Data Exfiltration To Cloud Storage

This guide assists UK lawyers in understanding data exfiltration to cloud storage. It covers tracing company data uploaded to personal and third-party clouds, examining the routes, records, and destinations of such transfers, and how to quantify and prove them.

e-discovery.uk, Computer Forensics Lab. Published 2026-08-31.
https://e-discovery.uk/library/data-exfiltration-to-cloud-storage

CLOUDEXFILTRATION · A GUIDE FOR UK LAWYERS Data Exfiltration to Cloud Storage Tracing Company Data Uploaded to Personal and Third-Party Clouds COMPUTER FORENSICS LAB

§ ABOUT THE AUTHOR PREPARED BY COMPUTER FORENSICS LAB E-DISCOVERY TEAM ESTABLISHED 2007 · LONDON ISO 17025-ALIGNED PROCEDURES CLOUD-EXFILTRATION INVESTIGATION SYNC-CLIENT & EGRESS ANALYSIS CPR PART 35 EXPERT REPORT S FULL CHAIN-OF-CUSTODY DOCUMENTATION

§ CONTENTS In this guide 01 Executive summary 02 The problem in plain English: the network copy that writes to both ends 03 The routes: sync clients, browser uploads, sharing, webmail and rules 04 The end point record: sync databases, browser artefacts and local traces 05 The platform and network record: audit logs, sharing events and egress 06 The destination: reaching the personal cloud account through process 07 Quantification, deployment and the innocent explanation 08 Source architecture: where else the evidence lives 09 Worked examples 10 Common mistakes and technical limitations 11 Questions to ask · Suggested wording 12 Checklist and red flags · When to involve a digital forensic expert 13 Frequently asked questions 14 Glossary · References · Disclaimer · How a specialist laboratory can assist

§ 01 · ORIENTATION Executive summary THE HEADLINE POINT: CLOUDEXFILTRATIONWRITESTOTHEENDPOINT, THE CORPORATE PLATFORM, THENETWORKANDTHEDESTINATIONACCOUNT: PROVEWHAT LEFTFROMTHEFIRSTTHREE, REACHWHEREITWENTTHROUGHTHEFOURTH, AND QUANTIFYTOAFILE - LEVELMANIFEST

§ 02 · FIRST PRINCIPLES The problem in plain English: the network copy that writes to both ends

§ 03 · THEROUTES The routes: sync clients, browser uploads, sharing, webmail and rules

§ 04 · THEENDPOINTRECORD The end point record: sync databases, browser artefacts and local traces

§ 05 · THEPLATFORMANDNETWORKRECORD The platform and network record: audit logs, sharing events and egress

§ 06 · THEDESTINATION The destination: reaching the personal cloud account through process 97

§ 7): what arrived, who accessed it, and its quarantine and return: the receiving side of the

transfer.

§ 07 · QUANTIFICATIONANDDEPLOYMENT Quantification, deployment and the innocent explanation

§ 08 · THEWIDERMAP Source architecture: where else the evidence lives QUESTION PLATFORM ACCOUNT + EMPLOYER ORIGINATING EGRESS BEHAVIOURAL END POINT (PROXY/ LAYER CORPORATE DESTINATION NEW AUDIT PROVIDER ESTATE NETWORK DLP/CASB)

§ 09 · IN THE WILD Worked examples EXAMPLE1 · THEPERSONALDRIVETHATMIRROREDTHEWHOLEDESK EXAMPLE2 · THEFOLDERTHATWASSHARED, NOTDOWNLOADED EXAMPLE3 · THESYNCTHATWASSANCTIONED, ANDTHECLAIMTHATNARROWED

§ 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 (the former employee / new employer) Ask your e Discovery / forensic provider (FIRST LETTER)

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

§ 13 · COMMON QUESTIONS Frequently asked questions The data went to a personal cloud account. Can we even prove it? The employee just shared a folder rather than downloading anything. Is that exfiltration? Can we get into the employee's personal cloud account? The employee had a sanctioned personal cloud for home-working. Does that defeat the claim? How fast do we need to move? Does the employer have its own obligations if client personal data left?

§ 14 · REFERENCE Glossary CASB DLP 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

The data went to a personal cloud account. Can we even prove it?

Yes, and usually well: the corporate machine's sync database or browser artefacts name the files and the account (§4), the platform audit log records the downloads or shares (§5), the network bounds the volume, and the destination account: reached through process: holds the material itself (§6). Example 1 was proven at both ends to the minute. The cloud feels elusive and is in fact doubly-recorded.

The employee just shared a folder rather than downloading anything. Is that exfiltration?

Squarely: sharing corporate content to a personal or external address, or creating a link and taking it away, moves the data to the employee's control without a d own load or a USB trace (§3, Example 2): and it is logged as a sharing event with the destination in the platform audit trail, which is why that log is exported first when downloads and USBs come up empty.

Can we get into the employee's personal cloud account?

Through process, not self-help: a preservation letter and undertakings first, then delivery-up and imaging orders, commonly via an independent examiner who reports only on your material and protects the employee's private data (§6, guide 97 §7): the account holds both the manifest and the files. Where the holder will not cooperate, the provider's records are reached by disclosure. Plan the route early; the account can be emptied in minutes.

The employee had a sanctioned personal cloud for home-working. Does that defeat the claim?

Only for what it sanctioned: the innocent-explanation pass (§7, Example 3) separates policy-permitted sync of the employee's working folder from unsanctioned transfers outside it, and the genuine exfiltration usually stands out clearly against the baseline. Running the pass first protects both sides: it narrows an over-broad claim to what will survive, and clears what was legitimate.

How fast do we need to move?

Same-day for preservation of the near-end evidence and the destination account: audit logs expire, the personal account can be emptied, and springboard relief dies of delay (guide 97 §7): Example 1's account still held everything because the letter reached it in the first week. The manifest can be built afterwards; the preservation cannot be redone.

Does the employer have its own obligations if client personal data left?

Yes: a transfer of client personal data to an uncontrolled personal account is a personal-data breach with UK GDPR not if i c at i on questions on the ICO's clock (guide 99 §6): assessed from the manifest's sensitivity classification (§7) as the investigation proceeds, not after. The exfiltration investigation and the breach assessment run together. cflab. u k · e-disc ove r y. u k