Deal Lens privacy notice

Last updated 4 November 2026

This notice explains how personal information is used when you visit Deal Lens, create an account, save a deal workspace or contact us. Deal Lens is a free UK legal-information app for exploring M&A issues.

Who is responsible for your information

Milo Brooks operates Deal Lens and is the controller for the processing described in this notice. In this notice, “we” and “us” mean Milo Brooks operating Deal Lens.

Privacy enquiries and requests: milobrooks100@gmail.com

What we collect and why

Account information includes your email address, account identifier and authentication information. We use it to create and secure your account, verify your email, allow sign-in and support password recovery. Firebase handles authentication.

Saved workspace information includes deal details, questionnaire answers, tasks, preferences and selected avatars, where these contain personal information. We use it to provide the workspace and, for verified accounts, save and retrieve progress across devices. You choose what you enter; avoid including unnecessary personal or sensitive information about other people.

Company Radar retrieves public Companies House register information. Records may include information about directors, officers and other individuals appearing on the register. We use it to display company information, identify changes and let you save relevant findings with a deal.

Technical information, such as IP addresses, request details and error or security logs, may be processed by our infrastructure providers to deliver and protect the service. If you contact us, we use your contact details and message to respond and keep an appropriate record.

Where information comes from

Information comes from you, your use of the app and public Companies House records. Without an account, deal progress is stored in your browser. Verified accounts can sync workspace data to Cloud Firestore. Company Radar requests pass through our hosting infrastructure to Companies House.

How long we keep information

We keep personal information only for as long as it is needed and review account retention monthly under the schedule below. You may request deletion sooner.

Information	Retention period or rule
Verified accounts and saved workspaces	While the account is in use. At the monthly review, accounts with no meaningful activity for at least 24 months are identified for deletion. We send a warning and allow 30 days to return or request continued retention before deleting the account and its saved data.

Information	Retention period or rule
Unverified accounts	At the monthly review, we delete accounts that have remained unverified for at least 30 days. This means removal may occur during the following month, rather than exactly on day 30.
Account deletion requests	The in-app control attempts immediate deletion of saved account data and the sign-in account. For requests made by email, we aim to complete live account deletion within 30 days after any necessary identity checks, subject to applicable legal exceptions.
Company Radar snapshots and findings	For as long as the associated saved workspace is retained. They are included in account deletion where stored in the account. Public source records remain subject to Companies House's own arrangements.
Support messages	12 months after the enquiry is resolved, unless a specific ongoing issue justifies longer retention.
Privacy requests and complaints	A minimal record for 3 years after closure to demonstrate how the matter was handled. Unnecessary attachments and duplicate information are removed sooner.

Guest data remains on your device until you delete it or clear the relevant browser storage. Deleting a cloud account does not erase separate guest data, offline copies on every device or files you have downloaded.

Technical logs have provider-specific retention periods. Firebase Authentication keeps IP logs for a few weeks and says other authentication information is removed from its live and backup systems within 180 days after user deletion is initiated. That period is separate from our live account deletion process.

We may retain limited information longer where required by law or necessary for a specific dispute or security incident. We document the reason, restrict its use and review it until it can be deleted.

Cookies and browser storage

Deal Lens uses browser storage for deal progress, preferences and account state. Guest progress is separate from account data. Browser site-data controls let you clear this storage, but may remove unsynced work or sign you out. Clearing local storage does not delete your cloud account. See the retention section above for how long locally saved information remains.

Protected Vercel previews may use _vercel_jwt for deployment access and vercel-feature-flags for the Vercel toolbar. These cookies relate to the preview environment; other deployments may differ. You can manage or delete cookies through your browser. Blocking necessary storage may stop features working.

Any additional storage uses must be explained before they operate, with consent or an objection mechanism where the applicable rules require it.

Our lawful bases

We rely on performance of our contract with you for processing necessary to provide the account and saved-workspace service you request. We rely on legitimate interests to operate and secure Deal Lens, diagnose faults, respond to enquiries and provide Company Radar's public-register information. These interests are in providing a useful, reliable service while limiting unnecessary use of personal information.

Where a legal obligation requires us to keep or disclose information, we rely on that obligation. A free service does not remove your data protection rights.

Service providers and overseas processing

Google Firebase provides authentication and cloud database services. Vercel provides application hosting, deployment and supporting infrastructure. They may use infrastructure and support subprocessors to deliver their services. Companies House receives the search and retrieval requests needed to provide Company Radar results.

The current Firestore database is in London. Firebase Authentication runs in the United States. Vercel and service-provider operations may also involve processing outside the UK. A UK database location does not mean all processing stays in the UK.

Google LLC and Vercel state that they participate in the UK Extension to the EU–US Data Privacy Framework. For transfers within the scope of a recipient's active certification, this is the UK–US data bridge. Other transfers require an applicable adequacy decision or appropriate safeguards, such as standard contractual clauses with the UK Addendum. You can contact us for information about the safeguards applicable to your data.

Firebase privacy and processing information

Vercel privacy information

Your rights

Depending on the processing and applicable exceptions, you can request access to your personal information, correction, erasure, restriction of use or a portable copy. You can object to processing based on legitimate interests. Where processing relies on consent, you can withdraw it without affecting earlier lawful processing.

Contact milobrooks100@gmail.com to exercise your rights. We normally respond without undue delay and within one month. Where the law permits additional time or requires identity checks, we will explain this to you.

Questions and complaints

Please email milobrooks100@gmail.com if you have a privacy concern. You may also complain to the Information Commissioner's Office, the UK data protection regulator.

Make a complaint to the ICO

ICO helpline: 0303 123 1113. We will update this notice when our practices change and make the latest version available with the app.