



Beyond Compliance

Unlocking Enterprise Value Through Robust Data Governance

Dentons

Peter Stockburger
San Diego Managing Partner
peter.stockburger@dentons.com
619.595.8018

July 18, 2024

Data Governance Discussion

- What is data governance, and why is it an important business driver?
- What are the legal trends driving the need for robust data governance?
- What are actionable insights to raise your data governance game?





The what and the why

What is data governance?

What is data governance?

Data governance is a principled approach to managing enterprise data across the life cycle – from acquisition to use to disposal.

What is data governance?

Data governance is a principled approach to managing enterprise data across the life cycle – from acquisition to use to disposal.

Data governance can take the form of policies, procedures, training, and cultural practices within the enterprise.

Why is data governance important?

Why is data governance important?

Maximizing promise while mitigating peril.

Why is data governance important?

Maximizing promise while mitigating peril.

Good data governance maximizes the value of enterprise data and positions the enterprise to take advantage of new technologies while mitigating the compliance, legal, financial, and reputational risk that comes from getting it wrong.



Data Governance

Benefits of getting it right

- **Improved Data Quality.** Ensures accuracy, consistency, and reliability of data.
- **Enhanced Security.** Protects sensitive data from breaches and unauthorized access.
- **Regulatory Compliance.** Ensures adherence to legal and regulatory requirements.
- **Better Decision-Making.** Provides reliable data for informed business decisions.
- **Increased Efficiency.** Streamlines data management processes and reduces redundancy.
- **Risk Management.** Identifies and mitigates data-related risks.
- **Cost Savings.** Reduces costs associated with data errors and inefficiencies.
- **Enhanced Trust.** Builds stakeholder trust by ensuring data integrity and transparency.



Data Governance

Challenges to implementation

- **Organizational Culture.** Resistance to change and lack of a data-driven culture can hinder implementation. “Policy” versus “Principle”.
- **Data Silos.** Fragmented data across different departments can make it difficult to establish consistent governance practices.
- **Resource Constraints.** Limited budgets and staffing can impede the development and enforcement of data governance policies.
- **Complexity and Scope.** The broad scope of data governance, including security, compliance, and quality, can make it a complex initiative to manage.
- **Rapid Technological Changes.** Keeping up with fast-evolving technologies such as AI and data management tools can be challenging.

2024 ACC CHIEF LEGAL OFFICERS SURVEY

KEY FINDINGS



669 Participants



20 Industries



31 Countries

01

CLOs continue to face intense pressure to do more with less

Forty-two percent of CLOs say their legal department received a cost-cutting mandate over the past year. At the same time, 58 percent of departments have been impacted by law firm rate hikes, with 23 percent saying the increases have been difficult to manage. The results also show a decrease in the percentage of departments that will add staff in 2024.

02

Regulations and enforcement keep CLOs up at night

The top 3 issues that keep CLOs up at night are regulations and enforcement (53 percent), privacy and data security (41 percent), and cybersecurity threats (37 percent). Outside of the US, talent retention is the top issue (42 percent).

03

Data breaches are the biggest data-related threat CLOs want to mitigate in 2024

Thirty-four percent of CLOs say that data breaches are the biggest data-related threat that they are focused on mitigating in 2024 and 40 percent say they plan on instituting new processes to help defend against these threats, yet just 9 percent are "very confident" in their organization's ability to mitigate emerging data risks.

04

CLOs rank operational efficiency as their top strategic initiative

Forty percent of CLOs rank operational efficiency as their law department's top strategic initiative for the coming year, followed by the "right-sourcing" of legal services (15 percent), and talent management/retention (10 percent).

05

The majority of CLOs experienced an increase in workload over the past year

Fifty-nine percent of CLOs say their workload has increased over the past year and just three percent say their workload has decreased. Fifty-nine percent say they are happy with their work-life balance, but only 20 percent among those who experienced a significant increase in workload say they are happy.

06

The majority of CLOs oversee at least three additional business functions beyond legal

Fifty-eight percent of CLOs oversee three or more additional business functions beyond legal and 27 percent oversee five or more. These most commonly include areas such as privacy (44 percent), ethics (43 percent), and risk (38 percent).

