LEADING THE CHARGE FOR REGULATORY COMPLIANCE
# TABLE OF CONTENTS

1 EXECUTIVE SUMMARY  
2 WHY DATA AND DATA EXPERTISE MATTER NOW MORE THAN EVER  
3 A REGULATORY SEA CHANGE  
   a: GDPR  
   b: CCPA  
4 THE WAY FORWARD: Building a Future-Proof Data Governance Strategy for Today and Tomorrow’s Compliance Requirements  
5 DATA GOVERNANCE LEADERSHIP: How Acxiom Can Help
EXECUTIVE SUMMARY

Trust for brands is more important than ever, and nowhere is that more critical today than in how brands use consumer data.

Witness the current state of data privacy and regulations, such as the EU’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Governments, privacy advocates and consumers want to know what data is being collected, how it is being used and with whom it is being shared. Data governance is key to ensuring continued responsible use of data and engendering trust in your brand.

In this eBook, Acxiom shares insights into best practices for managing global data and the importance of building a strategy around a strong data governance program.

YOU WILL DISCOVER:

- Ways to create a lasting data governance strategy to protect the consumer and your business
- Key implications and best practices for managing global data
- How CCPA and other privacy laws will change our future and how brands need to prepare for today and tomorrow

Consider CCPA an opportunity to...

…Connect and build a better relationship with consumers

…Create a customer-first foundation for everything your company does relating to data.
WHY DATA AND DATA EXPERTISE MATTER NOW MORE THAN EVER

Today we live in a digitally oriented, data-driven economy supported by advertising. According to GE Digital, the production of new data continues to explode with 2.5 quintillion bytes of data created each day at our current pace. By 2020, it’s estimated that 1.7MB of data will be created every second for every person on earth.¹

The Data-Driven Marketing Institute (DDMI)² has estimated that the data-driven marketing economy generates nearly 22 million jobs in the United States and adds more than $200 billion in revenue to the U.S. economy. Global advertising spend is forecasted to reach $790 billion by 2023, showing the worldwide impact is even more significant.³

Data fuels innovation. And every year more and more innovative products and services appear in the marketplace. Businesses, regulators, advocates and many consumers acknowledge the benefits that accrue to the consumer and to companies from data sharing. Consumers learn about all kinds of new and beneficial products and services. They receive special deals on products and services they are more likely to be interested in and receive fewer unwanted offers (i.e. spam or junk mail). Ever-connected consumers now expect brands to know them across every touch point and to deliver relevant messaging along the way.

 Responsible use of data means companies profit from a greater return on their marketing investment, and small businesses enjoy cost-effective access to prospects to grow their companies. It’s vital for consumers and businesses alike that we continue to share data for marketing purposes.

MORE THAN 70% of marketers say their investments are driven by customer expectations of more personalized and relevant brand interactions.²
A REGULATORY SEA CHANGE

The world has transformed into an era of constant connection. The escalation of connected devices and creation of data will expose gaps in companies’ ethical codes of conduct that they will need to address. We have seen this escalation trigger a snowball effect in the introduction and enforcement of new legislation, not only in the European Union, where privacy is viewed as a fundamental right, but also in the U.S.

83%

The portion of internet users worldwide who said they are concerned about their privacy.¹

Symantic, The Harris Poll
GDPR, which took effect in May 2018, began the wave of legislation focused on data privacy and consumer protection and was designed to harmonize data privacy laws across Europe and protect EU citizens from privacy and security breaches. GDPR applies to non-EU companies that offer goods or services or monitor an individual’s behavior in the EU. Among other things, it requires increased transparency, access, rectification and erasure.

GDPR has already had an eye-opening impact. European Data Protection Authorities (DPAs) have rushed to enforce GDPR, in some cases imposing fines of more than 50 million Euros. Perhaps more unsettling, some EU DPAs that were historically inactive from an enforcement standpoint are now very aggressive in bringing enforcement actions. In the U.S., there are at least 15 states considering CCPA-style legislation.

Cookies and Tracking (ePrivacy): The EU ePrivacy Regulation is another legislative effort to update privacy laws in Europe. It replaces the current ePrivacy Directive and sets out specific rules on direct marketing, online tracking — including cookies but expanding to include any method of device or browser tracking — and confidentiality of communications. The latest draft proposal imposes a mandatory requirement that all websites or apps ask users for opt-in consent to tracking, along with an obligation for browsers to offer tracking consent options upon installation.

