Legal Data Intelligence™

Data Protection

The Compliance Need and Strategic Value of the Legal Data Intelligence Model

By: Briordy Meyers, Joe Bartolo, and Mike Kearney

October 2025

Contents

Today’s Global Data Protection Landscape

According to the United Nations, 79 percent of countries have data protection and/or data privacy legislation.[1] Nine in ten countries have laws governing e-transactions, and just as many have legislation addressing cybercrime.[2]

Although countries vary in their approaches, the overwhelming majority recognize that data protection—whether in the context of privacy, commerce, or cybersecurity—is central to securing the free flow of commerce, consumer safety, and human rights. Data protection is a core tenant of not just business, but the operation of modern-day society.

In the context of legal data, organizational intelligence and consistent risk management around data protection and privacy are at the heart of market innovation, key performance indicators, and today’s definitions of business success.

The Compliance Need for Data Protection

Organizations must prioritize investment in data protection compliance for several compelling reasons.

First, compliance ensures legal and regulatory alignment, helping organizations avoid costly penalties and reputational damage in an era where most countries enforce dedicated data protection laws.

Failure to comply with the General Data Protection Regulation (GDPR) can lead to fines ranging from €10 million or 2 percent of a company’s annual turnover (whichever is higher) for less serious violations to €20 million or 4 percent of a company's annual turnover. Luxembourg’s Commission Nationale pour la Protection des Données (CNPD) fined Amazon €746 million in 2021.

US state attorneys general are becoming increasingly active in the data protection space, responding to consumer sentiment around data protection. In 2024, the Texas Attorney General fined Meta $1.4 billion over allegations of illegally collecting and using facial recognition data.[3] The Texas Attorney General settled another large data protection case with Google in 2025, issuing a fine of $1.375 billion for allegedly tracking and collecting user data in an unlawful manner.[4]

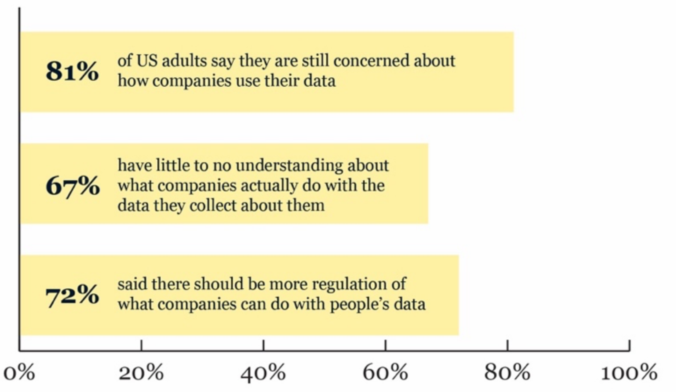
[1] UN Trade and Development, Data Protection and Privacy Legislation Worldwide at https://unctad.org/page/data-protection-and-privacy-legislation-worldwide, last accessed July 31, 2025.

[2] UN Trade and Development, Global Cyberlaw Tracker at https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide, last accessed July 31, 2025. Percentages are based on dividing the number of United Nations Conference on Trade and Development (UNCTAD) member states with legislation by the total number of UNCTAD member states (currently 195).

[3] https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture, last accessed on September 11, 2025.

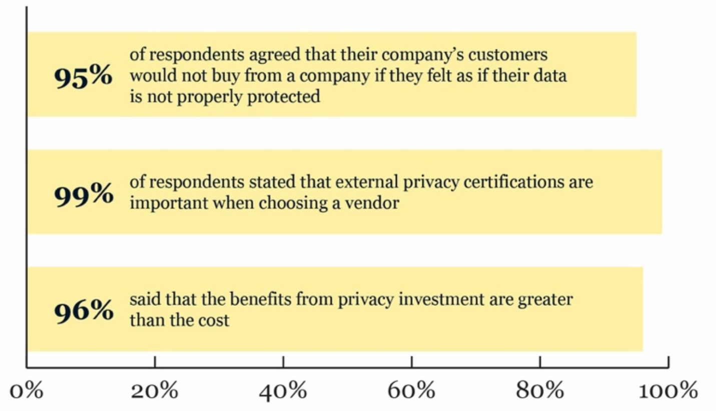
[4] https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-historic-1375-billion-settlement-google-related-texans-data, last accessed on September 11, 2025.

While regulations like the European Union's GDPR, Texas' Data Privacy and Security Act (TDPSA), and California's Consumer Privacy Act (CCPA) make headlines for their comprehensive approach to data protection and individual privacy rights, a 2023 study by the Pew Research Center found that 81 percent of US adults say they are still concerned about how companies use their data. Another 67 percent said they have little to no understanding about what companies actually do with the data they collect about them, and 72 percent said there should be more regulation of what companies can do with people's data.[5]



Second, robust data protection practices build trust with customers, partners, and stakeholders, demonstrating a tangible commitment to safeguarding personal information and upholding fundamental rights in the digital age.