07

Most CLOs believe that artificial intelligence (AI) will have a positive impact on the profession

Sixty-seven percent of CLOs believe that AI will have a "mostly positive" or "somewhat positive" impact on the in-house legal profession, with 35 percent saying that the applications with the most potential will be in document analysis, and 28 percent saying drafting documents.

08

CLOs want their staff to develop greater business acumen

Sixty-three percent of CLOs say they are seeking to develop greater business acumen among the lawyers in their department, followed by communication skills (51 percent), and executive presence (45 percent).

09

Three out of four CLOs are involved in leading their organization's ESG strategy

Despite 77 percent of CLOs being involved in leading their organization's ESG strategy, just 29 percent say they are "very involved", and 36 percent say they are "somewhat involved." Nineteen percent say their organization has no ESG strategy in place at all.

10

The Chief Legal Officer title is becoming more common

Twenty-eight percent of participants hold the "Chief Legal Officer" title. Although "General Counsel" is still the most common title, there has been a reduction in its usage among respondents, with 57 percent now holding this title compared with 66 percent in 2022.

AI Example

Generative AI tools are expanding, opening doors to opportunity

Text, Audio,
and Visual
Generation



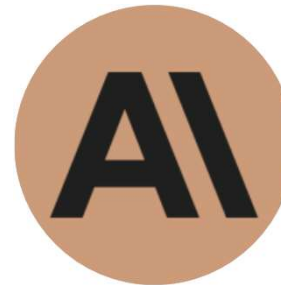
OpenAI
Chat GPT



Google
Bard



Meta
Llama



Anthropic
Claude



Microsoft
Bing

Enterprise
Tools



IBM
WatsonX



Microsoft
Copilot



Adobe
Sensei

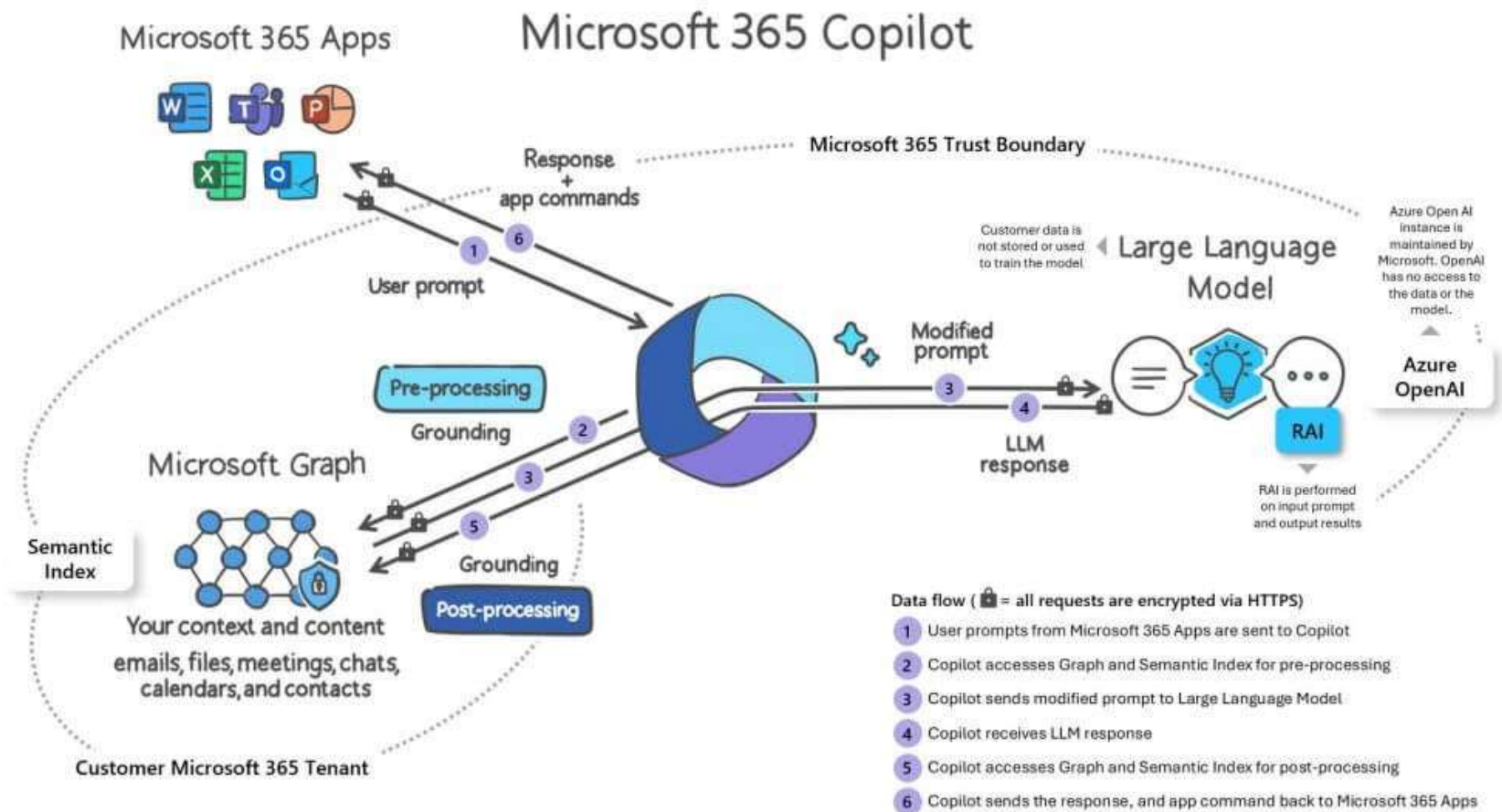


ChatGPT
Enterprise



GitHub
Copilot X

Data Governance Challenge - AI



Data Governance

Four Pillars (All Hands On Deck – Legal, HR, Privacy, Security...)

Mapping

- What data do we have, and where is it stored?
- How is data being used?
- What is our future looking use case for data?

Classifying

- How will different types of data be classified? Confidential? Personal? Sensitive?
- What are the access controls / use limitations on certain classified data sets?
- How can we address unstructured data?

Governing

- Do we have a policy minimizing the amount of data we collect and how we use it?
- Are we mapping where data exceeds its original purpose? Do we have clear use guidelines?
