

Building the Trust Layer

The Hidden Data Supply Chain: Why Millions of People Have Lost Control of Their Most Valuable Documents

A LinkedIn Article by Chris Els

During more than three decades working with global payroll, HR and enterprise software platforms, I witnessed organisations invest enormous amounts of time and money protecting employee and customer information. Yet the more closely I looked, the more I realised something surprising.

Very few organisations could confidently explain where that information actually travelled once it left their immediate control.

Employee records moved between payroll providers, HR systems, pension administrators, insurers, regulators, recruitment agencies, software vendors, data centres and countless other third parties. Every transfer created another copy, another database and another organisation responsible for protecting someone else's personal information.

Nobody intended to create this complexity. It simply evolved as organisations digitised their processes one application at a time.

Over time, I came to think of this as a hidden data supply chain.

Unlike a physical supply chain, where goods can be tracked from manufacturer to customer, digital information often follows invisible paths. Copies are created, forwarded, archived and backed up across multiple systems, while the individual who owns the information rarely knows where it has gone or who now has access to it.

The recruitment industry provides a simple and familiar example.

According to the Office for National Statistics (ONS), the UK currently has around 720,000 active job vacancies and a workforce of more than 36 million people. Every year, millions of individuals change jobs or actively participate in the employment market, generating tens of millions of job applications. Each application involves sharing personal information with recruiters, employers and technology platforms that process and store those documents. Official statistics illustrate the scale of the employment market, even though no central authority measures how many copies of those documents are ultimately created.

Consider what happens when a candidate submits a CV.

A recruiter stores it in an Applicant Tracking System. It may then be forwarded to several employers. Each employer may upload it into their own recruitment platform, circulate it

to hiring managers, include it within interview packs, retain it for future vacancies and protect it through backup and disaster recovery systems.

One CV can quickly become many copies.

Multiply that process across millions of job applications each year and it becomes reasonable to conclude that hundreds of millions of employment-related documents exist across recruitment databases, employer systems, email servers and cloud storage platforms.

During a recent discussion, respected cybersecurity commentator Lou Covey described these uncontrolled copies as 'digital litter', a phrase that perfectly captures the unintended accumulation of personal information across countless systems.

Not because organisations are careless, but because our current way of sharing information is based on distributing copies rather than controlling access to the original source.

This matters because every additional copy creates another governance obligation, another privacy exposure and another potential cyber security risk.

The introduction of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 significantly strengthened the rights of individuals and the responsibilities of organisations acting as data controllers. The Information Commissioner's Office (ICO) has consistently highlighted information governance, inappropriate data sharing and inadequate organisational controls as recurring areas of concern through its guidance and regulatory activity.

The legislation gives individuals important rights over their personal information. The practical challenge is that those rights become increasingly difficult to exercise when information has been copied across numerous independent systems and organisations.

Recruitment is only one example.

The same pattern exists in healthcare, financial services, education, government, legal services, insurance and increasingly throughout global supply chains. Qualifications, licences, certifications, contracts, identity documents and compliance records are continually copied and redistributed because our systems have been designed around document exchange rather than controlled information sharing.

This raises a simple question.

Why are we still sending copies of documents when modern technology allows us to share secure, permission-based access to information instead?

That question became the foundation for Resolut.

Rather than asking how we could build another document management system, we asked a different question entirely:

What if the owner of information never had to lose control of it in the first place?

The answer is not simply better storage or stronger encryption.

It is replacing uncontrolled document distribution with controlled, auditable access.

Recruitment illustrates the problem because everyone understands it.

The opportunity, however, extends far beyond recruitment.

It reaches every organisation that relies on trusted information moving between people, businesses and regulators.

Perhaps the next evolution of digital transformation is not about creating more data.

Perhaps it is about finally giving people back control of the data they already own.

A Question to Consider.

If you asked every organisation that has ever received a personal document from you to prove where every copy is stored today, could they?

Next in the series

Building the Trust Layer - Article 2

Why GDPR Can't Solve a Visibility Problem

References

Office for National Statistics (ONS): *Jobs and Vacancies in the UK and Workforce Jobs*.

Information Commissioner's Office (ICO): UK GDPR guidance for organisations and published guidance on controllers, processors and information governance.

UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

