DekkoSecure

Are you concerned that your shared sensitive data may not be 100% secure and compliant?

Use Cases

Private and public organisations handle a wide range of highly confidential information that must be shared securely and efficiently between teams, departments, and external stakeholders. The information includes:

- Personal information
- Digital evidence
- Healthcare information
- Passwords
- Business projections/marketing plans
- Sensitive financial information
- Client/Customer lists
- Intellectual property
- Legal documents
- Vendor and client/customer agreements
- Technology contracts

8 critical data security questions to ask your data security team about your current data sharing practices

1. How comfortable are you with the security of our data sharing practices (e.g., email, messaging, USBs, hard drives, video conferencing, and cloud-based file sharing solutions)?
2. Who in our organisation has access to shared data, and how is that access controlled and regularly viewed?
3. Are we enforcing multi-factor authentication (MFA) to limit data access?
4. Is our data encrypted at rest, in transit, and at work?
5. Are we using end-to-end encryption to ensure only authorised recipients can access shared data
6. Are we actively monitoring for unauthorised access or suspicious activity in our data-sharing systems?
7. Do we have the ability to view a comprehensive audit trail on every piece of data uploaded and shared by the team?
8. Do our current information sharing practices satisfy Data Sovereignty?

If you are concerned about any of the above, your data may not be as safe as you need it to be.

DekkoSecure's end-to-end encrypted solution addresses all eight of the above security concerns with no hardware or software to purchase or download and with minimal IT administration required.

Contact us to learn more:

Contact DekkoSecure

DekkoSecure