

# DSARs and FOIA Requests Made Easy

## eDisclosure uses include:

- Civil litigation
- Employment tribunals
- Data subject access requests (DSARs)
- Freedom of Information Act (FOIA) requests
- Public inquiries
- Major investigations
- Serious case reviews
- Criminal Procedure and Investigations Act (CPIA) compliant reviews
- Internal investigations
- Regulatory (e.g., FCA, CMA, Judicial) reviews

## Benefits of eDisclosure include:

- Increase public confidence due to greater transparency and standardised processes
- Improved compliance, which leads to a reduction in risk
- Stronger accountability with audit trails of decision making
- Access to integrated analytics and AI tools
- Increased security, due to permission-based access controls

The UK public sector has been undergoing a period of sustained change and financial contraction. Public sector leaders are experiencing financial pressure as never before, alongside an increasing demand for essential services. At the same time, the public sector in the UK is creating, sharing and securing more electronic data than ever. This is driven in part by a growing public appetite for transparency and accountability from society's central institutions.

Managing information, particularly for the purposes of legal processes and disclosure can be highly resource-intensive and pose significant legal risk to already stretched public service resources. Where data needs to be processed and shared as part of a legal process, specialist technology platforms are frequently used to ensure that this work is done rigorously and efficiently. The term eDisclosure (or sometimes eDiscovery) is used to describe the systems, processes and practices associated with this work.



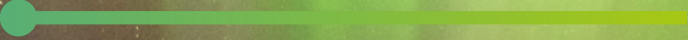
# Contents

Recognising the Challenge of DSARs and FOIA Requests .....3

Our Experience.....6

Data Security.....8





# Recognising the Challenge of DSARs and FOIA Requests

Many public sector organisations face the challenge of increasing volumes of public records requests, greater digital data complexity, and stringent privacy and data protection rules under the GDPR and the Data Protection Act. The processes surrounding responding to these can be time-consuming and cumbersome. Finding the relevant documents across all systems (including multiple email accounts, Teams, Slack and shared drives) is complex. Once found, the redaction (and the risk of being reversed if done incorrectly) and disclosure process can be arduous. Studies have shown that 70-80% of collected materials are duplicates, which adds an extra layer of complexity and adds unnecessary volume to the task. Undertaking these tasks within the statutory deadlines on potentially thousands of sensitive documents is a significant burden for public sector organisations.

## Enabling Stress-Free Data Compliance

Our service reduces the burden of managing data requests through our simple, rapid and robust process. We will bring peace of mind through our service, which is focused on both safety and savings. By introducing intuitive automation through our state-of-the-art DSAR/FOIA service, we can reduce the heavy burden of manual tasks on your team and eliminate duplication. Our software platform streamlines data collection from diverse sources, collates that data, reduces errors, and applies robust redactions for sensitive and exempt information. This simultaneously lowers your operational costs, alleviates pressure on overworked staff, supports on-time delivery, and shields your organisation from risk.

We believe you deserve to see the whole picture, which is why our intuitive dashboards show every step of your journey, providing total process transparency, trust and full compliance. Our innovative technology enhances accuracy — spotting details the human eye might miss — and navigates regulatory timelines with confidence and ease.

## How Our Service Works

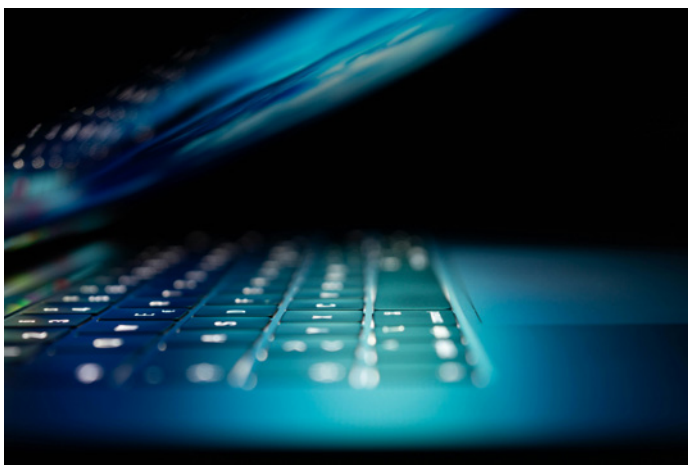
We understand how overwhelming high volume and unpredictable FOIA/DSAR requests can be. Navigating the complexities of DSARs and FOI/FOIA enquiries need not be stressful. We have designed our service to be your capable partner, transforming a typically disjointed and manual obligation into a streamlined, automated, and secure workflow. We guide you through a simple, standardised process that removes the heavy lifting from your team, ensuring accuracy and peace of mind from start to finish.

