Crown Commercial Service *Supplier*

anexsys

Revolutionise your Dispute Practice with TrialView's AI Litigation Software

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 rigourously and efficiently. The term eDisclosure (or sometimes eDiscovery) is used to describe the systems, processes and practices associated with this work.

Contents

High Impact Disclosure Scenarios 3
The Electronic Discovery Reference Model (EDRM) 6
Aurora Overview 9
Use Cases 10
Aurora Key Features 11
Aurora Ecosystem Overview 13
Staff Clearances and Security 14
Scoping and Ordering 16
Data Security 17

High Impact Disclosure Scenarios

Here are some practical examples of how eDisclosure services could be of benefit to your organisation.

Public Inquiries, Serious Case Reviews and Major Investigations

A devastating public safety incident takes place, and your organisation has been involved in providing services to those involved before, during, and in the aftermath of the event.

There could be relevant information spread across numerous corporate and individual systems, geographic and specialists teams. There is likely to be relevant material which exists within your organisation, that you may not be aware of without a physical and technical scoping or mapping exercise. The relevant material may relate not just to individuals, but to the functioning of entire teams and the strategic decision-making at executive level. The number of relevant documents could be over 100,000, drawn from a pool of tens of millions and range from published policy documents to mobile phone text messages.

Bespoke Workspace Design

Our platform provides workspaces that grow with the matter, which may last for several years and change in scope throughout that time. The workspace includes features such as:

- **Automated document processing and data extraction**, which helps reduce the manual effort required and makes it easier to conduct effective analyses
- **Advanced search and analytics capabilities** make it easy to quickly find and analyse the most important data, using tools like email threading, concept searching, and automated document clustering
- **Collaboration and communication tools** make it easy to share documents and information with internal and external teams, and includes features like document tagging, annotations, and notes
- **Document review tools** like redaction, bespoke coding and privilege logs make it easy to review documents quickly and accurately
- **Production and presentation tools** include features like document bundling and PowerPoint presentations, to make it easy to create and present documents in court

Our platform retains the source identifiers and location details of every document, to provide a global view of all material that has been identified as relevant; and when, where and how that material was collected. This continuity trail is particularly crucial in public inquiries; when the source, circulation and dating of a document is often as important as the document itself.

Fully Auditable, Legally Defensible Document Handing

Our platform protects documents from subsequent changes and provides a full audit trail of every user's interactions with the document set and the platform. This provides complete peace of mind, with processes that are recognised as fully compliant with legal and court requirements.

Employment Tribunals

A former member of staff from your organisation alleges that they were subject to discriminatory treatment over a five-year period.

The staff member believes that the management of their performance at work was discriminatory on the basis of their protected characteristics under the Equalities Act 2010. In their statement, they cite comparisons with the treatment of five other colleagues over the same period as evidence of their adverse treatment using examples such as volume, length, timing and tone of communications, as well as the quantity and quality of the work itself. All members of staff are engaged with front-line service delivery, and have had thousands of interactions with the relevant manager across several systems over the cited period.

Timeline Visualisation

Timelining tools can quickly build an accurate picture of the member of staff's interactions with their supervisor, arranging interactions dispersed across channels such as text messages, email and corporate system case management notes into a meaningful chronology. Timelining rapidly decreases the time required to make decisions, increasing confidence and reducing cost.

Early Data Assessment

Our platform provides a wide range of tools that allow legal teams to quickly understand significant data sets and summarise the supervisor's activities over the period, including all management communication and task allocation. Concept clustering uses linguistic and statistical methods to group related words, phrases, and documents into clusters that can then be used to classify the documents, identify topics, and uncover evidence. Sentiment analysis can be used to determine the emotional tone behind a piece of text and gauge the opinion of the author. Rapid insight into the case, gained through tools like these, enables quicker decisionmaking on whether or not to defend the claim. These and other early data assessment techniques bring the most impactive or significant data to the surface, enabling faster, more empowered legal decision-making.

Data Subject Access Requests & FOIA Requests

A journalist is working with interested members of the public, exercising their rights under the Data Protection Act 2018, the General Data Protection Regulation 2018, and the Freedom of Information Act 2000.

