exterro®

THE CONVERGENCE OF E-DISCOVERY & PRIVACY

PREPARING FOR DEFENSIBLE COMPLIANCE

THE CONVERGENCE OF E-DISCOVERY & PRIVACY

THE CHANGING LANDSCAPE

As high-profile cases and ever-increasing regulations highlight, we are entering a new age of dealing with data that's causing companies to rethink everything – from how they collect data to storage, retention, access, disposal, and more.

The General Data Protection Regulation (GDPR) set the stage for a new era of data protection and privacy compliance and effectively sparked a regulatory movement, beginning with the hasty passage of the California Consumer Privacy Act (CCPA) in the United States. Shortly thereafter, several other states introduced their own "CCPA Copycat" laws, and more are on the way. Failure to comply with this increasingly complex terrain of privacy regulations could result in litigation that is damaging, both reputationally and financially. Companies must develop a defensible approach to data privacy regulations and ensure that their e-discovery preservation and information governance programs are up to par.

> "E-discovery needs to reckon with the changing landscape of data privacy regulations. GDPR is just the tip of the spear. The California Consumer Protection Act, the New York Department of Financial Services Cybersecurity Regulation, and likely many more state regulations are on their way. Organisations' obligations to manage data—and the costs of failure—are growing exponentially."
>
> **Bobby Balachandran**
> CEO, Exterro

THE COSTS OF FAILURE

Organisations' obligations to manage data—and the costs of failure—are growing exponentially. Just look at recent examples from data breaches. A well-known retailer paid almost $70 million in settlements with banks, states, and class action suits stemming from a single data breach. In July 2019, Facebook received a $5 billion privacy fine, representing about 9% of Facebook's annual review - more than double the maximum percentage (4%) of annual revenue that can be imposed as a penalty under the EU's General Data Protection Regulation (GDPR).

> "Global privacy concerns — and in some jurisdictions, accompanying privacy laws — will test how discovery in U.S. litigation can be reconciled with data protection requirements."
>
> **Skadden Arps Slate Meagher & Flom LLP**
> For Lexology

The e-discovery process inherently opens organisations up to unintentionally compromise personal data if processes are not in place to incorporate privacy principles into the e-discovery process. Legal teams must make sure their e-discovery preservation and data privacy and governance programs comply with data privacy and cybersecurity regulations to avoid opening their organisation up to layers upon layers of lawsuits. The plaintiff's bar will no doubt leverage the complexities of these regulations to their advantage. Organisations must be prepared.

THE CONVERGENCE OF E-DISCOVERY & PRIVACY

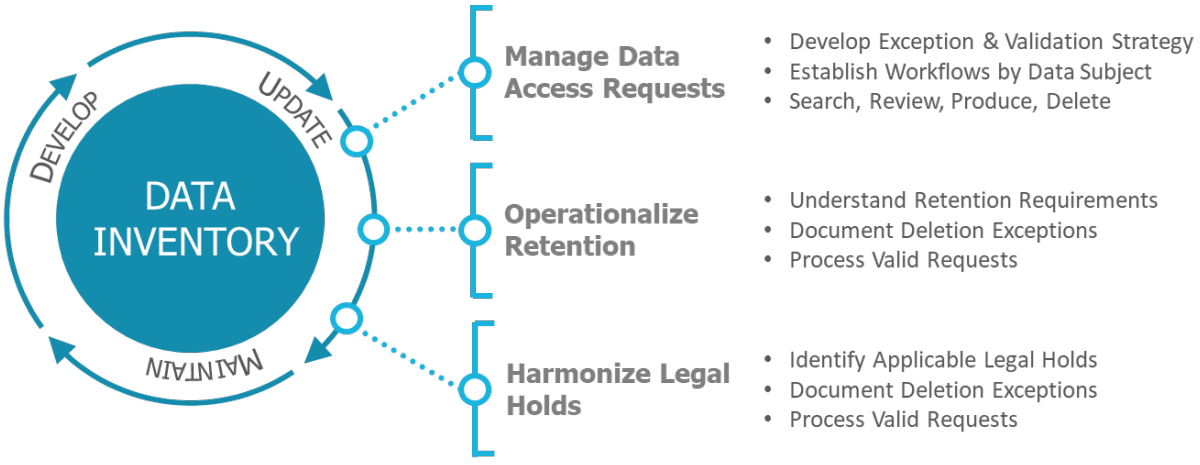
SIMPLIFYING THE PROCESS

Both e-discovery and data privacy tasks require an accurate and comprehensive data inventory, the ability to identify and preserve data, and the ability to review, redact, and produce relevant data under tight timelines. Organisations must be able to quickly and accurately 1) understand the data they control, 2) define precisely where it exists inside IT infrastructure, and 3) secure, access, retrieve, and manage it in accordance with both regulations and business needs.