Our proprietary workflows and tools are designed specifically for DSAR and FOIA requests. These are embedded within RelativityOne, the market-leading platform for this work. By combining our knowledge with the best in today's technology, our service simplifies deduplication and ensures robust redaction, all in an easy-to-learn interface that supports productivity.

**Centralised Intake and Identity Verification:** We provide a single, centralised platform to operationalise all data subject requests, allowing you to track and monitor every case in one place. To protect you against fraudulent enquiries, we simplify identity verification using industry-recognised methods, ensuring you are engaging with the correct individual before any data is processed.



**Intelligent Discovery and Collection:** Once a request is validated, our discovery tools go to work. We reach across your entire digital landscape, scanning on-premise systems, cloud platforms (e.g., Office 365 and SharePoint), databases, and file systems to locate every trace of relevant personal data. For organisations with physical archives, we can even capture and digitise paper files, microfiche, and other non-digital formats, converting them into a consistent, searchable digital format. This automated retrieval ensures comprehensive coverage without the need for manual hunting through folders.



**Automated Redaction and Review:** Protecting third-party privacy is where our technology truly shines. Using AI, our service automatically detects and highlights sensitive Personally Identifiable Information (PII) across all documents. Our “Sensitive Data Scan” and PII Tools automatically identify, extract, and redact sensitive information without opening documents. We can apply bulk redactions to sensitive keywords or data types and propagate redactions across duplicate documents, significantly reducing the risk of human error. For absolute security, we offer “burnt-in” redaction capabilities, ensuring that once data is hidden, it cannot be uncovered by the recipient.

**Secure Delivery and Audit:** Finally, we help you respond to DSARs and FOIAs with confidence. The solution provides standard reports that give an overview of data upon ingestion, helping teams understand the key data types relevant to the request. You can compile the final response and deliver it via a secure, encrypted web portal, or digitally publish it with your organisation’s preferred branding. Throughout this process, the system maintains a rigorous, defensible audit trail of every action taken, ensuring you remain fully compliant with regulatory timelines and can demonstrate your process to auditors if required.

By blending AI with intuitive human oversight, we turn a high-risk compliance task into an effortless, repeatable standard for your organisation.

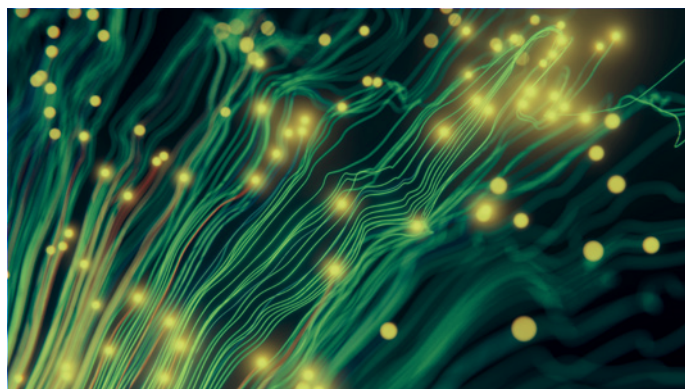
## Streamlining Collections from Office 365

The integration of Purview Sync provides a streamlined “fast lane” for moving complex data from Microsoft 365 directly into a review-ready environment. By automating the migration process, teams can bypass traditional, error-prone manual exports and FTP staging. This seamless connection ensures that challenging data types, including Teams chats, Copilot interactions, and encrypted files, arrive with metadata intact and formatted for immediate analysis.

