Datasite®

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.

Vulnerability assessment

Regular code scans, vulnerability assessments, and penetration testing are conducted by industry-recognized third parties.

Application security

Every Datasite product is built with security top of mind. You can execute deals end-to-end without leaving the security and comfort of the project environment.

Platform security

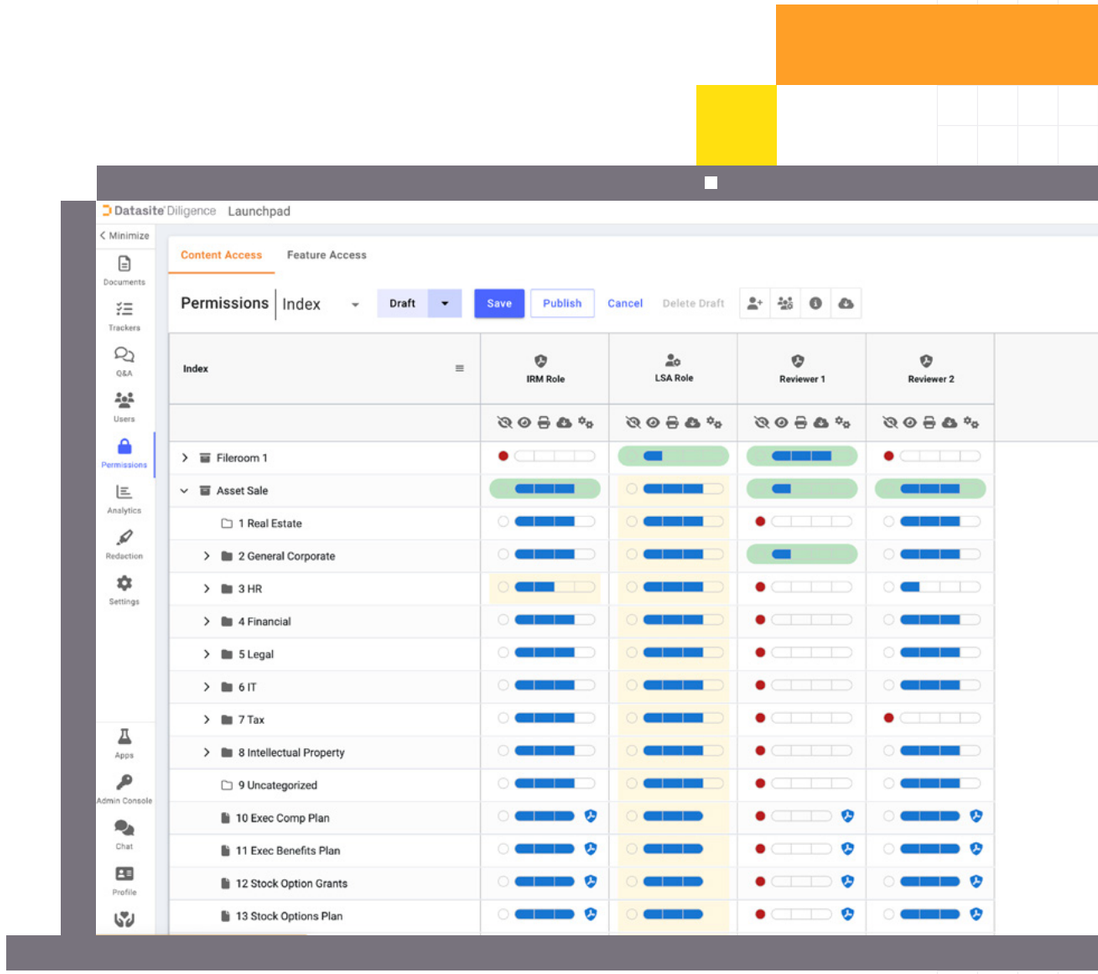
Datasite is securely hosted on Microsoft Azure. Cloudflare provides WAF and DDOS protection. Separate storage for user information, app data, and logs.