Data Transfers Between the EU and the U.S. (Privacy Shield): Privacy Shield is an agreement for maintaining the flow of data between the EU and the U.S. It is a successor to a previous agreement called Safe Harbor, which was struck down in 2015 by the EU Court of Justice due to a lack of protections against U.S. surveillance practices. Privacy Shield certification began in August 2016.\(^5\)

---

**GDPR (General Data Protection Regulation)**

<table>
<thead>
<tr>
<th>WHERE</th>
<th>The European Union</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHAT</td>
<td>General Data Protection Regulation (GDPR) is designed to:</td>
</tr>
<tr>
<td></td>
<td>• Harmonize data privacy laws across Europe</td>
</tr>
<tr>
<td></td>
<td>• Protect EU citizens from privacy and data breaches</td>
</tr>
<tr>
<td>WHO</td>
<td>Applies to companies in the EU and to non-EU companies that offer goods or services to EU citizens or monitor behavior in the EU</td>
</tr>
<tr>
<td>WHEN</td>
<td>Enforcement began in May 2018</td>
</tr>
<tr>
<td>HOW MUCH</td>
<td>Companies that fail to comply can be fined up to 20 million Euros or 4% of their annual global turnover (i.e. revenue), whichever is greater.</td>
</tr>
<tr>
<td></td>
<td>It is imperative that organizations understand the changes needed to comply with GDPR and to have dedicated data privacy officers in each region of the world to stay on top of local privacy and regulatory changes.</td>
</tr>
</tbody>
</table>
On June 28, 2018, California signed into law the California Consumer Privacy Act, which grants California consumers new rights regarding the collection and disclosure of information about them. The CCPA also imposes a number of obligations on companies doing business in California regarding the type of notice and control they must give regarding the collection and disclosure of personal information. When the law goes into effect January 1, 2020, it will effectively apply to companies that either: 1) have annual gross revenue of more than $25 million; 2) have annually bought or received for commercial purposes personal information on at least 50,000 California residents; or 3) have derived 50% or more of their revenue from selling consumer information.

Fueled by today’s digital ecosystem, the questions surrounding responsible data collection and management will only increase, and rightly so. Many states have proposed or will be proposing consumer privacy legislation. Several coalitions, including the U.S. Chamber of Commerce and the Business Roundtable, are proposing frameworks for a national privacy law, but we do not expect passage of one before 2021. Therefore, it is imperative that companies start, if not accelerate, their CCPA compliance now.

WHAT ARE THE KEY REQUIREMENTS OF CCPA?

Among other things, covered businesses will be required to provide California residents with:

• Access to the types and sources of personal information collected about them
• The specific pieces of personal information collected about them
• Access to the categories of personal information about them that has been sold or disclosed
• The types of entities with which the personal information was shared
• The ability to delete a consumer’s personal information and to opt out of future data sales and sharing

Consumers will also have a limited private right to pursue actual or statutory damages in the event a company suffers a security breach that results in exfiltration, theft, or disclosure due to a failure to implement and maintain reasonable security procedures and practices.
Though CCPA is a state-specific law, companies should begin to think in terms of future-proofing data compliance by building in best practices to allow them to nimbly respond to new and changing regulations as additional state, and eventually federal, regulations come into play – and they most certainly will.

Importantly, a company’s data governance framework should be built to respond not only to CCPA but provide the foundation for responding to the varying regulations that are sure to follow. It should anticipate likely extensions in the laws, such as giving consumers the ability to change their data, not merely delete it or opt out.

A CCPA CHECKLIST INCLUDES THE FOLLOWING STEPS:

- Determine if you’re a business collecting or selling consumers’ information
- Review transparency, notice and non-discrimination obligations
- Create a data inventory that tracks the flow of personal information throughout the data lifecycle and categorize it
- Update your website in accordance with CCPA requirements to post “Do Not Sell My Personal Information” on your homepage
- Be able to respond to consumers’ personal information access requests
- Be able to respond to requests for deletion and opt out
- Educate staff with consumer response strategies and keep them up to date

THE WAY FORWARD: A FUTURE-PROOF DATA GOVERNANCE STRATEGY FOR COMPLIANCE REQUIREMENTS

BENEFITS OF AN ETHICAL DATA USE FRAMEWORK

1. Deliberate method that addresses complexity, nuance and uncovers data/analytic quality issues
2. Deliberate method that results in outcomes that are good for the brand and the consumer: legal, respectful and fair (accountability)
3. More mature organizational information governance system
4. Data governance as a competitive differentiator to protect brand trust and loyalty – and to get the outcomes right
STEP 1, SHIFT YOUR PERSPECTIVE TO THE CONSUMER

As you begin this journey, consider a shift in your perspective. Instead of viewing each new privacy regulation as just another regulation to be addressed; consider it an opportunity to connect and build a better relationship with consumers as well as an opportunity to build a data governance strategy to set the foundation for everything your company does that relates to data. Companies today no longer see data as a byproduct; they understand it is a key corporate asset to be protected and leveraged to create optimal consumer experiences.

With that said, here is a high-level look at what your compliance journey will entail.

We recommend immediately starting a process to assess the impact of the law on your operations. As a threshold matter, determine whether your company is covered by the new law. Assuming it is, determine whether any statutory exemptions apply. For example, protected health information already covered by HIPAA data is generally exempt.

Each day, **2.5 quintillion bytes of data** is created at our current pace.

