opentext™

Powerful new applications for eDiscovery technology and techniques

Improving cybersecurity incident response, data privacy requests, internal investigations and M&A due diligence

opentext™

Contents

Executive summary

Organizations are facing an evolving legal landscape. Stringent privacy and data security regulations must be met, ranging from the EU's cross-border transfers to U.S. state laws in lieu of comprehensive federal protection. COVID-19-driven remote and hybrid work has escalated ransomware attacks and other sophisticated cyber threats. Organizations need to prepare for when—not if—an incident or data breach will occur. Newer data privacy laws and regulations have raised the stakes for protecting sensitive data and notifying affected parties quickly.

Legal departments must work with other decision makers, including security and compliance leaders, to develop strategies to manage data privacy compliance risks. Proven eDiscovery workflows and technology are being applied beyond litigation to cybersecurity and other use cases, including data subject access requests, internal investigations and M&A due diligence.

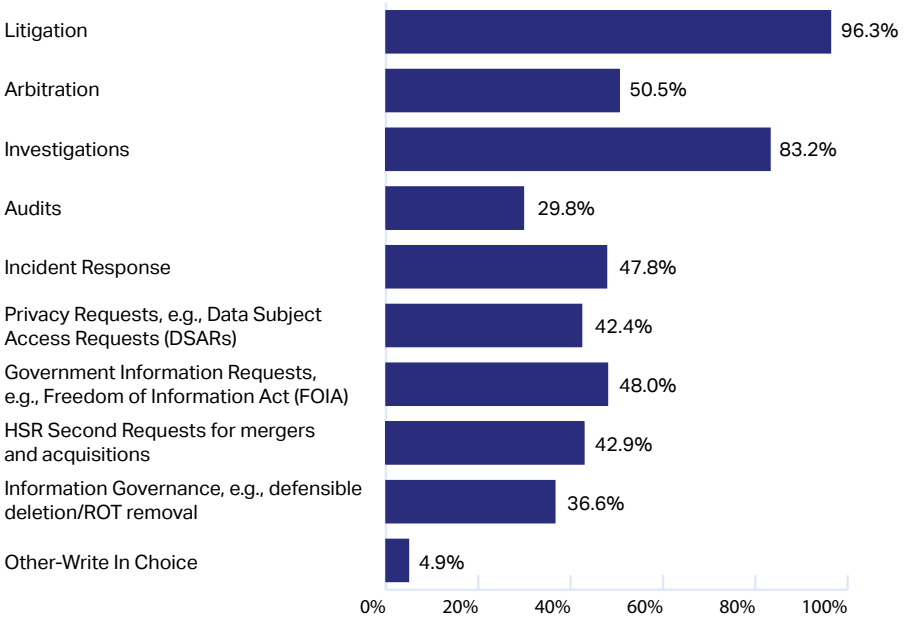
This position paper discusses legal departments' growing influence on organizational strategy and provides insight into how eDiscovery technology and techniques can be leveraged to minimize new and emerging legal risks.

opentext™

Legal departments' growing influence on organizational strategy

In the 2023 State of the Industry Report published by eDiscovery Today, 410 respondents identified use cases where they apply eDiscovery technology and workflows:

To which use cases do you or your organization apply eDiscovery technology and workflows today? (select all that apply)



Respondents using eDiscovery technology and workflows for different use cases[1]

Not surprisingly, litigation was the top use case for more than 96% of respondents. However, six more use cases were endorsed by more than 40% of respondents. Two notable ones were incident response from data breaches (with 47.8%) and data privacy requests, e.g., data subject access requests (DSARs) (with 42.4%).

Factors influencing eDiscovery expansion

A convergence of dynamic regulatory forces and corporate mandates have influenced the expanded use of eDiscovery tools.