A recent survey by Cisco of more than 2,600 security professionals in 12 countries around the world found that 95 percent of respondents agreed that their company's customers would not buy from a company if they felt as if their data is not properly protected. 99 percent of respondents stated that external privacy certifications are important when choosing a vendor. Perhaps most importantly, 96 percent said that the benefits from privacy investment are greater than the cost.[6]



[5] Pew Research Center, October, 2023, "How Americans View Data Privacy" at https://www.pewresearch.org/wp-content/uploads/sites/20/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf, last accessed August 12, 2025.

[6] Cisco 2025 Data Privacy Benchmark Study at https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2025.pdf, last accessed August 12, 2025.

Finally, effective compliance frameworks foster operational resilience and competitive advantage, enabling organizations to navigate rapidly evolving threat landscapes and leverage data responsibly as a strategic asset.

This is particularly true in the era of artificial intelligence. Increasingly, organizations seek value in building, buying, or adopting generative AI technology, leveraging agentic AI, and exploring enterprise-level solutions to drive automation. They rely on protected information to train AI applications during development and proof of concept exercises. Data protection is at the root of responsible deployment of AI applications in both internal- and external-facing production environments.[7] Compliant use of protected information is central to AI governance principles as organizations begin to build out policies, standards, and procedures around AI use.

AI not only multiplies the use cases for data protection and privacy workflows but adds complexity to existing compliance strategies and use cases. Organizations must ensure legal and regulatory compliance, but they must also develop and maintain the trust of customers and data subjects everywhere whose protected information is used to develop, train, and deploy AI applications. Those organizations that do so effectively give themselves a competitive edge in their respective markets.

The Strategic Value of an LDI Approach to Data Protection

In a rapidly evolving digital landscape dependent on data protection and privacy compliance for risk management and business success, organizations often struggle to get started and remain consistent. Laws and regulations are complex, cross-jurisdictional, inconsistent, and rigid. Internal and external subject matter experts and key stakeholders across functions—including data protection, privacy, security, legal counsel, compliance, information technology, information and data governance, business strategy and development, AI governance, sales, marketing, and executive leadership—often speak different languages and operate with varied success metrics.

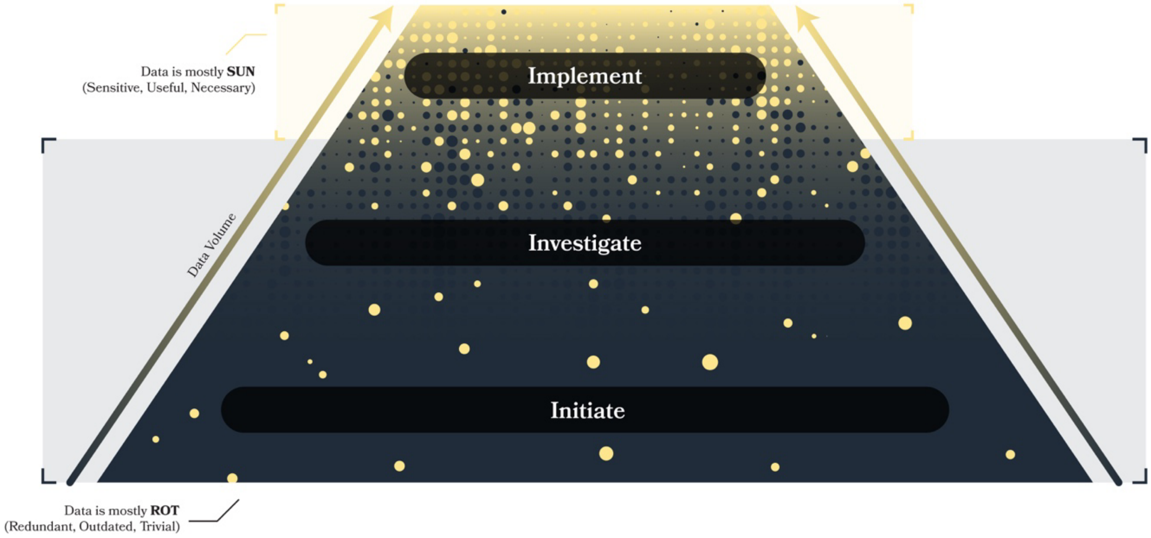
Colleagues wrestling with data protection and privacy compliance often speak at cross purposes. It can be difficult for key stakeholders to align efficiently and proactively to address data protection use cases.

