Ebiquity Report 2019

U.S. Data Privacy

Patchy preparation for GDPR shows U.S. businesses are unprepared for new legislation

In collaboration with

DIGITAL ANALYTICS ASSOCIATION

ebiquity

Overview

U.S. companies have only taken small steps to protect consumer data since the advent of the E.U.'s new General Data Protection Regulation (GDPR) in 2018, and substantial work remains to prepare for the forthcoming U.S. data protection/privacy laws.

About this research report

Ebiquity and the Digital Analytics Association (DAA) fielded a survey on GDPR in late 2018 and early 2019 (closed in February 2019). The responses come from DAA members and Ebiquity clients. Respondents represent 60 different U.S. organizations, ranging in size from Fortune 50 enterprises to mid-size companies. Responses were from various levels within the organization, from CEOs to Managers. Most responses were from personnel at the VP/Director level.

View from the Digital Analytics Association

GDPR and similar laws don't just create a new legal compliance environment for business that wishes to use personal data for marketing or analytics – they create a new ethical framework for thinking about the collection and use of this data, especially in the service of goals that the individuals who own that data may not be excited about, such as highly targeted marketing.

This report shows that, in the U.S. at least, far too many organizations are treating GDPR as a minimum-bar compliance issue, taking actions such as restricting users from the E.U. which are unlikely to deliver longer-term compliance with the laws that are being put in place internationally, as well as doing damage to their brands and core businesses.

The DAA encourages our members, and any organization that is using personal data, to think about the broader ethical implications of the use of this data, and the role it plays in their business. As compliance with multiple privacy and data protection laws becomes ever more complicated, it is the organizations that can demonstrate that they have a good set of principles for using this data, and not over-using it, that will be looked upon favorably by regulators and the public at large.

Ian Thomas
Chief Data Officer, Publicis Spine
Digital Analytics Association Board Member

Introduction

It is almost a year since GDPR became law at the end of May 2018, an event marked most visibly by the flurry of last-minute consent emails from brands desperate to keep email communication lines open. Despite dire predictions, marketing has carried on without missing a beat. Brands continue to find novel ways to engage consumers, including advertising, relevant media placements, and valuable digital experiences.

In fact, despite considerable global media coverage on the implications of the new legislation, the consumer response has been relatively muted. While consumers do appear to have a better understanding of how companies are using their personal data, the law has not dramatically impacted their relationship with brands. Indeed, almost two-thirds of consumers (65%) say GDPR has had no impact on their experience with brands.[1]

The technical response has been more pronounced, with many companies investing heavily to achieve compliance. Beyond visible consent and opt-in changes, there are other, more subtle differences. For instance, the number of 3rd-party cookies in the UK has fallen by 45%.[2]

This report addresses how U.S. companies have responded to GDPR a year after its introduction, and considers the implications for compliance with the imminent arrival of the new data privacy legislation in the U.S.. With the upcoming California Consumer Privacy Act (CCPA), we were particularly keen to understand how well-prepared U.S. companies are for potential U.S. regulation. We wanted to know whether companies had done enough work with GDPR to prepare themselves for other data protection regulations that might emerge around the world.

What we found was that many companies have only taken minimal steps to protect consumer data, and substantial work remains to prepare for forthcoming U.S. data protection and privacy laws. The solutions put in place for GDPR compliance are inadequate to protect consumer data privacy more broadly.

“

This report addresses how U.S. companies have responded to GDPR a year after its introduction, and considers the implications for compliance with the imminent arrival of new U.S. data privacy legislation.

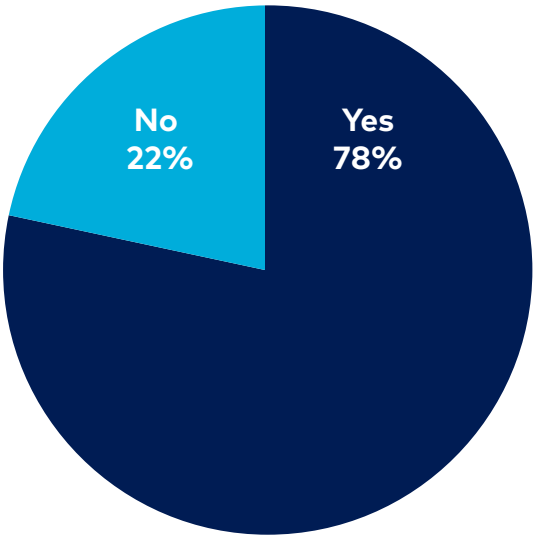
[1] GDPR three months on: Most consumers feel no better off, Marketing Week, 24 August 2018, http://bit.ly/2Gbn3o4