Your organisation has provided a reduced scope of information to date under Section 8(2) of the Act, due to the disproportionate effort required to locate the further known material. An appeal has subsequently been made to the Information Commissioner, citing technical advances which reduce that disproportionate effort. The ongoing appeal and disclosure requests result in adverse media comment regarding the apparent transparency and information law compliance of your organisation.

Specialist Support

Our eDisclosure consultants can forensically collect, sift and sort even the most unstructured of shared drives and unregistered data repositories. Our workflow specialists can design efficient, defensible processes. Our review teams can examine the document set quickly to determine how much material should be released, and what redactions need to be applied.

Redaction Solutions

The nature of personal data within public sector organisations means that redaction to protect the privacy of any third-parties is almost always a crucial activity whenever material is to be released. Manual redaction relies on human accuracy and processes that are often circuitous, leaving room for error and confusion. Our platform applies redactions to documents securely, with customisable features and a full audit capability. It removes the need for risky workaround processes such as 'flattening' black highlight text onto re-saved PDF documents, which can then be removed with PDF editing software.

Civil Litigation

A member of the public alleges that your organisation has failed in its statutory duties by knowingly allowing a factory to discharge waste into a waterway that is adjacent to a school.

They cite five to ten individuals whose work may be relevant to the alleged systematic failure covering a period of five years. Relevant documents are emails, documents, meeting minutes, shared drives and numerous, complex entries on your organisation's case management system, call handling and other information management systems. There are likely to be over 1,000 relevant documents to this claim.

Forensic Collections

Our team can be deployed rapidly across the UK, with high-quality and pre-prepared forensic collection kits capable of collecting data from a range of digital devices. We operate to ACPO standards and have experience in leading collections to both criminal and civil standards. We are able to react quickly to urgent or unexpected collections.

