Security & compliance

Be secure in your success.
Built-in security

Know your data is secure with Datasite. We have embedded security at every level: platform, processes and people. The key components are outlined here – see our website for full details.

Culture
We have an industry-leading security culture, led by our VP of Information Security.

Application security
Execute deals end-to-end without leaving the ironclad security of the project environment.

Vulnerability assessment
Regular code scans, vulnerability assessments and penetration testing conducted by industry-recognized third party.

Data/Content security
Encryption of data both at rest and in transit. Purging of files 30 days after project close.

Platform security
User information, app data and logs all stored separately. Perimeter defenses include reverse proxy and a proactive multi-layer network.

Secure architecture by design
Cloud-based secure processing
Added security from Microsoft Azure
Global compliance and privacy

Datasite commits to the highest global standards to bring you the best in technology and security. Wherever you are in the world, we help you get your deal done right.

Maintaining global standards

Datasite products have:
- ISO 2701 certification since 2007
- ISO 27017, 27018, and 27701 certifications
- SOC 2 Type II attestation

Committed to data privacy

Datasite abides by all applicable data protection laws and regulations, and the highest standards of ethical conduct. We enforce strict policies for our employees and contractors pertaining to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to a Datasite user, employee or customer.
Rigorous data protection policies

We ensure that personal data is processed in accordance with local data privacy laws, all across the globe.

Here’s how we uphold data privacy:

In general
- Obtaining consent and notification before processing personal data
- Conducting impact assessments on new data processing activities
- Confidentiality obligations for staff and sub-contractors
- Storing personal data on encrypted infrastructure
- Routine testing of our Incident Response Plan (IRP)

In AMERS
- Hosting US, Canada, and South American content in US data centers
- Retaining no personal data that is subject to CCPA

In EMEA and APAC
- Abiding by Article 28(3) GDPR via a data processing agreement with our customers
- Hosting EMEA and APAC content in EU data centers, and covering other data transfers with standard contractual clauses

In Australia
- Abiding by Australian Privacy Principles (APP)
- Hosting content in data centers in Australia

GDPR compliant
CCPA compliant
APP compliant
Is the Datasite mobile app as secure as the desktop version?
Yes. The mobile app has the ironclad security credentials that make Datasite the world’s most trusted data room:

- SOC 2 Type II attestation
- ISO 27001, 27017, 27018 certified
- GDPR, CCPA, APP compliant

All communication between the mobile app and the backend is also encrypted with AES-256, while in-transit communications use at least TLS 1.2. This makes the app as secure as using your desktop.

What additional safeguards does the mobile app have?
The app only supports recent OS versions. Older, less secure versions of the OS are not supported.

Furthermore, the mobile app intentionally limits how much users can do. For example, a user can view content, but the documents are never stored on the device. The user is also unable to redact content or make bulk changes to the data room.

When the user logs out, the app clears all temporary sensitive data, encryption credentials storage and caches.

What if a user’s mobile device is lost or stolen?
Only registered users can access projects and documents, and these users must pass strict access controls.

The app supports SSO and includes biometric login. The app will not open without the device’s passcode. If the device is jailbroken or rooted, the app detects this and will not activate – or, if already in use, will stop processing.

How secure is the app development process?
To ensure potential vulnerabilities are found and dealt with, the app is tested with each monthly update, in addition to annual pen-testing. The app also prevents possible modifications to its source code.

At each phase of development, we follow Secure SDLC procedures, to guard against any vulnerabilities emerging via updates or new versions. We also scan our code base and third-party code libraries for potential issues.

Does the mobile app collect user data?
User data is collected only for analytics and application performance improvement. Data is not stored on mobile devices. Furthermore, the app does not access the phone’s keychain for any storage.