[2] Changes in Third-Party Content on European News Websites after GDPR, Reuters Institute for the Study of Journalism, August 2018, http://bit.ly/2ImJk3q

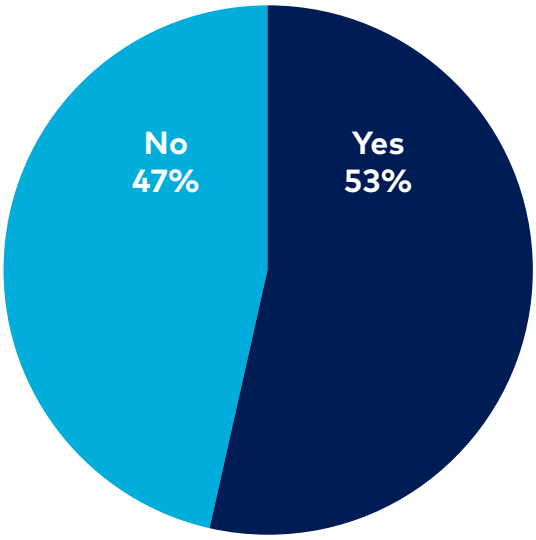
The state of GDPR compliance

As anticipated, U.S. companies did take note of GDPR. More than three-quarters of companies surveyed (78%) have taken some type of action to become GDPR compliant. This is not surprising, given the potential penalties for non-compliance are so significant; organizations have felt compelled to respond. In fact, what is more surprising is that almost a quarter (22%) of organizations have not taken any action at all. Further research is required to understand their rationale.

Our organization has implemented updates to our site for GDPR compliance.



I am confident that my organization fully complies with GDPR requirements



When we dug deeper to assess confidence in compliance, the story becomes more nuanced. Just half of the respondents are confident their organization fully complies with GDPR requirements. The general sentiment is: **"I've done some stuff, but I'm not sure I've done enough ..."**

Some of the hesitancy appears to relate to uncertainty about the bounds of the legislation. Brands are waiting on precedent and further judgments to understand more fully what GDPR means for them. These penalties will further clarify the implications of the law for brands.

E.U. member states have only levied a handful of fines in the first year, and the largest fine ($57 million) was imposed on Google by the French data protection regulator. There appears to be a general expectation (if often left unspoken) that the European courts will target higher profile companies. The consensus is that there may well be a dramatic increase in fines in the second year of GDPR.

Achieving compliance

The lack of confidence is certainly related to the limited actions organizations have taken to ensure they are GDPR compliant. Most companies appear to have done the bare minimum to comply with GDPR. Many are yet to take comprehensive steps to improve their collection and processing of customer data. Instead, they have simply been trying to avoid falling foul of the law.

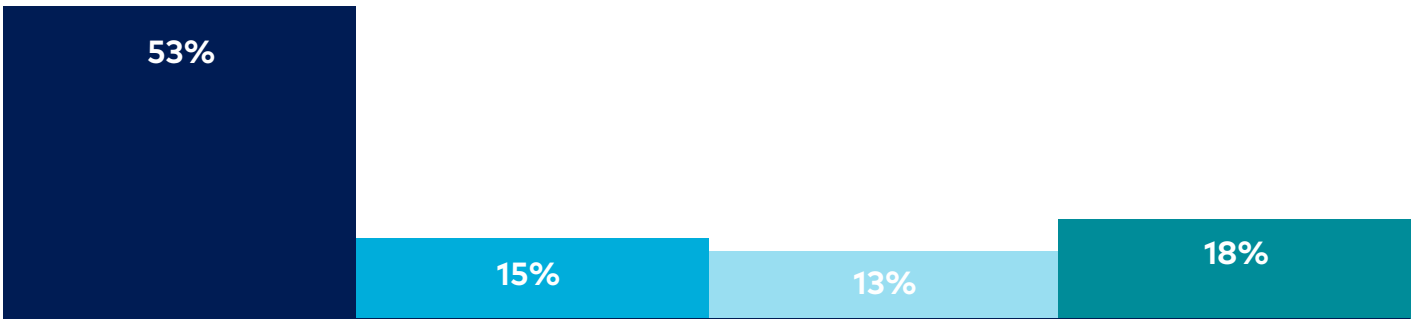
Just over half of respondents in our survey (53%) currently ask for consent to track E.U. visitors. The remaining 47% made a calculated decision that it was easier to block European traffic, disable tracking, or simply remain non-compliant.