An evolving regulatory environment

Countries worldwide, including the U.S. and many in Europe, have passed new data privacy laws in recent years. Each data privacy law is unique, with different requirements for protecting personal data. Not only that, but the U.S. has no comprehensive national data privacy law. Instead, five states (so far) have passed their own separate data privacy laws. This global patchwork of new regulations is raising the stakes, introducing many complex legal variations across markets and in the process, necessitating Legal's involvement in cybersecurity decisions and workflows.

1 eDiscovery Today, 2023 State of the Industry Report. (2023)

Legal's growing responsibility for cybersecurity

The recent 2022 State of Cybersecurity Report[2] provides several findings that illustrate Legal's growing responsibility for cybersecurity, including:

- Cybersecurity reports to the Chief Legal Officer (CLO) in 38% of departments surveyed.
- 84% of CLOs now have at least some cybersecurity-related responsibilities, whether it be a leadership position, being part of a broader team with cyber responsibilities or being a part of an incident response team.
- 22% of companies now employ an in-house counsel with responsibility for cybersecurity.
- In 48% of cases, this lawyer is responsible for coordinating cyberlaw strategy across the entire enterprise and in 29% of cases, this lawyer is fully embedded in cybersecurity/IT and works directly with technical resources.
- Regarding data breaches, damage to reputation (77%), liability to data subjects (61%) and business continuity (51%) are the most immediate concerns.

The role of outside counsel

Data privacy and cybersecurity have become important considerations for outside counsel firms as well, with several larger firms offering data privacy and data protection practice groups to support corporate clients. Law firms—especially those that regularly coordinate eDiscovery for litigation—understand the benefits of eDiscovery technology and workflows, as well as how they can be applied to other use cases.

Protecting data in routine litigation and regulatory matters

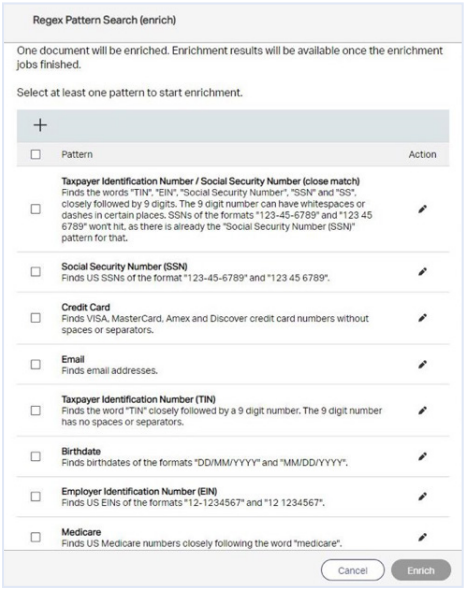
In litigation and regulatory matters, identifying personally identifiable information (PII) and personal health information (PHI) has become important in any processes involving disclosure of information to another party. That includes routine litigation, third-party subpoenas and regulatory matters where sensitive data must be effectively managed to avoid violating data privacy laws.

Several eDiscovery technology tools can facilitate PII identification:

- **Smart filters:** Leverages more than 50 metadata fields to focus queries and narrow the document population.
- **Predictive filters:** Guides reviewers on the most relevant privacy terms to find personal data with predictive scores that are continuously updated via unsupervised machine learning.
- **Regular Expression (RegEx) engine:** Uses common and custom patterns to quickly identify personal data such as Social Security numbers, credit card numbers, email addresses, birth dates, etc. wherever they reside in a document collection. The pre-configured patterns can be embedded in the smart filter framework so data privacy searches can be run easily and stacked in tandem with keyword searches for relevant data.
- **Automated detection of people, places and organizations:** Automatically highlights the names of entities for easy identification so they can be flagged for redaction if needed, either individually or across all entities.