**By 2020, it is estimated that 1.7MB of data will be created every second for every person on earth.**¹

The sheer volume of data being created demands that companies consider how to most effectively manage their data — what data to collect, how to collect it, how to make it accessible across the organization in a consistent manner and how to provide transparency to consumers. Setting a proper foundation can create new opportunities for collaboration and help departments work together better.
If your company is impacted by the new regulation, start assembling the relevant stakeholders (e.g. legal, privacy, marketing and operations) as soon as possible to begin auditing when, where and how you collect data and discuss the necessary changes to become compliant with the regulation. It may take significant lead time to properly identify and categorize the types of personal information your company collects and shares.

47% of those surveyed believe a federal privacy law that preempts the CCPA will not be passed by Congress over the next year or two.7

IAPP and One Trust research, April 2019
A consistent strategy for compliance can lay the groundwork you need to be agile in your response to future regulations as well.

**KEY ACTIONS TO CONSIDER IN BUILDING YOUR FRAMEWORK ARE:**

1. **Establish the key stakeholders who will approve the plan for regulatory compliance and monitor its progress.**

2. **Define clear goals for data management to facilitate full compliance with consumers’ personal information access requests.** Streamline processes for data collection and sharing. Determine what types of data you will collect and where it will come from.

3. **Identify the resources you’ll need to implement your compliance strategy, including people resources, capital investments and new processes, and gain approval to move forward.**

4. **Be cognizant of where data resides and where you will be required to bring together multiple sources for a single output to the consumer to adhere with compliance requirements.**

5. **Establish clear data governance rules and standards for managing data to eliminate guesswork around how to manipulate, analyze and use data.**

6. **Identify third parties in your marketing ecosystem that provide or handle personal data.** Determine how you will verify that agencies and vendors are compliant with legal and contractual requirements.

7. **Leverage automation and technical controls as much as possible for honoring consumer access, deletion and opt-out requests.**

8. **Determine how you will verify consumers are who they say they are when requesting access to the data you have collected.**

59% of marketers surveyed said that breaking down organizational silos would be the most important step their businesses could take to drive growth and better customer connections.⁵
A group of key stakeholders will need to closely track short- and long-term goals within your plan to monitor progress and refine the plan as it progresses.

Finally, stay abreast of ongoing developments and adapt your strategy accordingly. Use a legislative tracking service or ticker to automatically notify you of pending legislation, enforcement actions or new case law.

**MONITOR AND ADAPT**

**CONCLUSION**

Moving forward, privacy legislation, data volumes and the importance of data will only continue to increase. A thoughtful and comprehensive data governance strategy lays a foundation to future-proof your operations and allows you to respond to new and changing regulations in the coming years.

* Statements made are for informational purposes only and should not be considered legal advice.

**Sources:**

1. [https://www.ge.com/digital/blog/better-data-better-decisions](https://www.ge.com/digital/blog/better-data-better-decisions)
5. ANA Insight Brief: Global Marketing, 2017; [www.ana.net/](http://www.ana.net/)
DATA GOVERNANCE LEADERSHIP:
HOW ACXIOM CAN HELP

The technology and partners you choose are factors essential in your success in implementing an enterprise-wide compliance response. Nobody knows data like Acxiom with its 50-year history in data and identity solutions.

DATA GOVERNANCE: A HISTORY OF LEADERSHIP

Like any industry, advertising needs to operate under standards and codes that ensure the rights of consumers are protected. Worldwide, advertisers must comply with the law, be truthful, provide transparency, not mislead or deceive and be socially responsible. Other guidance applies when advertising to specific audiences, like children, or for specific products, like alcohol, health and financial products. It is our privilege and responsibility as part of this industry to carry the banner for the highest standards of ethical data use.

- Appointing first Chief Privacy Officer
- Being a voice for industry standards and self-regulation with legislators and via forums and partnerships
- Offering privacy-by-design products and solutions

Acxiom has provided consumers notice about our data collection and use practices and offered U.S. consumers the opportunity to opt out of our marketing products for many years. We also rigorously vet our data suppliers to ensure they are in compliance with the same notice and opt-out provisions. Additionally, we are obtaining our sources’ categorization of the data they provide to us as well as documentation regarding each source’s plan to respond to consumer access, opt out and deletion requests.

Acxiom offers an expansive suite of services and solutions to help brands learn about and properly plan for data protection compliance. These include a range of consulting services for data asset regulatory impact assessment – from a half-day workshop to a multi-week engagement, including a detailed data workflow, an assessment and checklist for getting started, client-specific recommendations and more. There are also identity solutions and enterprise identity graph capabilities as well as a full enterprise data management solution that streamlines a company’s ability to comply with CCPA.

Visit www.acxiom.com/ccpa to learn more.
ABOUT ACXIOM

Acxiom provides the data and technology foundation for the world’s best marketers. We enable people-based marketing everywhere through a simple, open approach to connecting systems and data to drive better customer experiences for people and greater ROI for business. A leader in identity, customer data management and the ethical use of data for more than 50 years, Acxiom now helps thousands of clients and partners around the globe work together to create millions of better customer experiences, every day. Acxiom is a registered trademark of Acxiom LLC and is part of The Interpublic Group of Companies (IPG). For more information, visit acxiom.com.