Many U.S. companies initially chose to block European traffic (15% of respondents still block traffic from the E.U.). For example, the LA Times initially prevented consumers in the E.U. from accessing its content (they have since re-enabled access). While ensuring compliance, this approach did not address the real, underlying issue. One can hardly imagine an organization like the LA Times blocking consumer traffic from California as a response to the forthcoming CCPA regulation. As data privacy regulations become more common, these organizations will need to provide greater consumer controls.

These answers indicate compliance was a top-down initiative driven by legal departments. While understandable, this approach fails to appreciate the spirit of the law. It means that companies have not put their consumers first. They have failed to listen to their requests for greater data control and security.

> “The general approach many companies have taken to compliance fails to appreciate the spirit of the law.

Our organization has implemented the following GDPR compliance standards for European Union (E.U.) visitors



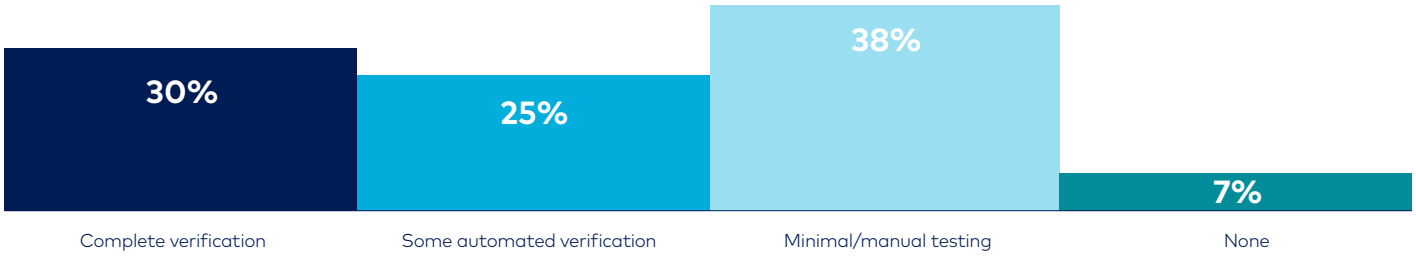
Most importantly, it means that many companies are not prepared for U.S. data privacy legislation. They have missed the opportunity to use GDPR as a test-bed for domestic regulation.

Interestingly, even the companies that have taken steps to be compliant still have more work to do. Less than one-third of organizations surveyed have performed 'complete verification' of compliance. A further 25% have performed 'some automated testing', but it is clear that sustained compliance has not been elevated to become an organizational priority.

There is also work to be done to automate testing and build further controls for data protection. This suggests that many companies may have considered GDPR compliance to be a one-time event rather than an ongoing process and "the new normal".

Our research found a correlation between the level of testing and the level of confidence in organizational compliance. 53% were confident in their compliance, a proportion that broadly matches the 'complete verification' and 'some automated verification' responses. It is likely that the degree of confidence tracks with the level of automated testing/verification performed.