Data / content security

Data is encrypted both in transit and at rest. The purging of all project files begins 30 days after completion of the project.

Data privacy

Datasite enforces 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.



Secure architecture by design

Cloud-based secure processing

Added security from Microsoft Azure

Highest global standards

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 27001 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.

ISO
27001
27017
27018
27701
CERTIFIED

SOC 2
Type II
ATTESTATION

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:

Key principles

- Ensuring all personal data is processed according to each jurisdiction's laws
- 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)

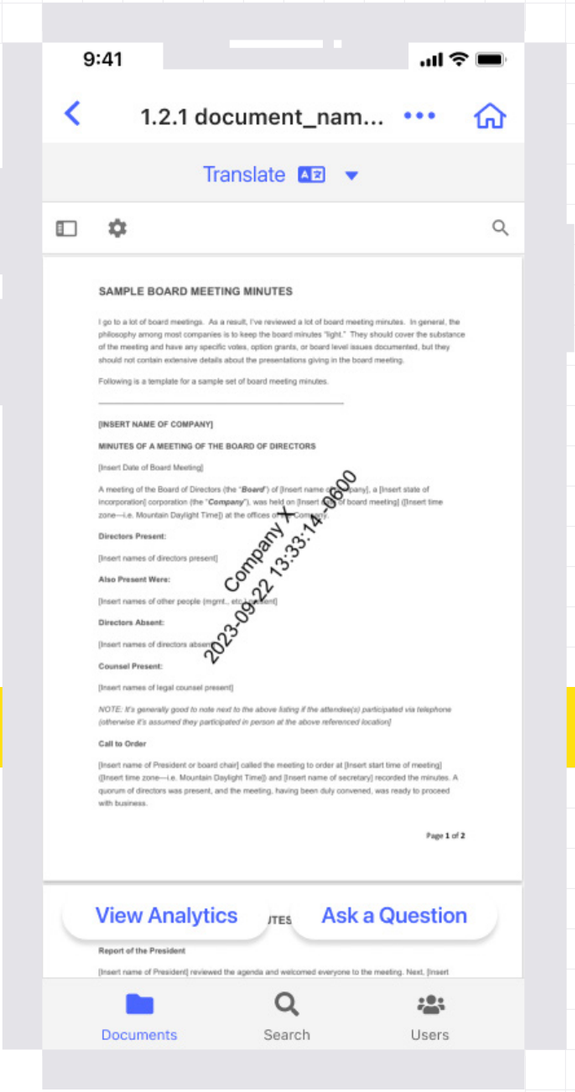
Hosting

- Abiding by all global, regional, and local data privacy laws
- Compliance with EU and UK GDPR, CPRA, and APP
- Hosting of all AMERS data in US data centers, EMEA and APAC data in EU data centers, and Australian data in Australian data centers
- Covering overseas data transfers with standard contractual clauses
- Participating in the Privacy Shield Framework. Datasite is an active particpant in the EU-U.S. Data Privacy Framework, UK extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework

EU & UK GDPR
compliant

CPRA
compliant

APP
compliant



The most secure and trusted mobile app

All the security and additional safeguards. So you can do your deals wherever you are. Safely and securely.

Is the Datasite mobile app as secure as the desktop version?

Yes. The mobile app has the wall-to-wall security credentials that make Datasite the world's most trusted data room:

- SOC 2 Type II attestation
- ISO 27001, 27017, 27018, 27701 certified
- EU & UK GDPR, CPRA, APP compliant

In-transit communications use at least TLS 1.2 encryption, and all communication between the mobile app and the backend is encrypted with AES-256. 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.

Get the **Datasite mobile app**

#Wheredealsaremade

Get in touch, visit www.datasite.com **or contact:** info@datasite.com
AMERS +1 888 311 4100 | **EMEA** +44 20 3031 6300 | **APAC** +852 3905 4800

Datasite®