- Are there data sets that present value propositions that have not yet been considered?

Retaining

- Do we have a schedule governing how business records are kept and stored?
- How long do we need data, and how do we execute on retention schedules?
- How do we get participation and shift the culture?



The legal challenge



Legal Requirements

A Shifting Landscape

- **Historic Trends.** Data governance has largely been seen as a business need (IP protection, trade secret) and a security need (cybersecurity protections).
- **New Landscape.** New and emerging data privacy laws, regulatory positions, litigation trends, and shifting rules around AI are introducing data governance as a legal imperative and compliance imperative. It's no longer a nice to have – it's now a must have.

The Global Trends

- [North America](#). The US and legal markets are quickly shifting their approach to data collection and use, and privacy laws evolving. Trade secret laws are also complex.
- [Europe](#). The GDPR and related data rules focus on having a legitimate basis for collecting and using data and impose strict data minimization standards. Data transfers are also of critical importance.
- [Asia & Latin America](#). These jurisdictions have growing data privacy regimes that increasingly require data minimization by design and data localization considerations.
- [India](#). India is quickly becoming a hotbed for data regulation, including a new national data privacy law slated to take effect this year. Data minimization and governance are central to compliance.



US Privacy Compliance Challenge

Federal

Unfair
Business

Children

US Federal Financial Laws

US Federal Healthcare Laws

FTC Act

COPPA

Fair Credit
Reporting Act

GLBA

HIPAA

HITECH

State

Data breach

Consumer
privacy laws

Health
information

Cybersecurity

Surveillance
laws

Biometric
information

Insurance
information

Financial
information



US Federal Trends

Data Governance Trends

- **Regulatory focus on notice & consent.** The FTC and state regulators are increasingly focused on requiring expanded and detailed notice, as well as obtaining consent regarding the collection of data.
- **AI guidance requires fidelity to data.** The FTC and other regulators are focused on the use of AI, how it's being disclosed, and the limitations on use for certain populations.
- **Data Minimization.** The concept of data minimization is on the rise in the US.