The Legal Data Intelligence (LDI) model is unique in its aim to break down silos across functions and key stakeholder groups and drive efficient best practices regarding legal data management through simple, concise, and common nomenclature organized by an accessible action paradigm.

[7] The Intersection of Privacy and AI Governance, by IAPP Research and Insights at https://iapp.org/media/pdf/resource_center/intersection_of_privacy_and_ai_governance.pdf, last accessed August 12, 2025.

Legal Data Intelligence Model

Transforming sensitive, useful, necessary data to answers, insights, and advice.



The model focuses on the strategic management of Sensitive, Useful, or Necessary (SUN) data within an organization. SUN data includes protected data, personal information, sensitive data, confidential information, and trade secrets. Data, metadata, and related data-hosting architectures often face multiple overlapping and inconsistent categorization and classification schemes. By focusing more simply on SUN data in the context of data protection and privacy, colleagues can begin with a basic and shared language that makes sense to all stakeholders. The LDI framework is clear: deprioritize Redundant, Obsolete or Trivial (ROT) data that when unmanaged leads to data protection risk and focus on the SUN to solve legal data challenges.

The model also espouses a concise, proactive engagement framework broken down into three consistent phases: Initiate, Investigate, and Implement.

The Initiate phase focuses on scoping the data protection problem, gathering information, and identifying both the SUN data at issue and the respective regulatory, legal, or compliance paradigm applicable to the specific use case.

The Investigate phase involves active fact development, scope adjustment, data searches, analysis, and strategic planning in preparation for implementation of core data protection strategy.

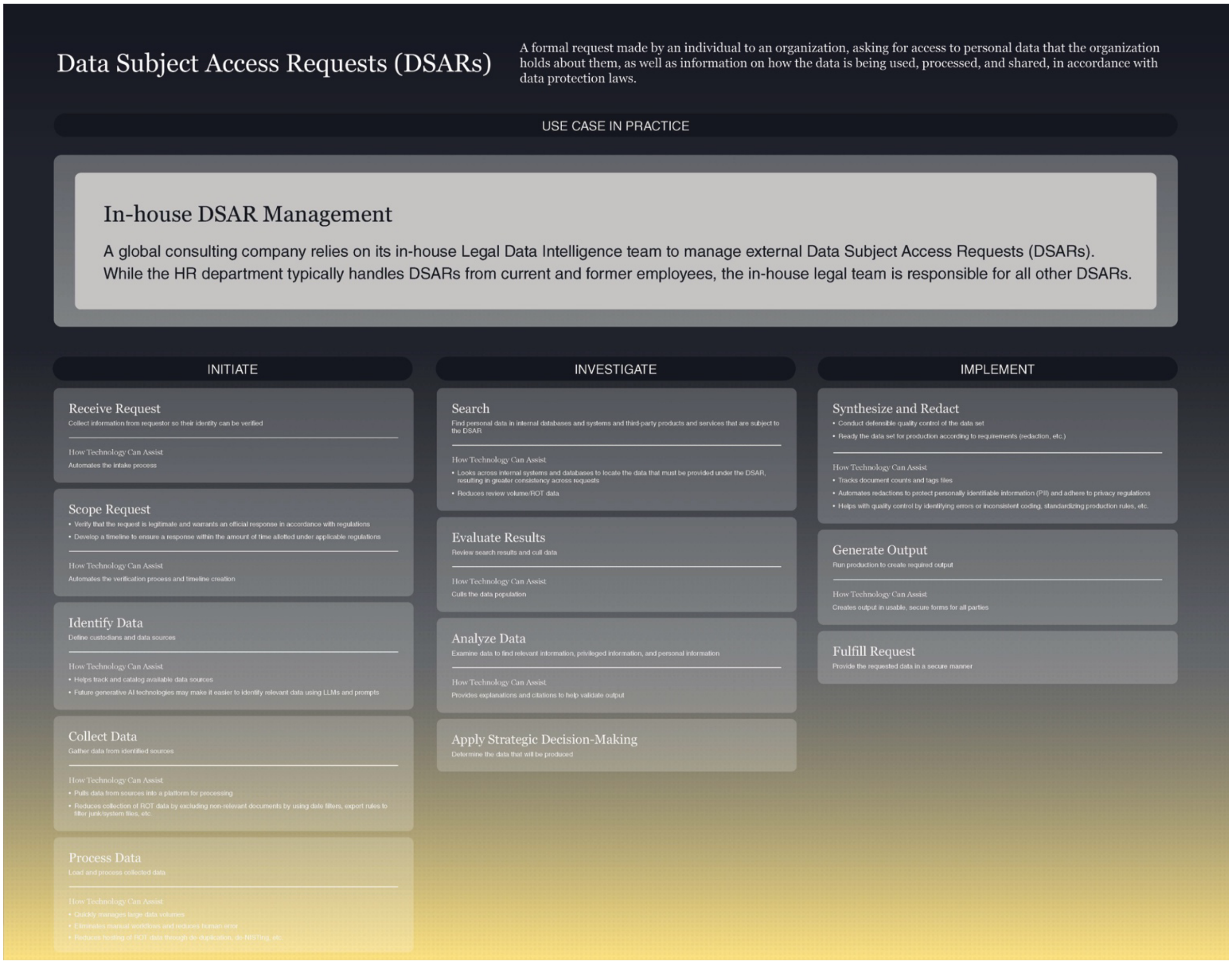
The Implement phase centers on application of the developed data protection approach through task execution, finalizing the risk management strategy developed in the first two phases.