Companies that don't have a handle on their data practices face a costly e-discovery nightmare and potential oversight when responding to data access requests that could spark litigation.

Effective e-discovery and privacy compliance begins with developing a sustainable and robust data inventory that identifies what information an organisation holds, where it's stored, how it's generated and used within the company, retention requirements, and more. Your data inventory informs data privacy compliance and how data can be used in the e-discovery process. Understanding what data is protected not only limits exposure to a potential breach of sensitive information, but also limits the time and resources spent early in the discovery process including managing data access requests from residents exercising their data privacy rights.

> "The increased focus on protecting personal privacy may pose a new challenge to the bounds of e-discovery in U.S. litigation as courts reconcile whether and how new data protection laws apply to a litigant's obligation to produce relevant information... A new challenge to the bounds of U.S. discovery, therefore, will be addressing the intersection of discovery with the increased awareness and focus on privacy and data protection."
>
> **Skadden, Arps, Slate, Meagher & Flom LLP**
> For Law.com



THE CONVERGENCE OF E-DISCOVERY & PRIVACY

AVOIDING A DISCOVERY & DATA PRIVACY NIGHTMARE – DATA ACCESS REQUESTS

Data Subject Access Request (DSAR)– one of the privacy obligations that management will need to provide for, is the obligation to allow data subjects access to their personal data. The GDPR states that the reason for this obligation is 'in order to be aware of, and verify the lawfulness of the processing' (Recital 63).

Companies that don't have a handle on their data practices and have a well-orchestrated process for managing data access requests face a costly discovery nightmare.

Another key consideration is time. Information must be provided without delay and at the latest within one month of receiving a request.

There are three foundational distinct capabilities that legal teams must have in place to be prepared to respond compliantly and defensibly to data access requests.

> "Building a data inventory that includes the types of information that will be required for your disclosures is a rational first step towards compliance. To create a data inventory you will need to survey all aspects of your business, from Marketing to IT to HR to Vendor Management and all points where you receive information from any source and in any format."
>
> **Catherine Meyer & Fusae Nara**
> Pillsbury

1. KNOW YOUR DATA

The first step to effective and defensible compliance begins with a comprehensive, sustainable data inventory. You have to know where your data exists in order to protect it, produce it, and ultimately delete it. As a privacy professional or legal executive, you simply can't meet your obligations with out a data inventory.

2. PROCESS ORCHESTRATION

Different types of data access requests require different workflows and verification processes. Requests from job candidates or past employees must trigger a different role-based workflow than requests submitted by customers or subscribers. Legal teams need a well-orchestrated process that is configurable based on the data subject and type of request.

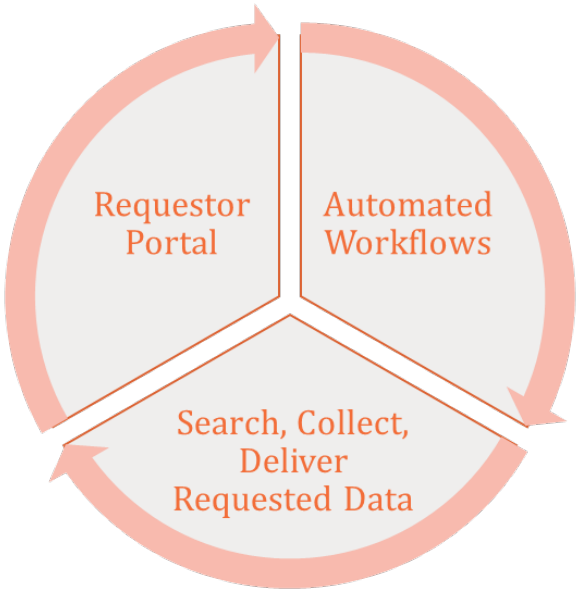
3. REQUEST FULFILLMENT

Organisations have 45 days to respond to and fulfill verifiable data access requests. You need a secure process for authorised personnel to quickly find relevant information stored across your IT infrastructure, review information to ensure documents are appropriate to the request, redact information as necessary, and produce the information.

THE CONVERGENCE OF E-DISCOVERY & PRIVACY

A WELL-ORCHESTRATED DATA SUBJECT ACCESS REQUEST PROCESS

1. **Facilitating Requests.** Identify how your organisation will accept DSAR submissions (online portal, toll-free phone number, email address, etc.)
2. **Verifying Requests and Identifying Exceptions.** Responding to an unverified request is both a waste of time and resources and a data breach risk to your organisation. Before you begin the process of responding to a DSAR, you must first verify the request and check for exceptions.
3. **Setting Up Workflows.** The ability to run configurable workflows based on the category of data subjects who submit DSARs is essential.
4. **Managing Deadlines.** Deadlines are essential when responding to DSARs – data privacy laws typically mandate a specific time period within which an organisation must respond to a DSAR (typically 30-45 days). Workflows must incorporate essential timelines and keep appropriate personnel updated on upcoming deadlines.
5. **Searching for Relevant Information.** When responding to a DSAR, you must be able to search for data across infrastructure, locations and third parties and to modify data in those locations as necessary.
6. **Reviewing Information.** Collected documents and data should be reviewed prior to disclosure to ensure that each document is appropriate to the DSAR.
7. **Fulfilment.** Data should typically be provided electronically in an easy-to-use format (such as spreadsheet or .csv file). Organisations should take care to harmonise data retention requirements and legal holds for deletion requests, etc.