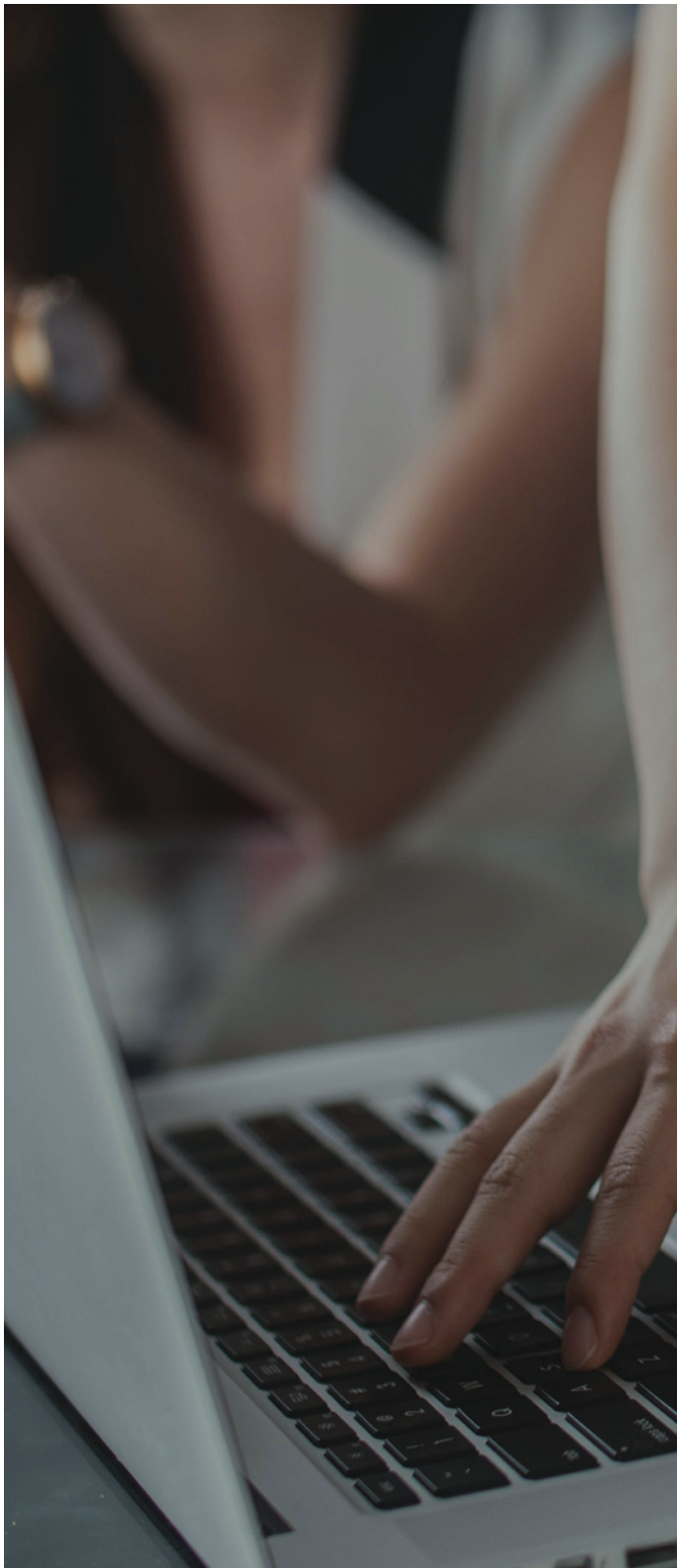
Operating entirely within the secure Azure boundary, Purview Sync maintains strict data integrity and permission models throughout the transfer. This innovative approach drastically reduces timescales from weeks to mere hours, allowing organisations to focus on strategic legal work rather than data management. Ultimately, the solution offers a faster, more secure, and defensible path from collection to disclosure for modern enterprise data.

## The Benefits of AI

The implementation of AI DSAR workflows offers a transformative advantage for organisations facing increasingly complex requests. By moving beyond traditional keyword searches, generative AI understands context, effectively distinguishing between meaningful discussions of a data subject and irrelevant mentions. This capability significantly reduces the volume of data requiring human intervention, allowing compliance teams to focus solely on pertinent information while ensuring that the response remains proportionate and cost-effective.



