Data privacy compliance 101:

A guide for corporate legal

SimpleLegal

Introduction

In a 2020 Exterro study, general counsel listed "complying with new data privacy laws" as a top priority.

Despite this, corporate noncompliance fines from violating the European Union's General Data Protection Regulation (GDPR) shot up seven times higher by 2021. What's causing the disconnect?

We'd argue that while most GCs know data privacy compliance is critical for managing risk, it can be difficult to figure out what they actually need to do about it.

Until just a few years ago when data privacy regulations like the GDPR started emerging, IT departments handled anything data-related — including compliance. But now, as Exterro's Dan Sholler notes, this growing "focus on data" has forced top legal leaders "to take on the job of managing this big hunk of risk." This is a whole new world for GCs, who have to learn the ins and outs of this complex area while juggling a variety of additional responsibilities.

Keep this risk management manageable by first mastering the basics of data privacy compliance and learning five key strategic actions to take.

The major consequences of data privacy noncompliance

The most glaring consequence of noncompliance with data privacy laws is the financial impact of fines. However, the related damage to a business's reputation also negatively affects the bottom line.

Steep regulatory fines

To impart the seriousness of noncompliance and serve as a warning to companies, data privacy regulations intentionally include major financial penalties for businesses that violate the laws. The **GDPR website** clearly notes that "stiff fines are aimed at ensuring best practices for data security."

As the most stringent and comprehensive data privacy regulation currently out there, the GDPR has the most extreme penalties.

> **GDPR fines can be up to**
> **$22.8 million or 4% of a company's global turnover**
> **whichever is higher.**

While **fines vary across regulations** and may be less punitive than GDPR penalties, the point remains: companies that don't take steps to ensure compliance will face financial losses that could've been prevented. And with more organizations operating on **tighter margins in the wake of COVID-19**, even smaller financial hits can jeopardize the health of a business — and your place within it.

Reputational damage and loss of trust

Even if it's not intentional, any violation of data privacy regulations will negatively impact your company's credibility. According to KPMG's 2021 Corporate Data Responsibility report, most consumers are worried about the amount and type of **personal data organizations collect** from them. Additionally, 40% already don't trust that businesses use data ethically. Instances of noncompliance reinforce these concerns, resulting in lost customers, investors, and revenue.

88% of consumers won't buy from or work with **brands they don't trust.** And with word traveling so fast in the digital world, companies that violate data privacy regulations lose support fast.

For example, Target — which is well known for its loyal, **high-spending consumers** — reached a historic low in **consumer perception** after their 2013 data breach, which they delayed in telling consumers about. And across organizations, shares decline **3.5% on average following a data privacy event**, according to a Comparitech study.

The fundamentals of data privacy laws

Since there's currently no **federal law governing data privacy in the United States**, the best way to develop a general understanding of the basics of these regulations is to look at GDPR compliance. While other U.S. federal and state laws differ in specific instructions across industries, the GDPR's core elements apply across them and give GCs a solid framework to keep in mind.

The GDPR lays out 7 key principles for businesses to follow when handling sensitive data.

01 Lawfulness, fairness, and transparency

Companies must collect consumer data through legal means, offer consumers the clear option to choose if their data will be collected and used, and tell them up front why and how they collect, store, and use data.

Violation: Google was fined **$120 million** after placing tracking cookies on Google France without giving users a clear avenue to opt out.

02 Purpose limitation

Companies must use collected data for its originally intended purpose. So, companies can't say they're collecting user information for a newsletter when they're actually collecting it to sell to a third party.

Violation: Bankia was fined around **$55,180** after retaining data for over 16 years from an individual who was no longer a client.

03 Data minimization

Companies must only collect information relevant to their explicitly stated objective. For example, if a retail company was collecting information to register users for an online rewards account, asking for their name and email would make sense. However, they couldn't ask for their social security number or mother's maiden name.

Violation: Online retailer Spartoo was fined nearly $276,000 for collecting consumer bank and health insurance information while recording customer service calls.

04 Accuracy

Companies must keep customer data records updated and take proactive steps to correct inaccurate entries.

- **Violation**: Equifax was hit with a **$1.1 million fine** for multiple violations, including repeatedly contacting individuals who had already paid what they owed.

05 Storage limitation

Companies must delete or anonymize data after it serves its intended purpose

- **Violation:** Insurance company AG2R La Mondiale was fined approximately **$1.9 million** for keeping records of 2,000 individuals past the industry's maximum 3-year retention period.

06 Integrity and confidentiality (security)

Companies must take adequate security measures to protect sensitive information and must also have backup systems in place to preserve data. These methods vary across companies but generally include a combination of cyber and physical defenses like proper encryption, login authentication, and file shredding and disposal.

- **Violation:** British Airways was fined **$26 million** after a data breach compromised personal information from 420,000 consumers and employees.

07 .Accountability

Companies must be able to show the actions they've taken to maintain regulatory compliance, including work with third parties. Proper documentation is especially critical in case of something like a data breach, when companies are legally required to disclose the details of the event, what safeguards were in place, and what remediation is happening.

- **Violation:** Enel Energia was fined $30.1 million for, among other violations, a failure to "prove compliance with data protection laws in relation to unwanted promotional calls carried out by a business partner and for its failure to carry out the required checks on the activities of its business partners," according to DataGuidance.

For an even deeper dive into each principle, visit the Information Commissioner Office's website.

