Data and Security

Data Protection and GDPR

intheOffice ensures it complies with the seven key principles set out in the UK GDPR.

Limited Personal Data

Personal information collected is kept to the absolute minimum required to fulfil the Contract defined in our Subscription Terms and Conditions and the features that you have enabled.

Email and Name Only

Most features only require a users: name (or other identifier), and work email address.

No Special Category Data

None of our features require any users to enter special category data.

[Data Processing Agreement](#) | [Privacy Policy](#)

Security

intheOffice is built using a powerful and secure technology stack, to ensure premium protection, scalability and platform uptime. Using Firebase for it's Backend-as-a-Service, all data transactions and storage are protected, certified and encrypted.

Securely Authenticated

Firebase Authentication is a robust authentication layer that leverages industry standards like OAuth 2.0 and OpenID Connect to provide a secure SDK that supports authentication using passwords, Microsoft 365 SSO and other federated identity providers.

Least Privileged Access

Services are controlled through strict security rules based on the principle of least privilege, preventing unauthorised access.

Encrypted

Data at rest is encrypted within Firebase services, while data in transit is encrypted using HTTPS.

Certified

Firebase services are certified under major privacy and security standards, to ensure the highest levels of platform security and protection.

Service	ISO 27001	ISO 27017	ISO 27018	SOC 1	SOC 2	SOC 3
Cloud Firestore	Yes	Yes	Yes	Yes	Yes	Yes
Cloud Functions for Firebase	Yes	Yes	Yes	Yes	Yes	Yes
Cloud Storage for Firebase	Yes	Yes	Yes	Yes	Yes	Yes
Firebase Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Firebase Hosting	Yes			Yes	Yes	Yes