2 Association of Corporate Counsel (ACC) Foundation and Ernst & Young, 2022 State of Cybersecurity Report.

- **“Mark for redaction”:** Flags data staged for redaction for easy review.
- **Redaction:** Redacts data by individual document or in bulk across groups. Redacts selectively within documents, either single pages or across pages, including chat strings and Microsoft® Excel.
- **Entity extraction:** Extracts people’s names from all content in the review to aid the identification of other individuals who may require additional consent or redaction prior to production.
- **Advanced text analytics:** Identifies occurrences of names of data subjects, facilitating automatic redaction of that data.
- **Technology-assisted review based on continuous active learning:** Prioritizes the most likely content across virtually any data set by continuously suggesting new documents for review based on personal data already identified.
- **Automated QC processes:** Ensures accuracy and reduces the risk of inadvertent non-compliance with data privacy laws.



Pre-configured library of common patterns in OpenText™ Axcelerate™

As discussed below, these tools are also critical in addressing new data privacy risks.

Aligning eDiscovery to address non-litigation use cases

It is important to seize opportunities to apply eDiscovery beyond traditional litigation applications to understand an organization’s data and reduce potential risks.

New use cases for eDiscovery technology and techniques include:

- Internal investigations
- Data breach response
- Data subject access requests (DSARs)
- M&A due diligence

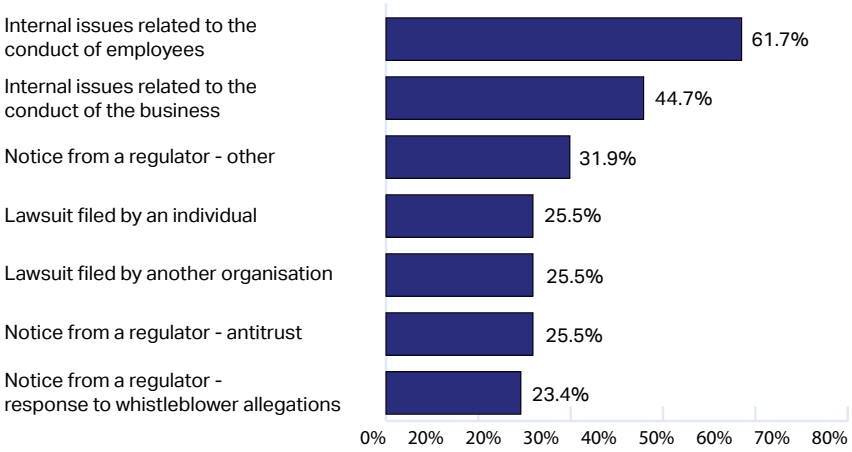
Each will be explored in greater detail below.

opentext™

Internal investigations

For corporate legal and investigations teams, the threat of internal misconduct is rapidly increasing in frequency and scale of impact. As an example, in the DACH region of Europe the highest frequency triggers for investigations are internal issues related to employee conduct (61.7%) and internal issues related to the conduct of the business (44.7%).

Highest frequency triggers for investigations[3]



As the problem grows, it also is becoming more complicated to deal with. Internal investigations now involve important external regulatory considerations: whistleblower protections and privacy laws.

Whistleblower protections

In 2019, the European Union (EU) passed Directive (EU) 2019/1937 (commonly referred to as the "Whistleblower Directive") to enact greater protections for whistleblowers by shielding them from retaliation and creating "safe channels" to report violations of the law. EU states are encouraged to enact greater whistleblower protections and incentives beyond the minimum standard set by the directive. In the U.S., the Whistleblower Protect Act similarly protects employees from retaliatory action for voluntarily disclosing information about dishonest or illegal activities occurring in a government organization. The Department of Labor's whistleblower protection laws similarly protect employees, and a host of similar state laws protect state employees who file complaints.

Privacy laws

Investigations may have to be conducted in compliance with several privacy laws. In Europe, organizations must adhere to GDPR's lawfulness principle when launching an internal investigation involving an EU resident's personal data. A company or third party may have the ability to use an individual's data if there is a legitimate interest, as long as the existing privacy rights of the individuals do not supersede it. Reasonable suspicion of misconduct based on certain facts and information is one such example. In the U.S., applicable privacy laws tend to be either by state or industry (such as HIPAA for healthcare).