One of the primary benefits of AI is its ability to accelerate turnaround times, often cutting review periods by more than half. This is particularly so, as the Information Commissioner’s Office (ICO) maintains strict one-month deadlines and has heightened scrutiny over incomplete or delayed responses.



Providing clear natural-language rationales and direct citations for every AI-generated decision, ensures that the process is transparent and easily auditable. This rigour allows organisations to meet their statutory obligations with greater confidence and precision.

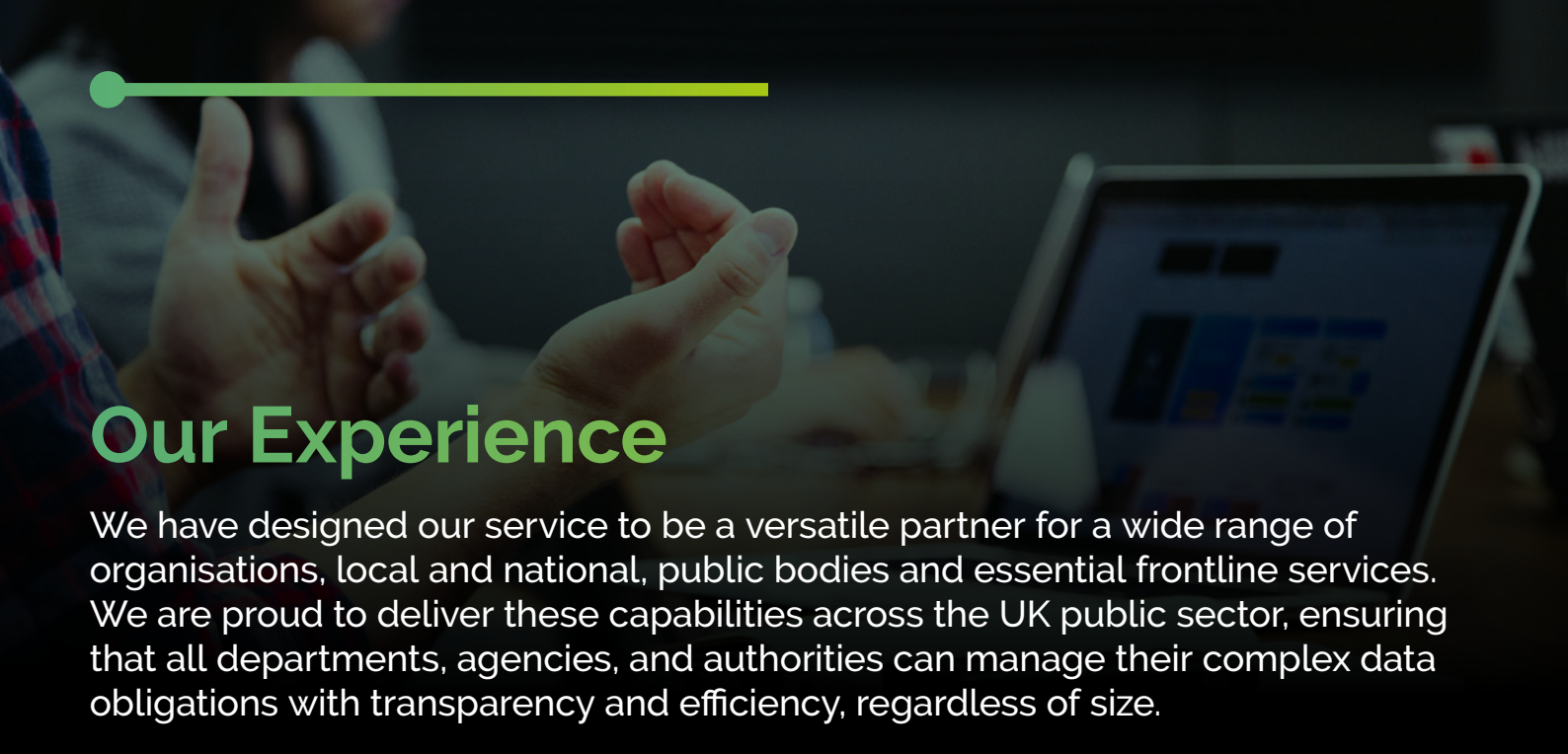
AI streamlines the DSAR lifecycle, for example, by identifying third-party personal data and managing complex redactions. By automating the detection of personally identifiable information and confidential business content, we ensure that disclosures are accurate and protect the privacy of others.

