Jordan Lawrence®

Top 10 Data Privacy & Cybersecurity Questions for In-House Counsel

PREPARING FOR REGULATORY COMPLIANCE

KEY QUESTIONS FOR A DEFENSIBLE POSTURE

Jordan Lawrence®

Top 10 Data Privacy & Cybersecurity Questions for In-House Counsel

1. Why should legal lead the charge on data privacy & cybersecurity?

Compliance with data privacy and cybersecurity regulations has become a predominant issue for corporate legal executives. GCs and CLOs are making company critical decisions when it comes to compliance. Kevin LaCroix of The D & O Diary advised, "*General Counsel should view cybersecurity issues with the same healthy skepticism they employ for other areas of risk.*"

One of the primary responsibilities of in-house counsel is identifying and mitigating potential risks to the company. Data privacy and cybersecurity regulations and risks top the list of concerns. Companies can't eliminate all data privacy and cybersecurity risks, but Legal can help ensure reasonable processes are in place to address risks, comply with regulations, and mitigate potential legal liabilities.

"*In 2019, CLOs have their eyes on data. Data breaches, regulatory changes, and information privacy top the list of concerns for CLOs in 2019.*" - 2019 ACC Chief Legal Officer Survey

2. What about personal liability?

All companies, their directors and officers, including the GC, are at increasing risk of becoming the subject of regulatory actions from state and federal authorities as well as litigation driven by the plaintiffs' bar brought about by customers, employees, and shareholders. You must be prepared to defend your company, your practices, and your directors. You don't have to look any further than the Yahoo data breach and Equifax for what liability companies and their top executives face in the wake of data breaches. These issues have the potential to be career-enablers or career-enders for in-house counsel.

3. Do we really know what personal data we have and where it exists?

How you develop and maintain your data inventory directly impacts your ability to meet your compliance obligations, demonstrate an effective level of diligence with regulators, and defend your compliance efforts against plaintiff's attorneys. Companies that have taken a limited approach and only identified personal data in applications or databases fall short of their compliance obligations. You must know where your data is to protect it, delete it, report on it, or produce it.

Donna Wilson of Manatt pointed out in a recent webcast that, *"[Data mapping is] a best practice regardless of the GDPR or the CCPA".*

4. Can we respond quickly and compliantly to data access requests?

Data access requests from current employees, past employees, job candidates, customers, and others will be a costly discovery, regulatory, and litigation minefield for companies that don't know where personal data exists or what third parties access their data, or those that vastly over-retain data. Successfully navigating and responding to data access requests requires organizations to have a comprehensive understanding of where personal data exists – and it's going to be in a lot of places, many of which will surprise you.

5. **Are we retaining personal data longer than necessary?**

Companies must understand what personal data they have, legitimate business needs to retain data, and any legal or regulatory obligations to retain data. The safest approach is to not retain personal data longer than necessary. You can't lose personal data you don't have, and you don't have to produce it (for data access demands or in litigation). Over retention of personal data will not be defensible. Companies that fail to undertake data minimization efforts will face severe regulatory or legal consequences if unneeded personal data is breached.

"*If you experience a data security incident or a data subject rights request (e.g. a subject access request), then you will be sitting on top of an awful lot more affected data - and the resultant risks, costs, and negative PR in responding to the incident or request will be substantially greater.*" Phil Lee Field Fisher, To Keep or Not To Keep: Data Retention Challenges and Solutions

6. **Which of our third parties (including law firms) are relevant to regulations?**

Third-party vendors are one of the fastest-growing risks to your company's sensitive and personal data. Yet most companies don't know which of their third parties are accessing their personal data – much less how they are protecting it. A recent Ponemon report found that **only 34%** of respondents say they have a **comprehensive inventory of all their third parties.**

Legal executives must ensure an effective vendor risk profiling process is in place to understand the nature of vendor relationships and the specific types of personal data your third parties access, process, or store. A failure, violation, or breach caused by one of your third parties can result in regulatory actions, penalties, and litigation. You can't afford the risk.

7. **Are our third parties protecting us and our data?**

Statistics from a recent Ponemon report confirm that vendors are increasingly a concern for companies' data privacy and cybersecurity practices, and resources to address this concern are often limited or focused elsewhere.

- **61 %** of US respondents confirm that their organization experienced a **data breach caused by one of their third-parties**.
- **76%** of respondents say the **number of cybersecurity incidents involving vendors** is increasing, but **only 46%** of respondents say **managing outsourced relationship risks** is a priority.
- **57%** of respondents do not know if their organizations' **vendor safeguards** are sufficient to prevent a breach.

8. **How will we respond in the event of a breach or regulatory violation?**
When a breach happens, law enforcement will ask, "What information was breached?" The regulators and plaintiffs' attorneys will ask a different question. They will want to know, "What did you do to try and prevent the breach or violation?" You need a be positioned to demonstrate reasonable diligence in meeting your regulatory obligations and mitigating risks.

9. **What's the potential for litigation?**
Savvy plaintiffs' attorneys are exploiting the rapidly changing data privacy and cybersecurity landscape. Private rights of action, statutory fines, and new theories of liability are supercharging litigation against companies of all types and sizes – and they never saw it coming.

"*There is a growing campaign by the plaintiffs' bar to target data privacy and security in the hopes of striking it rich in a new goldmine on the level of the asbestos litigation of the 1970s, 1980s, and 1990s. Class action lawyers are pursuing data privacy cases and amassing fortunes even where no one has been harmed*." – Engineered Liability

"The statutory damages potentially available under the CCPA will likely provide strong motivation for the plaintiffs class action bar to test its scope." - Ian Ballon and Rebekah Guyon

10. **Are we prepared for new regulations on the horizon?**
The regulations and privacy bill proposals currently under review are only the tip of the iceberg. As consumers become increasingly concerned with their privacy and the security of their data, we will continue to see data becoming more heavily regulated. CCPA copycat laws are quickly emerging. A recent JD Supra article provided an overview of all of the potential CCPA look-a-like laws under review; "*Legislators in nine states have introduced draft bills that would impose broad obligations on businesses to provide consumers with transparency and control of personal data. Of the nine states, six follow the full model established in the CCPA*."

"*All data is increasingly becoming regulated data, even without national-level data regulation.*" – Andrew Burt, The Hill

Jordan Lawrence®

About Jordan Lawrence

For over 30 years, Jordan Lawrence has been helping companies manage their information compliantly, defensibly, and cost effectively. We work with many of the world's leading organizations to ensure they effectively meet their obligations, mitigate risks, and reduce the costs of overall information compliance and control.

Legal, compliance, privacy, and IT teams at companies from Avis to Wyndham rely on us to help them meet expanding legal and regulatory obligations for data privacy, data minimization, and third-party diligence. We leverage over three decades of deep domain knowledge, robust frameworks and standards, and a proprietary service delivery model to provide predictable, practical, and defensible results for our clients.

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

ACC ALLIANCE
Exclusive Savings for ACC Members

Exclusive ACC Alliance Partner for
Data Privacy & Cybersecurity Compliance

Contact Us for More Information:

636.778.1700
services@jordanlawrence.com