3 Legal Business and OpenText, Maximizing Compliance and Minimizing Risk: Corporate Investigations in the DACH Region

eDiscovery tools and techniques that quickly identify relevant information in a litigation context, while finding and protecting personal data, are well-suited to addressing internal investigations' unique challenges.

Internal investigations and audits are highly confidential, making utmost data protection and privacy essential. eDiscovery tools such as RegEx engines to detect privileged or commercially sensitive data and automated detection of people, places and organizations can similarly be applied to keep sensitive data confidential. Legal hold tools with “silent hold” functionality similarly can execute data preservation workflows to secure data without informing custodians, mitigating the potential willful destruction of evidence.

Data breach response

It is important to be prepared – not only to prevent data breaches from occurring, but also to respond to data breach incidents once they do occur. Following a data breach, the task of determining exactly **what** personal or confidential information is contained in the body of data taken and **who** the information belongs to can be a daunting task. eDiscovery and investigative workflows can incorporate many of the same techniques and tools used in litigation to answer these questions.

For an in depth look at the opportunities for data breach response and analysis using eDiscovery tools, read Effective Response to Data Breaches Leveraging eDiscovery Technology and Techniques.

Data subject access requests (DSARs)

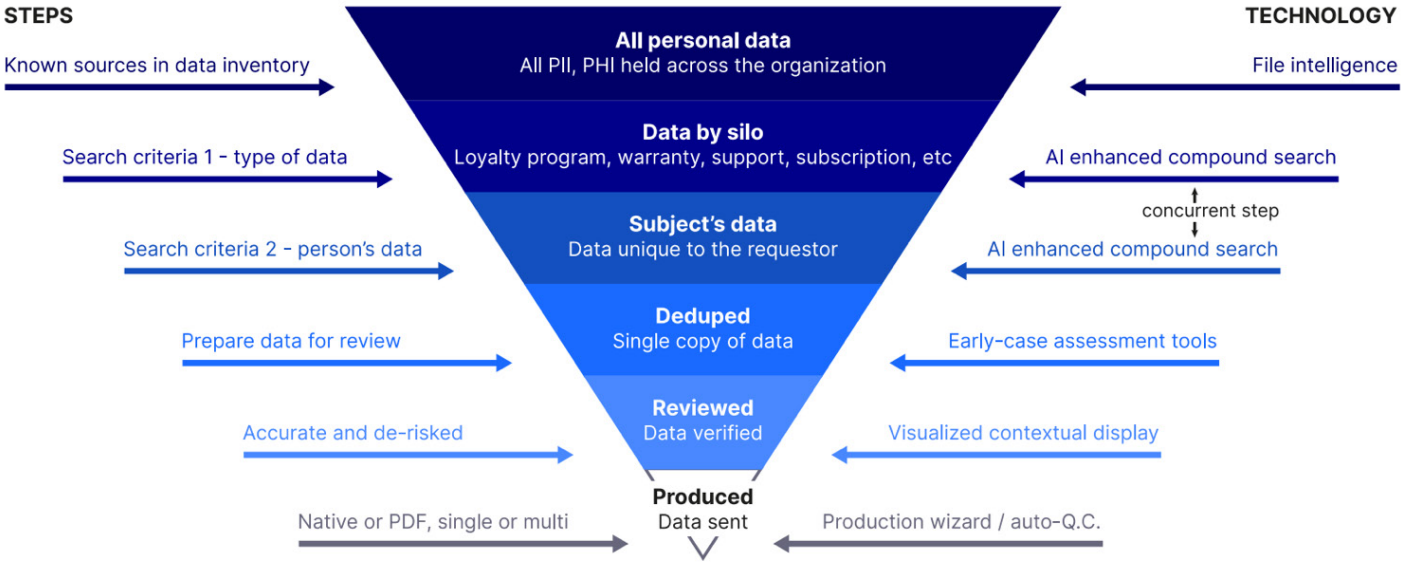
eDiscovery workflows can assist organizations in managing subject rights requests (SRRs), including the increased volumes of data subject access requests (DSARs).