Data Protection Compliance Use Cases: A Good Place to Start

Within the Data Protection Compliance category of the LDI model, there are currently eight use cases. Although the model is dynamic and evolving, these use cases provide a solid foundation for any organization looking to build out their data protection compliance program:

1. Freedom of Information Act (FOIA) Requests
2. Data Subject Access Requests (DSARs)
3. Data Breach Response
4. Personal Data Identification and Anonymization
5. Data Disposition
6. Cybersecurity Compliance and Governance
7. Data Loss Prevention
8. Source Code

Use cases are defined both individually and in the context of real-life practice before detailing the respective process steps to Initiate, Investigate, and Implement.



Data Subject Access Requests (DSARs)

A formal request made by an individual to an organization, asking for access to personal data that the organization holds about them, as well as information on how the data is being used, processed, and shared, in accordance with data protection laws.

USE CASE IN PRACTICE

In-house DSAR Management

A global consulting company relies on its in-house Legal Data Intelligence team to manage external Data Subject Access Requests (DSARs). While the HR department typically handles DSARs from current and former employees, the in-house legal team is responsible for all other DSARs.

INITIATE

Receive Request
Collect information from requestor so their identity can be verified

How Technology Can Assist
Automates the intake process

Scope Request
- Verify that the request is legitimate and warrants an official response in accordance with regulations
- Develop a timeline to ensure a response within the amount of time allotted under applicable regulations

How Technology Can Assist
Automates the verification process and timeline creation

Identify Data
Define custodians and data sources

How Technology Can Assist
- Helps track and catalog available data sources
- Future generative AI technologies may make it easier to identify relevant data using LLMs and prompts

Collect Data
Gather data from identified sources

How Technology Can Assist
- Pulls data from sources into a platform for processing
- Reduces collection of ROT data by excluding non-relevant documents by using date filters, export rules to filter junk/system files, etc.

Process Data
Load and process collected data

How Technology Can Assist
- Quickly manages large data volumes
- Eliminates manual workflows and reduces human error
- Reduces hosting of ROT data through de-duplication, de-NISTing, etc.

INVESTIGATE

Search
Find personal data in internal databases and systems and third-party products and services that are subject to the DSAR

How Technology Can Assist
- Looks across internal systems and databases to locate the data that must be provided under the DSAR, resulting in greater consistency across requests
- Reduces review volume/ROT data

Evaluate Results
Review search results and cull data

How Technology Can Assist
Culls the data population

Analyze Data
Examine data to find relevant information, privileged information, and personal information

How Technology Can Assist
Provides explanations and citations to help validate output

Apply Strategic Decision-Making
Determine the data that will be produced

IMPLEMENT

Synthesize and Redact
- Conduct defensible quality control of the data set
- Ready the data set for production according to requirements (redaction, etc.)

How Technology Can Assist
- Tracks document counts and tags files
- Automates redactions to protect personally identifiable information (PII) and adhere to privacy regulations
- Helps with quality control by identifying errors or inconsistent coding, standardizing production rules, etc.

Generate Output
Run production to create required output

How Technology Can Assist
Creates output in usable, secure forms for all parties

Fulfill Request
Provide the requested data in a secure manner

Conclusion

Data Protection Compliance is more important than ever to the successful operation of organizations. In a consumer market demanding data protection and privacy competency—as well as a legal and regulatory landscape evolving into complex, cross-jurisdictional, cross-functional, and expensive compliance propositions—the simplicity of the LDI approach drives efficient and sound compliance. LDI tactics drive market strategies and enable the type of technical innovation at the heart of competition.

Data protection challenges and needs are growing and changing every day, but all key stakeholders can understand SUN data, ROT data, and the shared LDI vocabulary. Every organization can get started by defining their data protection problem both objectively and in context, then moving through the Initiate, Investigate, and Implement phases with clarity, concision, and cooperation.