## Onboarding and Delivery

For continuous engagements, we define a straightforward onboarding process at the outset of the relationship to ensure we can establish cases with minimum delay. We consider various issues, including the scope of the matters being addressed, start-up meeting requirements, and any contractual or compliance issues. Having an agreed process in place allows all matters to commence in a robust and repeatable manner.

We take time to establish key contacts for each party and to determine the user skill levels and training requirements. As part of our best-practice approach, we use checklists that cover aspects such as processing specifications, deduplication requirements, search-term reporting, workflow and coding requirements. Our team provides comprehensive support throughout the life cycle of every matter, and our clients have direct access to our experienced security-cleared team of technical project managers.

Our platforms have logical user security and full audit trails. All systems are configured in accordance with the principle of least privilege. We restrict all user accounts to named individuals. Our platform features customisable permission levels, ensuring ease of use by providing only the features, work products, and documents that users need, commensurate with their role. We can easily adjust access as experience grows. Allocation to roles is done by job role rather than individually, with the Buyer's agreement.



# Our Experience

We have designed our service to be a versatile partner for a wide range of organisations, local and national, public bodies and essential frontline services. We are proud to deliver these capabilities across the UK public sector, ensuring that all departments, agencies, and authorities can manage their complex data obligations with transparency and efficiency, regardless of size.

We work closely with Health and Social Care Teams. We understand the critical sensitivity of clinical and patient-specific data, supporting NHS Trusts (acute, community, mental health and ambulance trusts) and care providers in handling complex Subject Access Requests involving Electronic Patient Records and inpatient data. Our tools are tailored to help these organisations navigate high volumes of requests while maintaining strict confidentiality and patient trust.

We partner with the Education sector. Universities, colleges, and schools can utilise our services to manage student and staff data, often benefiting from dedicated educational pricing structures to ensure robust compliance remains affordable.

Local authorities and government departments utilise our services to manage their public disclosure requirements. These teams implement our technology to improve efficiency, enabling them to meet deadlines more consistently and hit response-time thresholds.

The Defence, Security and Justice sectors also trust our service. We support legal teams, tribunals, and arbitration bodies in managing inquiries, investigations and regulatory matters. Furthermore, we extend our technology to the third sector, assisting non-profits, charities, journalists, and pro bono legal programmes to access enterprise-grade tools that support their work.

From local authorities reducing processing time to private-sector firms managing litigation, we empower Data Protection Officers, HR teams, and legal professionals to move away from manual processing and focus on what matters most.

## Example: Legal Services Company DSAR

We supported a Legal Services provider with a significant DSAR redaction exercise involving 10,000 Excel files, with a tight deadline and a rigorous redaction process required. We used Blackout, an automated redaction tool, alongside a keyword workflow. We supported the project by having members of our Managed Document Review team work alongside the client's own lawyers. We completed the entire exercise in under two weeks and kept under budget.

## Example: UK Health Security Agency FOIA Request

We worked with the UKHSA to expand their previous use of our platform on public inquiry work to other teams within the agency. We developed a specific FOIA workflow, which has been used on more than a dozen matters and has successfully reduced the time to respond to requests from weeks to days.

## Example: Independent UK Law Firm and Public Sector Clients

We work alongside a large UK law firm, supporting them in all their DSAR and FOIA requests. This work includes helping their client, the UK Atomic Energy Authority, over the last two years.

## Staff Clearances and Security

We clear all our eDisclosure staff to SC level, and when recruiting, we seek candidates who are willing to be vetted to the DV standard where this is required. Pre-employment, we conduct a comprehensive check of identity, right-to-work status, criminal records (DBS), UK financial status (5 years), and employment history (3 years) for all employees. This meticulous process is fully compliant with the Baseline Personnel Security Standard (BPSS). We perform rolling annual checks thereafter to ensure continuous commitment to your data security. A specialist industry-leading third-party provider completes these on our behalf.