Both DSAR and litigation responses requiring eDiscovery seek to extract vital information from large data sets while avoiding the inclusion of extraneous content where possible. Accomplishing this relies on some of the same approaches used for data breaches, along with others unique to data privacy and litigation requests.

These include tools to search, deduplicate and de-NIST the data for a more accurate set at review start time; analytics and machine learning technologies like TAR to automate relevant document identification; as well as automated redaction protocols to protect confidential or sensitive material before relevant documents are produced to the requesting party.

The illustration below shows how eDiscovery tools and techniques can surface relevant data from large document sets quickly and efficiently.[4]

DSAR Funnel—Homing in quickly to contain costs



Efficient use of eDiscovery technology to winnow down large document collections to the relevant personal data

M&A due diligence

Due diligence is a critical step and primary factor in the overall success (or failure) of mergers and acquisitions. Among the most pressing challenges of due diligence reviews, including second reviews under stringent timelines by agencies, is that document review is typically voluminous and expansive. Acquiring or merging parties need to find critical risks quickly.

Companies are not only worried about data protection while reviewing documents for production; data privacy programs are also playing a growing role in determining the value of M&A deals. Competition user agreements, various data protection regimes and insurers' increasing scrutiny can easily turn a gold mine unto unusable data. Even where an acquirer is not subject to one of the more stringent privacy laws, it likely must navigate laws that require companies collecting personal information to provide disclosures and secure it. Conversely, buyers will want assurances that the personal information that they are acquiring is "clean."

There are best practices for due diligence when it comes to navigating the data privacy landscape so that potential risks (such as data protection non-compliance, risky agreements, sanctions, false representations and warranties about the status of data privacy) are flagged early:

- **Know your data**
  Companies must have a clear picture of their information to reduce downstream risks. This includes knowing where sensitive data resides through data mapping exercises, ensuring alignment around privacy and security, and how commercially sensitive data is handled.

4 For additional information on applying eDiscovery to DSAR and SRR requests, read Efficient Data Privacy Compliance Using eDiscovery Workflows and Optimizing data subject access request (DSAR) processes with OpenText™ Axcelerate™.

- **Understand the scope of data sources and BYOD policies**
  Privacy-sensitive data is now generated in “shadow IT” communications sources such as chat, collaboration tools and more. Collecting, searching and reviewing may require specialized eDiscovery or investigation tools, techniques and expertise.

  For example, BYOD policies could raise data protection concerns due to the fact that the device is owned by the employee rather than the data controller.

- **Apply tools like RegEx, text mining and redaction**
  Organizations can identify and redact all sensitive data (such as customer names on sales contracts) when producing to the acquiring or merging party.

- **Leverage Rapid Analytic Investigative Review (RAIR)**
  In HSR Second Requests and EC RFIs, time is of the essence and productions must be deemed comprehensive to avoid the risk of non-compliance fines, penalties or risk of rejection of the transaction. Organizations can speed responses with RAIR, an investigative technique that quickly finds groups of documents with similar characteristics that are amendable to bulk coding leading to production.

Learn more about OpenText’s RAIR approach to document review in Maximizing document review efficiency with rapid analytic investigative review.

Conclusion

eDiscovery isn’t just for litigation anymore. Leveraging eDiscovery tools and techniques is key to not only responding to data breach incidents, privacy requests and other use cases, but also to preventing them. All data-oriented processes are candidates for eDiscovery workflows and technology.

As many of these processes involve data and risk reduction, legal departments are in a key position to influence how they are conducted. Leveraging eDiscovery tools and techniques to support new and emerging use cases simply makes sense.

Learn how eDiscovery workflows can be applied to data breach response and analysis, Effective Response to Data Breaches Leveraging eDiscovery Technology and Techniques.

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea’s blog
- Twitter | LinkedIn

opentext.com/contact