SaaS Platforms As Undiscovered Repositories

Business records increasingly live inside SaaS applications, not just email and drives. This guide helps UK lawyers map the SaaS estate, preserve platforms against their own retention, and collect structured records and audit trails for disclosure.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/saas-platforms-as-undiscovered-repositories

SA AS DISCOVERY · A GUIDE FOR UK LAWYERS SaaS Platforms as Undiscovered Repositories Finding, Preserving and Collecting the Business Records That Live Inside Applications COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: BUSINESSRECORDSINCREASINGLYLIVEINSIDESAAS APPLICATION S THAT NO EMAIL - AND - DRIVESDISCLOSUREEXERCISEWILLFIND: MAP THEESTATEFROMENDPOINTS, NETWORKANDEXPENSES; PRESERVEEACHPLATFORM AGAINSTITSOWNRETENTION; ANDCOLLECTITSSTRUCTUREDRECORDSANDAUDIT TRAILS, WHICHFREQUENTLYANSWERTHECASEMOREDIRECTLYTHANANYDOCUMENT

§ 02 · FIRST PRINCIPLES The problem in plain English: the record moved into the app

§ 03 · FINDING THE PLATFORM S Finding the platforms: mapping the SaaS estate a business actually uses

§ 04 · WHATEACHKINDHOLDS What each kind holds: CRM, project, HR, support, finance and messaging

§ 05 · THESTRUCTUREDRECORD The structured record: fields, history, comments and audit trails

§ 06 · PRESERVATION AND COLLECTION Preservation and collection: holds, exports, APIs and the format problem

§ 07 · DEPLOYMENT Deployment: disclosure obligations, proportionality and the audit trail's power

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION PLATFORM COUNTERPARTIES THE ITSELF INTEGRATION END POINT IDENTIT Y + PROVIDER REFLECTIONS TRACES NETWORK RECORDS

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THECUSTODIANWITHNODOCUMENTSANDACRMFULLOFTHEM EXAMPLE2 · THEPROJECTTOOLTHATHELDTHEREALCHRONOLOGY EXAMPLE3 · THEPROPORTIONATECOLLECTIONTHATAVOIDEDTHEWHOLESALEONE

§ 10 · WHEREITGOESWRONG Common mistakes and technical limitations Common mistakes Technical limitations

§ 11 · INTERROGATORIES & DRAFTING AIDS Questions to ask · Suggested wording Ask your client Ask your opponent Ask your e Discovery / forensic provider PROTOCOL

§ 12 · QUICK CONTROL Checklist and red flags · When to involve a digital forensic expert The SaaS-discovery checklist Red flags When to involve a digital forensic expert

§ 13 · COMMON QUESTIONS Frequently asked questions A key witness says they have almost no relevant documents. Is that the end of it? How do we even find out what SaaS platforms a business uses? Can data in a CRM or project tool really be collected for disclosure? What makes the audit trail so useful? The other side wants "all our HR system data". Do we have to extract everything? What if a record was changed or deleted in the app?

§ 14 · REFERENCE Glossary CRM SSO Sources and authoritative references DISCLAIMER

§ HOW A SPECIALIST LABORATORY CAN ASSIST Working with Computer Forensics Lab Speak to a forensic examiner, not a salesperson. INSTRUCTTHELAB NEWENQUIRIESEMAILE - DISCOVERY

Questions and answers

A key witness says they have almost no relevant documents. Is that the end of it?

Often it is the beginning: the question "what documents do you have?" misses the applications where modern work is recorded (§2). Ask what platforms they work in all day (§3): the CRM, the project tool, the messaging app: and the record is usually there in quantity (Example 1's 400 interactions), with a change history and audit trail the witness never thought about.

How do we even find out what SaaS platforms a business uses?

By triangulation (§3): the identity provider or SSO lists sanctioned applications, end point exam in at i on finds installed and browser-used ones, network and CASB logs catch the rest, and expense and card records reveal the department a l and shadow subscriptions IT never sees (Example 2). No single source is complete; together they map the estate the asset register does not.

Can data in a CRM or project tool really be collected for disclosure?

Yes, as structured data (§5-§6): through the platform's export or its API, preserving the records, their change histories, comment threads and audit trails, and rendering them into review in a form that keeps the structure and context (§6's format problem). Flattening them to screenshots loses the very history and links that make them valuable; proper collection keeps them.

What makes the audit trail so useful?

It is the platform's own neutral record of who did what and when: created, viewed, edited, exported, deleted (§5,

The other side wants "all our HR system data". Do we have to extract everything?

No: proportionality applies to SaaS as to anything (§6-§7), and the sensible answer is targeted API collection: the relevant individuals' records, the relevant period, the change history and audit trail: agreed through the DRD (Example 3). Wholesale extraction is usually disproportionate, buries the relevant material, and mishandles special-category data; targeted collection produces the decisive records without it.

What if a record was changed or deleted in the app?

The platform usually remembers: change histories record who altered which field and when (guide 109's backdating logic for structured data, Example 1's softened note), and soft-deleted records sit in the platform's recycle store with the deletion logged in the audit trail (guide 106). What was removed from the app, by whom and whether it is recoverable, is established per platform, and the integration reflections (§8) may hold the pre- change copy besides.