



## **Contents**

Executive summary	3
Legal departments' growing influence on organizational strategy	4
Aligning eDiscovery to address non-litigation use cases	6
Internal investigations	7
Data breach response	8
Data subject access requests (DSARs)	8
M&A due diligence	9
Conclusion	10

## **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

## **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**

### **Legal's growing responsibility for cybersecurity**

The recent 2022 State of Cybersecurity Report<sup>2</sup> provides [several findings](#) that illustrate Legal's growing responsibility for cybersecurity, including:

- Cybersecurity reports to the Chief Legal Officer (CLO) in 38% of





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.



The illustration below shows how eDiscovery tools and techniques can surface