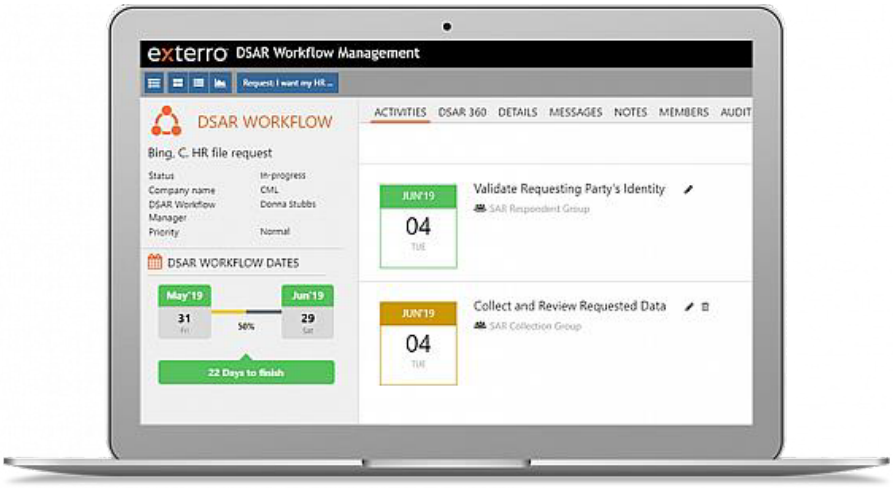
THE CONVERGENCE OF E-DISCOVERY & PRIVACY

DATA SUBJECT ACCESS REQUEST SOFTWARE

Effectively responding to Data Subject Access Requests (DSAR) as required by regulations such as GDPR or the CCPA is challenging. With new exciting advancements in DSAR technology, legal teams can now orchestrate the entire process beyond just workflow automation, including the capabilities to retrieve, review and deliver requested information to the requester, all in one software solution

Register for our upcoming product demo webcast to learn more about this essential solution or visit our website at jordanlawrence.com/DSARS

> "As Gartner puts it, these recent and evolving privacy regulations "cannot be dismissed with a narrow checkbox mentality." Organisations will need a portal for Data Subject Access Requests (DSARs), but that's just the front end. More importantly, they need a holistic information governance plan to understand the data in a contextual manner, and the ability to preserve, collect, review, redact, produce or remediate information—all on demand, in an efficient business process."
>
> **Bobby Balachandran**
> CEO, Exterro



KEY FEATURES

- Consumer/Requestor Portal for Submitting and Tracking Requests
- Configurable, Automated Workflows
- Comprehensive Information Search
- Delivery of Requested Information

ABOUT JORDAN LAWRENCE

Jordan Lawrence is a leading software and services company specialising in regulatory and legal compliance in the fields of data privacy, data minimisation, and vendor process risk management. For more than 30 years, Jordan Lawrence has delivered software and services that have helped more than 1,000 clients meet international and domestic data privacy regulations pertaining to record retention, information management, data privacy and security. Our products include Data Inventory, Data Minimisation (Data Retention and Disposal), Vendor Risk Profiling and Data Governance.

Since 2005, Jordan Lawrence has been an ***ACC Alliance Partner of the Association of Corporate Counsel***. In 2018, we were appointed the exclusive ***ACC Alliance Partner for Data Privacy & Cybersecurity Compliance***.

Top law firms from around the world partner with us and leverage our services to provide clients the most comprehensive legal guidance available.

Jordan Lawrence became part of the Exterro family in 2019. Learn more about the synergy of the offerings of both organizations **here**.

ABOUT EXTERRO

Exterro®, Inc. is the leading provider of e-discovery and information governance software specifically designed for in-house legal, privacy and IT teams at Global 2000 and Am Law 200 organisations. Built on a simple concept of process optimisation, Exterro helps organisations address their regulatory, compliance, and litigation risks more effectively and at lower costs. For more information, visit exterro.com.

ACC ALLIANCE
Exclusive Savings for ACC Members

CONTACT US FOR MORE INFORMATION

636.778.1700
services@jordanlawrence.com
JordanLawrence.com