We take an active role in ensuring our ongoing compliance with our vetting and security obligations. Each quarter, we ask our staff to provide updates (or “no change”) on matters that might affect their SC clearance (e.g., any change in cohabitation). This transparent approach ensures that we report any amendments back to the relevant authorising body immediately, keeping them informed and involved.

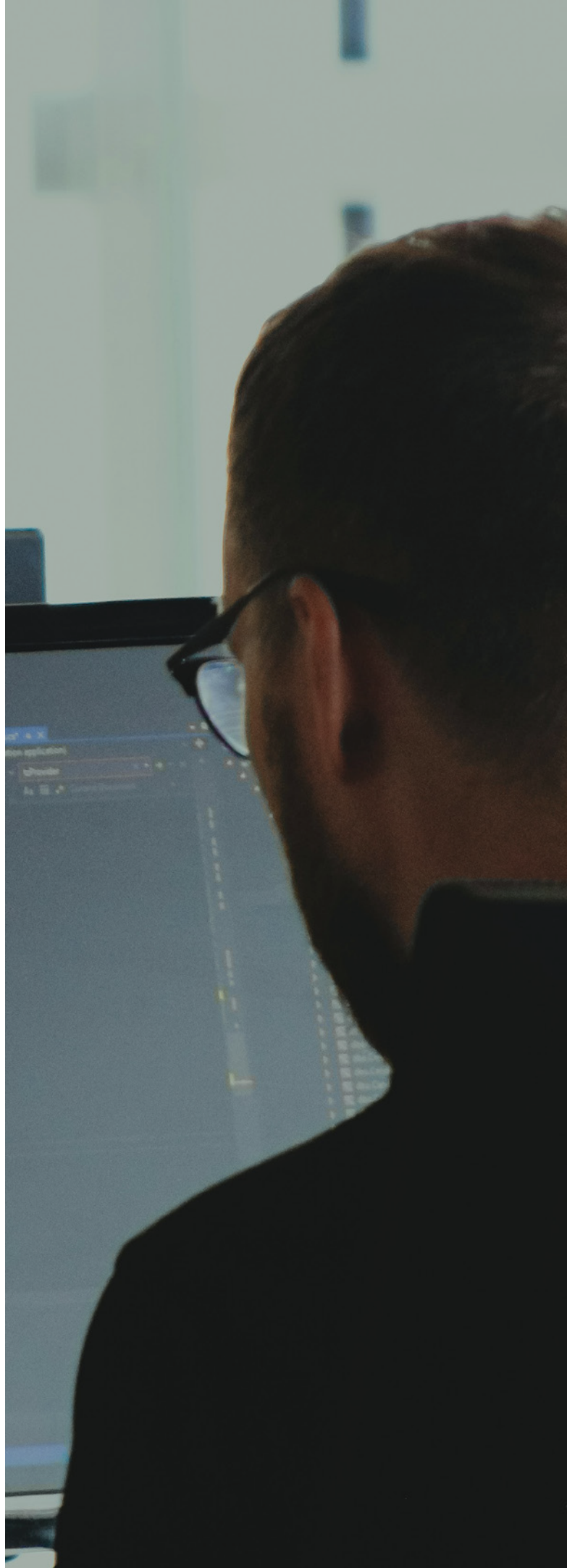
Our rolling HR Security Audits also check the clearance status of all staff quarterly, so we identify any expiring clearances and renew them promptly. Our operational practices retain work that may require clearance within our business, so vetting within our supply chain is unnecessary.

We routinely perform projects with contract-specific security requirements, including specific NDAs. To ensure staff integrity, every project staff member must undergo project-specific information security training and sign a security aspects letter (SAL) that draws their attention to the project’s security requirements. Staff must reassess and re-sign the SAL every six months, reconfirming their understanding. Any changes in scope mid-project result in complete retraining of the team on all aspects of security.