US State Trends

Data Governance By Law

- **20 Omnibus Data Privacy Laws.** Data minimization is now being written into the law.
- **Notice & Consent Requirements Are Expanding.** An expanding litigation landscape, regulatory and legal changes, and consumer expectations are changing how notice and consent is managed. Good data governance can capture these changes and react in line with business needs.
- **Data Security Obligations.** New and emerging state laws are imposing security requirements on a broader set of data (i.e., not just sensitive data). How will that impact your controls?
- **Trade Secret Protections.** AI introduces new complications with trade secret protection and maintaining confidentiality over data.



APPLYING DATA MINIMIZATION TO CONSUMER REQUESTS

SUMMARY

- Data minimization is a foundational principle in the CCPA. Many aspects of the CCPA's implementing regulations underscore this principle.
- Businesses must apply 11 CCR § 7002(d)—in coordination with other applicable sections of the CCPA and its implementing regulations—for each purpose for which businesses collect, use, retain, and share personal information.
- Data minimization principles apply to the processing of consumers' CCPA requests.

ENFORCEMENT OBSERVATIONS

Data minimization is a foundational principle in the CCPA. Businesses should apply this principle to every purpose for which they collect, use, retain, and share consumers' personal information.

Data minimization serves important functions. For example, data minimization reduces the risk that unintended persons or entities will access personal information, such as through data breaches. Data minimization likewise supports good data governance, including through potentially faster responses to consumers' requests to exercise their CCPA rights. Businesses reduce their exposure to these risks and improve their data governance by periodically assessing their collection, use, retention, and sharing of personal information from the

US Trends

Data Minimization

- **Data minimization is the focus.** The regulators are zeroed in on this principle.
- If your organization collects or processes personal information beyond what is reasonably expected, **consent may be required.**
- This new principle requires **careful oversight** regarding data collection and use.



Case Example

Sephora

- August 2022, California AG announced a settlement with **Sephora** under the California Consumer Privacy Act (CCPA).
- After conducting an enforcement sweep of online retailers, the AG alleged Sephora failed to disclose to consumers that it was **selling** their personal information, failed to process user requests via a global privacy control, and did not cure these violations.
- Specifically, the AG **alleged** the use of third-party tracking technologies constituted a “sale” of personal information, and users were not given appropriate rights.
- Sephora **agreed** to pay \$1.2m in penalties and comply with important injunctive terms, including providing mechanisms for users to opt-out.



Case Example

DoorDash

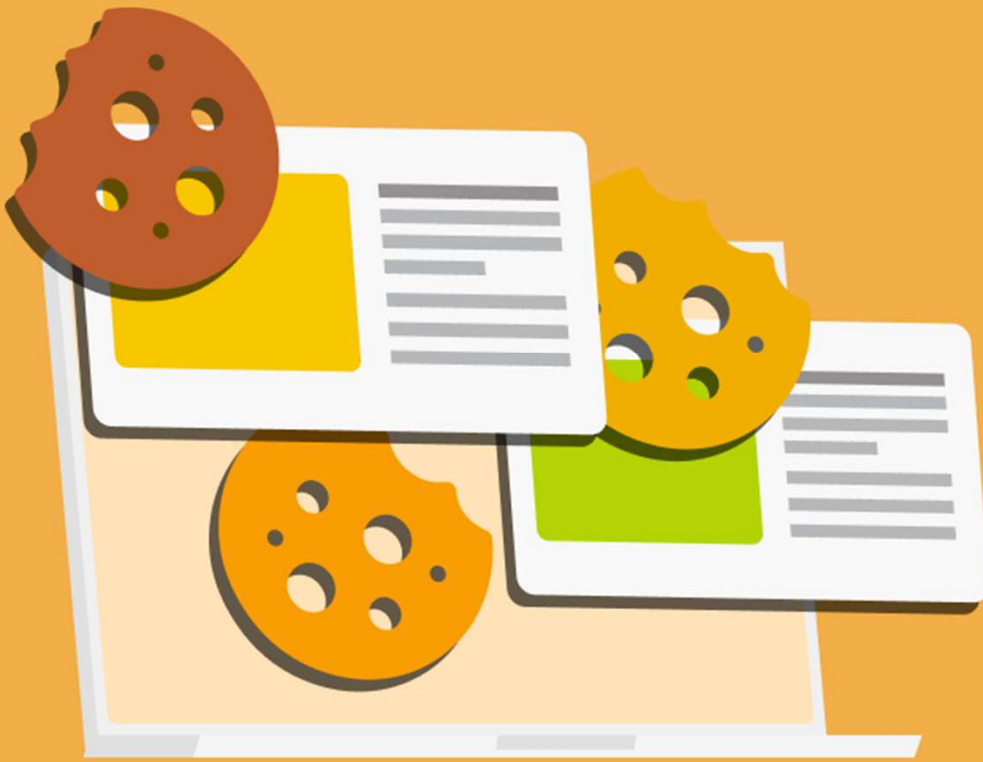
- The California AG announced a settlement with DoorDash under the CCPA and California Online privacy Protection Act (CalOPPPA).
- Allegation that DoorDash was selling customer personal information **without notice or an opportunity to opt-out**.
- Alleged **DoorDash participated in a marketing cooperative** where businesses contribute personal information of customers in exchange for the opportunity to advertise.
- **\$375,000 penalty plus injunctive relief**, including a duty to provide annual reports to the AG re: ongoing sale or sharing of consumer personal information.