5 ways to ensure data privacy compliance

As former The Globe and Mail GC Sue Gaudi notes, "privacy is a compliance matter, of course, but it is also a culture issue." To minimize chances of noncompliance, data privacy needs to be a company-wide priority. And how much time, focus, and money an organization invests in ensuring compliance with data privacy laws will ultimately determine how effective those measures will be.

01 Stay updated on regulations

You don't know what you don't know, but for GCs, what you don't know can devastate your company. As your company's expert on interpreting and applying laws, you need to have a solid understanding of the data privacy regulatory landscape so you can feel confident in checking off legal requirements.

Take 30 minutes out of your week to brush up on major regulations like the GDPR and the California Consumer Privacy Act (CCPA), and read up on any additional industry-specific laws your company needs to comply with, like healthcare's Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. By doing this now, you can save yourself from dealing with a breach that eats up significantly more of your time — one breach takes an average of 287 days to completely resolve.

Here are some quick tips to speed up the learning process:

1. Sign up for the Law360 Cybersecurity & Privacy section newsletter for coverage on recent cases.
2. Follow the American Bar Association (ABA) Privacy and Data Security Committee and check out the ABA Journal's Privacy Law section.
3. Subscribe to blogs and email newsletters from notable firms with cybersecurity practice areas, such as Hunton Andrews Kurth.
4. Register for cybersecurity and data privacy CLE webinars with local and state bar associations.

If you need additional context on a topic, reach out to your IT department! Since you're working together to mitigate risk, exchanging knowledge is key to successful collaboration.

02 Establish or review your privacy and tracking policies

Violations of the GDPR's "lawfulness, fairness, and transparency" principle make up a significant number of the **top fines to date**, with most of them connected to a lack of clear consent regarding tracking cookies and vague privacy policies. However, in terms of the resources that go into maintaining compliance, creating and updating these crucial notices is a relatively easy lift.

As DLA Piper **outlines**, the key to avoiding those penalties is to follow this general guideline: "Provide notice to individuals, at the time of collection of their data, about what is being done with that data: who is collecting it, why, where the data is going and to whom." Go check out your business' current language surrounding cookie opt-ins and how the company explains its data usage to ensure it meets the mark.

If you don't have a clearly defined privacy or cookie policy on your company's website, take a break from reading this article and go write a draft — it's that important.

03 Work with IT to audit current data management practices

GCs and IT need to work together to minimize risk. The best starting point is to collaborate on a thorough data management audit to identify vulnerabilities in terms of both compliance (GCs) and cybersecurity (IT).

Most people tend to think solely of consumer data when it comes to data privacy issues, but employee data is just as vulnerable. As noted in **Forbes**, data privacy lawsuits from employees are growing, along with "the willingness for courts to punish employers" who fail to protect their employees' sensitive information.

Use your understanding of regulatory requirements as a benchmark to evaluate if consumer and employee data storage, access, usage, and protection measures are compliant. And don't worry, IT can walk you through all of the different data types and processes before turning their attention to technical vulnerabilities. These come in many forms, from homegrown and legacy software built on risky "**spaghetti code**" to unsecured **virtual private networks (VPNs)** for remote work.

After you both finish your review, you can go over the findings and start drafting a follow-up plan to address the most urgent priorities first.

04 Help create formal data management policies and employee training

As we mentioned, under the GDPR's "accountability" principle, companies need to be able to show what steps they've taken to maintain compliance. Documented policies and procedures make it much easier to train employees on best practices, and they also serve as a record of your company taking action.

From breaking security rules to phishing, human error is the **most common cause of data breaches**. Even so, IT leaders ranked it at the bottom of their list of concerns in **Egress' Insider Data Breach Survey 2021**. So, employee training is an underutilized tactic for improving data security, but it's key to a strong cyber defense. Work with IT and human resources to oversee robust, mandatory training initiatives on company cybersecurity policies and best practices.

Your best chance of minimizing risk and potential liability is to include the following in training materials:

- What data can and can't be accessed or shared by employees (and why)
- Cybersecurity guidelines for remote work
- How to identify phishing scams and examples
- Best practices for creating strong passwords and avoiding password reuse
- Brief summaries of applicable data privacy laws
- Relevant industry examples of data breaches caused by humor error
- Clear explanations of the ramifications of violating company cybersecurity policies
- Who to contact with concerns about any suspicious cyber activity

Additionally, make sure the training takes them through real-world scenarios where they have to apply their knowledge to pass. As cyber education company Cybint **notes**, training will be of the most value when you "not only focus on what employees should know but what they should do."

05 Bring in a third-party expert for annual compliance reviews

It's always helpful to have another set of eyes reviewing complex work, and data privacy compliance is no exception. Once you and your IT department believe your company meets its compliance requirements, have an outside vendor conduct an objective evaluation. This fresh perspective increases the chance of catching any compliance gaps, which will save you money and time in the long run. For long-term compliance, try to bring experts in at least once a year.

Corporate legal departments that prioritize data privacy compliance will stay ahead of the curve

As technology continues to advance and change, so will data privacy regulations. Efforts to proactively ensure compliance and create a cybersecurity culture will help you lower risk for companies while proving **your team's value** as forward-thinking strategists.

About SimpleLegal

SimpleLegal provides a modern legal operations management platform that streamlines the way corporate legal departments manage their matters, track and interpret spend, and collaborate with vendors and law firms. SimpleLegal combines e-Billing and spend management, matter management, vendor management, and reporting and analytics into one comprehensive application to optimize legal operations and the management of the entire legal department.

For more information visit: www.simplelegal.com