee onboarding and offboarding activities.

Everlaw requires full disk hard drive encryption for all computers, multi-factor authentication, and controls employee access to customer and personal data using role-based access and account management procedures (including a BYOD policy). The Security and Compliance team monitors employee access requests and changes, enforces the clean desk and BYOD policies, and works with the Everlaw IT team to ensure secure machine configuration for all employees.

Data Protection and Privacy

Everlaw has implemented data protection and privacy by design principles into our system of internal control via business processes and our software development lifecycle. Employee training includes the 7 Foundational Principles of Privacy by Design, and team data inventories and data protection impact assessments are updated and reviewed by the Security and Compliance team on a quarterly basis coinciding with our Risk Committee meetings. Everlaw has also implemented a formal vendor management program to comply with our security and privacy commitments.

As described above, Everlaw has engaged independent auditors to review compliance readiness for both HIPAA and GDPR, and has a SOC 2 Type II certification in Privacy. For clients that are covered entities under HIPAA, Everlaw reviews and executes Business Associate Agreements. For clients operating in the EU, or processing personal data of EU data subjects, Everlaw provides a Data Processing Addendum that details our technical and organizational measures regarding security. The Everlaw Privacy Policy and Privacy Notice are available on each public website (United States, Canada, Australia, European Union, United Kingdom).

Cloud Service Provider and Data Center Security

Our primary data source is stored on secure AWS cloud servers, which surpass industry standards for privacy and security. Everlaw operates in several jurisdictions using AWS cloud hosting infrastructure: US (US East Region), Canada (Central Region), Australia (Asia Pacific, Sydney Region), UK (London Region), and EU (Frankfurt Region). AWS has SOC 1, 2, and 3, ISO 27001, FedRAMP, and FIPS certifications, in addition to meeting compliance standards for many other legal, security, and privacy frameworks. You can read more about AWS' compliance practices and certifications here: https://aws.amazon.com/compliance/.

Low-level Access Controls and Intrusion Detection

All data is encrypted in transit via TLS, and at rest using AES-256. We use intrusion detection software to monitor our servers for break-ins. We are notified immediately of any unexpected activity. Our servers are firewalled to prevent external access via any ports other than 80 (http) and 443 (https). We use key-only (no passwords) and multi-factor authentication for low-level server access to prevent password-guessing. We also impose IP address restrictions limited to our office to prevent third parties from accessing our servers.

Access Controls
We employ state-of-the-art practices to prevent cross-site scripting and cross-site request forgery. Access to data can be restricted by user or security group. All user activity is fully logged on the system. We store when users log in and out, and every action they take on the site – down to which pages of which documents they view. This information is visible both to us and to the case administrators, so any suspicious activity can be detected and acted upon quickly.

Everlaw supports single sign-on (SSO) and multi-factor authentication (MFA) for all users of our product. SSO enables users to log into Everlaw via their organization's existing directory service (e.g., GSuite, Active Directory, LDAP). They will not have to maintain a separate username and password for Everlaw. When MFA is activated for a case, users are required to authenticate every computer or device through which they access Everlaw by providing both their password and another piece of information. The second factor can either be a one-time code delivered to their email address, or a rolling Google Authenticator app on their mobile device.

Application Security
Everlaw's Application Development Policy requires that our engineers performing development tasks employ information security steps to ensure the protection of sensitive information, application availability, and data integrity. The Everlaw application servers respond only to SSL-encrypted HTTP calls. Our SSL certificates are signed by an industry-leading certificate authority and are signed with a minimum 1024-bit encryption.

System Availability
On average over an annual basis, our uptime exceeds 99.9%, including scheduled maintenance windows. The Risk Committee and Security Management Team work together on Everlaw's Business Continuity Plan and Disaster Recovery Procedure, which is tested every year.

Data Backup
Data is stored in triplicate in different AWS geographical locations, with 99.999999999% yearly durability. User work product is backed up in this same fashion 6 times a day. Recovery is provided as part of Amazon's cloud offerings.

Data Retention, Return and Destruction
Unless otherwise specified, we purge user data at the conclusion of the case. When a customer requests deletion, Everlaw destroys the media and deletes the case from the servers. Everlaw complies with contractual requirements to provide proof of deletion.

Security Incident Management and Breach Policy
Everlaw's Incident Reporting and Response Policy contains a procedure for incident management with a clear escalation path to the VP of Security and Compliance and CEO, as well as steps for breach notification. All incidents are logged in an incident tracking system, which is subject to auditing on an annual basis as part of SOC 2 testing. Incident Response is also tested annually as part of Everlaw's planned Business Continuity and Disaster Recovery testing. Everlaw is insured in case a loss of data causes our users economic harm.

Regulatory Compliance
Everlaw's compliance program includes regular monitoring and evaluation of our compliance with applicable laws and regulations, as well as employee training, managed by the Security and Compliance team. In addition to security and privacy, our program includes training for all employees on important regulatory and compliance issues such as AML, Antitrust, and Gifts & Entertainment.