Case Example

Tilting Point Media

- Case brought by **California AG** and **Los Angeles City Attorney**.
- Alleged Tilting Point Media collected and shared children's data without appropriate consent in violation of the **CCPA** and **COPPA**.
- Specific allegation of **misconfiguring the SDK** leading to children's data being collected.
- Settlement for **\$500,000 and injunctive relief** (including implementing and maintaining an SDK governance framework to review the use and configuration of SDKs within its apps).
- **Lesson Learned:** Don't skip the SDKs.



Litigation Risk

Rising Claims

- **Cookies & Pixels.** A growing wave of suits are alleging the use of cookies and pixels constitutes unlawful wiretapping, eavesdropping, and the use of a wire tap.
- **Cookie Functionality.** Lawsuits are alleging that the cookie choice function doesn't work as advertised (false advertising, unfair business practices).
- **Payment Processors.** Lawsuits are alleging that the use of a third-party payment processor on a check-out page runs afoul of the law.
- **Credit Card Claims.** Lawsuits are alleging that the collection of additional information at check-out is a violation of the Song-Beverly Credit Card Act.



Additional Issues

Security, IP, Claims, Liability

- **Security Requirements.** Mapping assets, structuring appropriate controls, and having visibility into threat landscape are critical components.
- **IP Protection.** Copyright, patent, and other IP / confidentiality protections requires full visibility into data and access controls.
- **Trade Secrets.** Trade secrets must be identified, kept private, and have limited access. This process requires fidelity and tight data governance.
- **Claims and Liability.** Having good data governance positions the enterprise to defend against myriad claims.



Raising your data governance game



Action Items

Driving Data Governance

- **Mapping Exercise.** Walk before you run. Gather the right data, talk to the right teams, and map your use cases. Use the interviews to drive trust and engagement.
- **Policy Exercise.** What do your policies around data classification, retention, and minimization look like? Before you can classify, you need to identify.
- **Classification.** Ensuring the appropriate classification around data is critical to executing a data governance program. This is not an easy lift.
- **Train and Execute.** Good data governance is only as effective as the front-line employees. Shifting culture is critical. It's enterprise not just IT. Gamifying sometimes helps.
- **Iterate and Innovate.** Data governance is not a static process. Effective data governance requires constant vigilance, iteration, and innovation.
- **View Data Governance As An Opportunity Driver.** Data governance is a principled approach, not a checklist. Maximize promise, mitigate peril.

The Dentons logo, consisting of the word "DENTONS" in a bold, sans-serif font, enclosed within a white arrow-shaped border pointing to the right. The background of the slide is a deep purple with a subtle, abstract pattern of overlapping circles and lines, creating a sense of depth and movement.

DENTONS

Thank you!

Dentons is designed to be different. As the world's largest global law firm with 12,500+ professionals in over 160 locations in more than 80 countries, we can help you grow, protect, operate and finance your business. Our polycentric and purpose-driven approach, together with our commitment to inclusion, diversity, equity and ESG, ensures we challenge the status quo to stay focused on what matters most to you. www.dentons.com.

© 2024 Dentons. Dentons is a global legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.