Building the Trust Layer

Article 2of 5

Why GDPR Can't Solve a Visibility Problem

One of the biggest misconceptions I encounter is that the introduction of the UK General Data Protection Regulation (UK GDPR) solved the problem of personal information.

It didn't.

It solved an important legal problem. It didn't solve the technical one.

Over the past decade, organisations have invested significant time and resources implementing GDPR. They introduced privacy notices, strengthened consent processes, reviewed retention policies, appointed Data Protection Officers and invested heavily in cybersecurity and compliance.

These were important and necessary changes.

Yet one question has remained surprisingly difficult to answer.

Where is this person's information right now?

At first glance, that sounds like a simple question. In reality, it exposes one of the biggest challenges in modern information governance.

Imagine an individual exercising their GDPR right of access.

As example they ask an employer:
"Please show me every copy you hold of every version of my CV."

Most organisations could identify information held within their core systems, such as:

- their HR platform;
- their Applicant Tracking System (ATS);
- email records; and
- documented personnel files.

But what about information that has moved beyond those systems? Can they also identify:

- archived backups;
- copies held by recruitment agencies;

- interview packs shared with hiring managers;
- documents forwarded to external consultants;
- files stored within cloud archives;
- local downloads onto laptops;
- shared network folders;
- third-party processors; or
- even temporary printer memory?

Often, the answer is no.

Not because organisations are careless.
Not because they have ignored GDPR.

But because they simply don't have complete visibility.

This is what I term **the Visibility Gap**.

GDPR establishes how personal information should be collected, processed, retained and, where appropriate, deleted.

It defines legal responsibilities and gives individuals important rights over their personal information.

What it cannot do is tell an organisation where every copy of that information exists at any given moment.

Legislation can establish accountability. Only technology can provide continuous visibility.

This distinction is becoming increasingly important.

A cybersecurity incident is not always the result of sophisticated hackers breaching a network. Sometimes the problem is much simpler.

- A forgotten copy of a document remains on an old server.
- A spreadsheet is downloaded onto a personal device.
- A CV is forwarded to another organisation and never deleted.

Nobody even realises the information still exists.

That is not simply a cybersecurity problem. It is a visibility problem.
Artificial Intelligence is now accelerating this challenge.

AI makes it easier than ever to create, analyse, summarise, copy and distribute information. Without better visibility, AI has the potential to multiply existing governance challenges rather than solve them.
T
his is where my thinking began to change.

Instead of asking how organisations could better manage millions of document copies, I started asking a different question.

What if we stopped distributing copies altogether?

What if individuals remained the owners of their information and organisations were granted secure, permission-based access instead?

Rather than attempting to track an ever-growing number of uncontrolled copies, organisations could know exactly where trusted information resides, who has access to it and when that access should end.

That thinking became the foundation for Resolut. Not as a replacement for GDPR, but as technology that complements it. Regulation establishes rights. Technology should make those rights practical.

Perhaps privacy is no longer our greatest challenge. Perhaps the real challenge is visibility.

A Question to Consider
If an individual exercised their right of access today, could your organisation confidently identify every location where their information exists, including every copy shared with third parties?

Next in the series
Building the Trust Layer - Article 3
The Business Case for Document Ownership

References

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Information Commissioner's Office (ICO): Guidance on the Right of Access, Data Controllers and Information Governance.