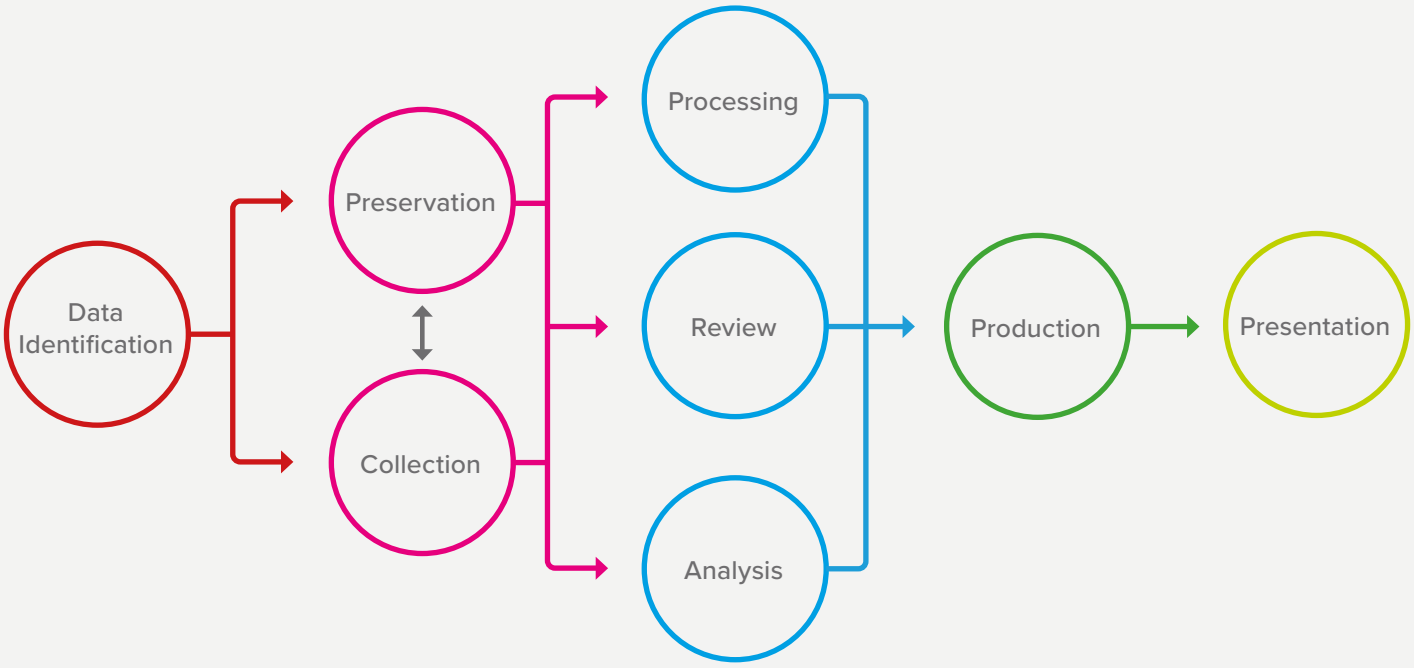
Global Data Search Capacity

Our platform allows all documents to be held centrally, regardless of their file type or where they were originally stored. This allows all documents to be searched at once, which is quicker and ensures that no systems are missed. Our advanced search tools are far more effective than general operating system search, and incorporate fuzzy matching to include near hits and common spelling errors. This reduces the volume of documents returned while also reducing the probability of relevant documents being missed. It is then easy to trace where a document originated, as original file structures and mailboxes are locked down.

Search Term Reporting and Audit History

Litigation in the public sector often involves highly emotive topics where a lack of organisational trust has become a factor. Our platform produces search term reports that can be used to demonstrate the process followed, the exact searches applied, when and to which data sources. Every key stroke is retained, traceable and reportable through comprehensive audit logs.

The Electronic Discovery Reference Model (EDRM)



The EDRM is the internationally accepted process by which electronically-stored information (ESI) is brought in and managed through legal processes, with a focus on civil litigation. Duke University School (US) is the leading institution for EDRM development, research and innovation. Further resources can be found here (edrm.net, 2017).

Data Identification

The first step is to determine what data exists, where it is and identify the correct process to collect it. The process of scoping and identifying all locations and formats for relevant data may include speaking with key organisational stakeholders who are able to identify the systems and individuals who will need to be involved.

This may involve interrogating legacy (mothballed) systems that have been replaced through subsequent IT infrastructure roll-outs. Depending on the context of the requirement, applying search terms that 'corral' relevant data is an appropriate technique that reduces the scale of subsequent work. For example, in the case of a Subject Access Request it is sensible to limit data to all emails where the data subject is explicitly named.

Data Preservation

Where issues of organisational confidence and integrity are central to a legal process or claim, ensuring procedural rigour in collection of data is essential.

The same principles apply to the retrieval of any type of document from archive boxes to 'Internet of Things' device data extracted from smart speakers like the Amazon Echo. The objective is to isolate and protect potentially relevant data from alteration, destruction or modification. While it is possible to extract and process entire mailboxes or file systems, (dependent on the nature of the disclosure or the purposes of the search) careful and forensic search term identification and collection can be more appropriate. Understanding data storage from the point of view of a computer scientist or computer forensic expert is essential in order to collect and report data with sufficient legal defensibility.

Data Collection

Collecting data must always take place securely, whether it is on site in your organisation, remotely via a web-based screenshare, or within a secure digital forensic laboratory.

We use the same chain of custody procedures and evidence bags that are used in police work to ensure continuity and integrity of data. A wide array of techniques are used, driven by the format of the data, from scanning and coding of hardcopy documents to the logical and physical imaging of hard drives to capture electronic documents and conversation threads in WhatsApp, Slack and SMS.

Data Processing

Processing converts the data that has been collected into a format that is appropriate for the subsequent work in a forensically sound manner.

This requires separating attachments from emails, expanding ZIP files, extracting metadata to make it searchable, deduplication and removing irrelevant system and application files. These processes bring down the number of documents that are required in subsequent stages. This reduces review labour costs and may also reduce the volume of data that needs to be hosted.

Review

This stage involves selecting appropriate documents to move forward to analysis and ultimate disclosure and disregarding ('demoting') irrelevant data in an industry-accepted and legally-defensible manner.

The challenges of review often centre on the ability to scale and equip large teams of reviewers at short notice, and then to ensure that those teams are engaged as productively as possible in the performance of the review. Reviews may last only a few weeks, or may continue over several years; often with a highly variable and unpredictable workload. Processes need to be tailored to the needs of the client and the matter, all delivered flexibly and with complete traceability and defensibility.