Our Information Security Management System underscores the crucial role of each staff member in maintaining our system security, data handling, and acceptable use policies. It requires that all staff sign to confirm their understanding and acceptance of our policies. We provide annual online training, testing, and accreditation to all staff, emphasising the significance of their role in information security, data privacy, GDPR, system security, and data handling and acceptable use.

Junior staff members are guided and supported by senior staff with extensive experience in delivering services that require adherence to information security best practices. We nurture information security awareness through regular knowledge sharing, seminars and conference attendance, supplier training courses, and audit performance. Conformance with security and confidentiality training is tracked by HR, providing our leadership team with constant visibility and ensuring that junior staff feel supported and guided in their journey towards information security excellence.

All our eDisclosure and Digital Forensic consultants hold degrees in Computer Forensics or Computer Science. Thereafter, we train them to have an advanced understanding of the fundamental importance of system security, data handling, and acceptable use policies, and how these are implemented and achieved in practice.





# Data Security

Our Data Protection registration number is Z1951856. We were first registered on 16/10/2009, and our registration expires on 15/10/2026.

From our extensive experience in handling sensitive data for the public and private sectors, we recognise the importance of secure data handling and hosting. We use secure cloud hosting for our services, which complies with all the stringent security standards you would expect from a provider to the NHS, government (central and local), education institutions and legal organisations.

We understand that data security is paramount in responding to DSAR and FOIA requests. We will draw on our expertise to ensure the highest level of data protection and eliminate the risk of human error when handling this sensitive data. Our robust data protection and security measures improve transparency and accuracy while reducing the risk of data breaches.

All personal data processed by Anexsys is within the scope of our Data Subject Access Request (DSAR) process. We maintain a formal DSAR policy to handle any requests from data subjects when we act as the data controller. Our Privacy team (comprised of members from the Legal and Information Security departments) handles all DSAR requests received. Data subjects are entitled to obtain from the Controller:

- Confirmation as to whether Anexsys is processing personal data about that individual
- Access to their data
- Any related information
- The logic involved in any automated decisions relating to them

The Data Protection Owner is responsible for the application and effective operation of this procedure and for reporting to the information owner (company directors) on DSARs.

In terms of our service, Anexsys acts as a Processor only, acting on the Buyer's instructions, who is the Controller of the personal data being processed. Anexsys acts as a Controller only with respect to the limited data collected about the Buyer to manage the service (such as email addresses for communications) and internal data relating to Anexsys staff.



# Background to Anexsys

Anexsys was established in 2004 and offers dedicated outsourced services to law firms, corporations and the public sector. Anexsys provides services including data collection, computer forensics, data processing, document hosting, managed services and outsourced review. All our facilities are ISO 9001, 14001 and 27001 accredited and Cyber Essentials Plus certified.

Anexsys is a division of Consilio, a global leader in eDisclosure, document review, risk management, and legal consulting services. Consilio supports governments, multinational law firms and corporations using innovative software, cost-effective managed services, and deep legal and regulatory industry expertise. Anexsys focuses on UK government and police force clients, who require additional data restrictions.

All Anexsys eDisclosure staff are cleared to at least HM Government SC and NPPV3 level. We are trusted to handle government material at Secret and Top Secret level. We are one of only a few companies able to supply the full range of litigation support services, ranging from digital forensics and collection (using forensic professionals with expert witness experience), through to data processing and document hosting, as well as managed document review and hard copy services.

For two decades, Anexsys has built on a wide array of technological solutions to deliver innovative, customised eDiscovery environments. Anexsys holds a large infrastructure footprint, covering all the leading platforms and complementing them with its own proprietary software. These proprietary solutions include advanced generative AI initiatives and custom tools to manage modern data, such as streamlining the review of chat logs (e.g., Slack and WhatsApp), providing transcription for audio and video files, and proprietary bundling solutions. This capability ensures that our workflows are constantly evolving to provide our clients with optimal efficiency and defensibility.

## Contact Us

### London

0203 217 0300  
6th Floor  
24 Chiswell St  
London EC1Y 4TY

[anexsys.com](https://anexsys.com)  
[info@anexsys.com](mailto:info@anexsys.com)