Defining and applying a cohesive review methodology, supported by innovative, yet tested technical enablers, means that large volumes of material can be sifted, sorted and assessed within short timeframes. We prepare a briefing document that captures the specific purpose of the matter, details any relevant background information and the key issues for consideration. Once reviewed and agreed with the client, this then forms the basis of the training delivered to the review team.

Real-time reporting on the size of the data enables the scale of work to be performed to be understood and a defensible and appropriate collection strategy defined. It also allows legal teams to make informed applications and give realistic, achievable undertakings to the internal and external stakeholders for the matter.

eDisclosure workspaces can be created within our platform that allow hundreds of documents to be reviewed each day. Workspaces, decision prompts and tagging actions are all easily customisable to the matter-at-hand.

Some clients prefer to conduct the review itself using their own staff. In these circumstances, we can help by delivering targeted review training to client review teams to ensure that they are productive and efficient.

Some clients outsource this work to us. There are several reasons why this may be the case. Examples include the importance or complexity of the matter meaning that it requires specialist expertise, or its size and scope being beyond the capacity of the client's own resources.

When conducting reviews on behalf of clients, we tailor our teams to suit review requirements. We will often use a mix of qualified lawyers and legally-qualified reviewers that have previous experience in the field relevant to the matter. Using lawyers allows rolling, in-depth analysis of review decisions, ensuring accuracy and consistency in decision-making. Our teams include NPPV3/SC cleared reviewers and review managers, enabling us to handle sensitive materials without delay. Through monitoring the productivity of the team and scaling the team accordingly to item volumes, we control cost and operate within agreed budgets.

Analysis

Powerful technological techniques determine the key information; topics, critical individuals, specific vocabulary and relationships.

Analytic techniques quickly distil, connect and clarify communication to reveal what was known, by whom and when. Our platforms use advanced analytics and artificial intelligence to streamline document review. Techniques such as email threading and textual near-duplicate identification significantly reduce review volumes by removing redundant content. Organising documents thematically allows teams to identify key issues without relying solely on keywords. Machine learning tools like Continuous Active Learning and Generative AI prioritise relevant documents and predict coding decisions. These innovations enhance accuracy and consistency while delivering substantial time and cost savings.

Production

The scope of the 'handing-over' process may be large or small, soft or hardcopy. Full original files (called 'natives') may be provided, or images with redactions applied to mask irrelevant content.

Smaller productions (*e.g.*, 75 redacted emails from a data subject access request) may be supplied in the form of a bound hardcopy document. Larger productions (*e.g.*, 900 files including emails, Word documents and database exports for a civil claim within a tribunal) may be supplied in an archive format such as ZIP. The largest productions (*e.g.*, 150,000 native files forensically extracted from a department's SharePoint and filtered for relevance) may be supplied in our platform's own format, as this supports subsequent analysis by the receiving party (by *e.g.*, a public inquiry team). We can also provide productions in multiple formats simultaneously (*e.g.*, hardcopy for individuals and different platform formats for each of the 'other side' legal team and public inquiry team).

Presentation

The data is then reviewed by the party in receipt of the production in order to determine which elements to present in the proceedings.

Depending on the case, the evidence might be presented as digital media, hardcopy or orally. This may require defence explaining the origin and chain of custody applied to the evidence, as well as any processing and filtering subsequently applied. This ensures that the evidence is presented in a way that is understandable and aligned with the legal requirements for admissibility.

TrialView Overview

TrialView is an AI-powered solution designed to revolutionise your litigation workflow and dispute resolution processes. Our robust platform has been built by lawyers, for lawyers, to streamline your case preparation, enhance your courtroom performance, and maximise your chances of success. With features including bundle creation, transcription, collaborative workspaces and interactive evidence presentation, we're passionate about mapping out a future where litigation is more seamless, cooperative and efficient.

TrialView Organises Litigation

TrialView's AI workspace addresses one of the sharpest pain points in hearing preparation. It provides a centralised platform that bridges the gap between disclosure and bundle preparation, offering a host of benefits.

TrialView eradicates the friction points of typical hearing preparation. TrialView's centralised platform facilitates seamless communication and information sharing among team members, regardless of location. It avoids duplication of communication and document sharing by engaging a single source of truth throughout the litigation process. It streamlines routine tasks such as pagination, indexing and hyperlinking, ensuring compliance with court standards while enhancing collaboration.

TrialView can automatically categorise, tag, date, and analyse documents as they are uploaded, making it easier for legal teams to find relevant information and identify potential issues. Its AI can analyse communication patterns, ensuring that crucial information is not missed and that all team members stay informed. Moreover, AI can identify insights and connections that the human brain may overlook. By empowering users to quickly and easily find relevant facts within large volumes of documents, inconsistency detection is feasible and fast.

AI excels at rapidly processing large datasets and extracting the most useful information. It can work across entire bundles of documents or through specifically selected groups of documentation, pulling out the salient and highlighting patterns and insights. This kind of data interrogation would take a typical lawyer hours to complete manually; with AI, it can take as little as seconds or minutes.

TrailView Key Features

Our AI tools rapidly detect patterns, uncover inconsistencies, and highlight key information from case materials. You can use it to ask questions about the evidence, the strengths of your client's case and the weaknesses of your opponent.

TrialView automates the creation of hyperlinked, court-compliant bundles, drastically reducing time spent on case preparation and ensuring all materials are organised and ready for any proceeding.

TrialView provides an intuitive platform for real-time, dynamic evidence presentation. With instant access to hyperlinked documents and intuitive navigation, you can respond agilely to arguments and present your case with seamless precision during any session.

Transcriptions

One of TrialView's most powerful features is its ability to provide real-time transcriptions during hearings, allowing you to view live, hyperlinked feeds within the platform. Using our innovative AI capabilities, users can analyse these transcriptions and easily identify inconsistencies and patterns within the information, allowing you to adapt and enhance your legal strategy on the go. Plus, with our intelligent search feature, users can quickly retrieve specific facts and information from these transcripts, with automatic hyperlinking that directly connects them to supporting documents.

Video Hearings

TrialView also helps during trial. It provides a seamless hearing experience and an engaging evidence presentation tool. TrialView's integrated video conferencing enables all parties to participate, regardless of location, enhancing both the flexibility and accessibility of the procedures. For an extra layer of security and customisation, permissions can be set to ensure everyone only sees the attendees and evidence that they are supposed to.

Staff Clearances and Security

All our eDisclosure staff are cleared to SC level, and when recruiting we seek candidates that 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, criminal records (DBS), UK financial status (5 years) and employment history (3 years) for all employees. This meticulous process is in full compliance with the Baseline Personnel Security Standard (BPSS). We perform rolling annual checks thereafter, ensuring a 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 any amendments are immediately reported back to the necessary authorising body, keeping them informed and involved.

Our ISO 27001:2013 Information Security Management System (ISMS) sets out this process. Our rolling HR Security Audits also checks the clearance status of all staff quarterly, so that any impending clearance expiries are identified and renewed promptly.

Our operational practices retain work where clearance might be required 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.

Security Training

Our Information Security Management System (ISMS) 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 providing services requiring information security best practices. General information security awareness is not just promoted, but nurtured through regular knowledge sharing, seminars and conference attendance, supplier training courses, and through the performance of audits. Conformance with security and confidentiality training is tracked by HR, providing constant visibility to our leadership team, and ensuring that junior staff feel supported and guided in their journey towards information security excellence.

Our ISMS requires all the above to be audited annually, which is how we ensure that our training remains current and that all staff members have been trained.

Our eDisclosure and Digital Forensic consultants almost all hold degrees in Computer Forensics or Computer Science. They are trained to have an advanced understanding of the fundamental importance of system security, data handling and acceptable use policies and how this is implemented and achieved in practice.

All staff sign a confidentiality agreement when commencing employment, which includes a warning that violation of security policies will result in disciplinary action, which may lead to loss of access privileges, termination of employment or civil and criminal prosecution. Training is completed during induction, and new staff are not permitted to engage in client work until all aspects of mandatory training have been completed and passed at 80% or higher.

Systems Access, Permissions and Role Management

Our platforms have logical user security and full audit trails. All systems are configured according to the principles of least privilege, with limited access to administrator privileges. We restrict all user accounts to named individuals. Access to our systems is via 2FA, with separate credentials for corporate systems (e.g., email) and eDisclosure platforms.

Our platforms' features all have customisable permission levels, ensuring ease of use by providing only the features, work products, and documents that the reviewers need, commensurate with their role. We can easily adjust access during a project. Our platforms' comprehensive audit histories ensure that clients can prove the accountable way access has been managed and all actions performed within the platform.

We use roles to control system access and what areas can be seen within individual platforms. We configure user access to match the job roles of employees and clients. Roles are defined within our ISMS and managed centrally to ensure consistency of application and prevent conflicts. Allocation to roles is done by job role rather than individually, through agreement between the client, HR, IT Security and Project Lead to ensure alignment with clearance, systems and project needs.

Local administrator privileges on workstations are restricted to end users, who cannot make configuration changes or install software without oversight by IT. Users outside of IT do not have local or domain administrator privileges on any workstations or servers. Where remote access is necessary, we only permit this via VPN with separate 2FA. Administrative access to our eDisclosure platforms is only possible via our hardware.

We can supply a Crypto Custodian where required.

Scoping and Ordering

Using over 100 years of combined experience, we advise clients on best practices, ensuring they have the scope and collate and collect their data appropriately and defensibly.

We provide consultancy from the outset of any engagement. We advise our clients to allow us to assist from the initial stages of data scoping and in forensic collections as, in our experience, this up-front consultancy ensures a more effective and efficient capture and transfer of data.

We regularly support our government and law firm clients with data scoping exercises. These typically involve working with an end client's IT department to carry out data mapping and develop a detailed understanding of the locations and types of data that require collection.

Onboarding

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 such as the scope of the matter start-up meeting, client-specific requirements and any contractual or compliance issues. Having an agreed process in place allows us to begin subsequent matters in a uniform and repeatable manner.

When engaged on one-off matters, onboarding begins with a data scoping exercise. This enables us to create a cost estimate based on data volumes, estimated matter length, number of reviewers, and expected support requirements. We focus on ensuring that we understand our clients' review needs and that they understand the scope of our services from the outset.

We then provide clients with our standard Service Order Form for signature, which includes a cost estimate and conflict checks. Once we have received the signed Service Order Form and have established that conflicts are clear, we commence work on the case.

Implementation

We take time to establish key contacts for each party and to determine the user skill levels and training requirements. We also confirm matter timelines, milestones and deliverables. As part of our best practice approach, we use checklists that cover aspects such as the processing specification, deduplication requirements, search term reporting, workflow and coding requirements.

We will start working on the matter once the specifics are agreed upon and understood. Below, we have provided a high-level summary of the stages a matter will generally follow. We can complete some of these tasks concurrently:

- Receive or collect the case data
- Ingest and process data
- Load processed data into the platform
- Set up any required analytics features
- Create user/reviewer access (licences)
- Perform training sessions
- Release the case workspace to the review team
- Provide ongoing case support through to completion

Delivery of Support

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 support team can assist with more complex tasks such as creating layouts, search term reports, applying analytics functionality, application of generative AI, and creating productions. We seek approval before undertaking work that is outside the scope of the initial agreement. If required, we will provide an updated cost estimate.

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.

Since the introduction of the GDPR / DPA 2018 regulations, we have:

- Appointed a member of staff responsible for data protection
- Established a data protection training programme and trained all staff, both on induction and annually
- Performed a Data Protection Impact Assessment on our eDiscovery processes and adjusted our processes appropriately to ensure compliance and mitigate risks; performed an inventory of our data processing, and established a Register of Processing Activities
- Continuously enhanced our technical and operational security measures to protect against damage to personal data
- Performed due diligence on our suppliers to ensure they comply with GDPR/DPA 2018, including having appropriate technical and organisation measures in place, appropriate contract terms, and ensuring that any transfers are appropriately protected
- Updated our standard contract terms to ensure they comply with GDPR/DPA 2018
- Published a Privacy Notice

DSARs and Data Rights Request Process

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 request from the data subjects where 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.

Our Role as a Processor and Controller

In terms of the eDisclosure service, Anexsys acts as a Processor only, acting on the instructions of the Buyer, who is the Controller of the personal data being processed. Anexsys acts as a Controller only in terms of 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
info@anexsys.com