Our organization has performed the following verification(s) to determine compliance with our privacy and date collection policies

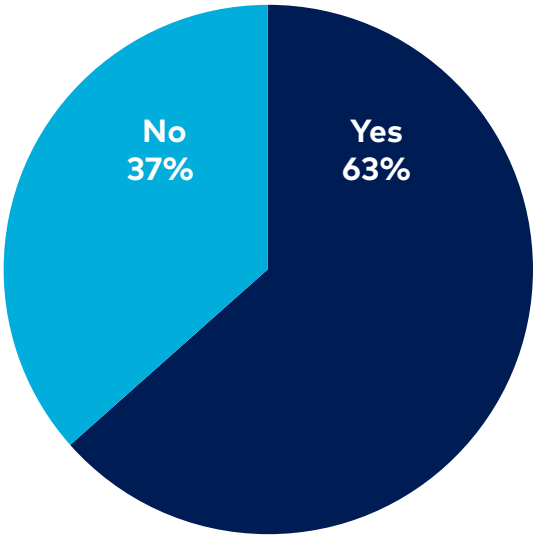


U.S. legislation

Given that U.S. data privacy legislation is coming soon – with the CCPA already passed and federal legislation likely – we wanted to gauge attitudes to this kind of data protection legislation in the United States.

We found broad support for data privacy laws, with almost two-thirds of respondents favoring GDPRlike legislation in the U.S.. These results are in line with data from Pew Research that indicate 64% of Americans support more regulation of advertisers.[3]

Regulation like GDPR should be implemented in the United States



It is ironic that responses were generally favorable towards similar data privacy regulations in the United States, yet these same organizations have done so little to support GDPR to date. Consumers clearly want control of their data and clarity on how it's being used, and yet companies are not responding. Interestingly, many of these same companies put great store in how customer-centric they are.

Marketers and data scientists can tend to live in a bubble and forget how little the average person knows about the way in which consumer data is used in marketing. Technology has outpaced the average consumer, making it challenging to understand the possibilities and intricacies of data tracking and digital advertising. A recent study by the UK government found that "while 63% of people said it is acceptable for websites to be funded by personalized advertising, once it gave a basic description of how personal data is used in the process, the figure dropped to 36%".[4]

It isn't just consumers looking for greater privacy and protection. Influential technology companies are weighing in on the issue in favor of federal privacy laws. Tim Cook, Apple's CEO, famously wrote an op-ed article in Time, calling for: "comprehensive federal privacy legislation —a landmark package of reforms that protect and empower the consumer".[5] Even Google and Facebook have joined calls for federal legislation in order to avoid a patchwork quilt of state laws.

[3] "Americans' complicated feelings about social media in an era of privacy concerns", Pew Research, 27 March 2018, https://pewrsr.ch/2GacAZG

[4] 5G poses 'dramatic challenges' to privacy and personal data, Marketing Week, 1 March 2019, http://bit.ly/2KlPfIU

[4] You Deserve Privacy Online. Here's How You Could Actually Get It, Time Magazine, 16 January 2019, http://bit.ly/2IkeY1H

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) caught many by surprise with the speed of its passage into law when it first appeared in 2018. Occasionally referred to as 'GDPR-lite', the legislation is indeed like the European law in many ways. It is similar enough to the European legislation that some GDPR compliant companies are likely prepared for CCPA. However, there are enough differences between the two sets of regulations that every affected company should perform a full compliance review.

CCPA does not come into effect until January 1, 2020, and enforcement will commence no later than July 1, 2020. It will affect nearly all businesses in the United States. Companies must be compliant if they sell goods or services to California residents – even if the business is not physically located in California. The revenue requirement ($25 million) is low enough that it will also catch most organizations.

Following the CCPA, a number of other states are now considering the introduction of their own data privacy laws, potentially requiring compliance with an array of differing regulations. At some point, the federal government may step in and create a single, national data privacy law to make compliance easier. Indeed, the leading U.S. advertising trade organizations (the American Association of Advertising Agencies [4A's], the Association of National Advertisers [ANA], and the Interactive Advertising Bureau [IAB]) have recently come together to form "Privacy for America", a new coalition that will lobby for federal legislation to avoid this patchwork quilt of various state laws. Regardless of the state regulations on the horizon, companies need to create some form of privacy protection governance.

Based on our experience, however, it is clear that few companies understand the true implications of CCPA and potential federal legislation. We expect there to be significant corporate and media focus on data privacy during the second half of 2019.

> Based on our experience, it is clear that few companies understand the true implications of CCPA and potential federal legislation.

The opportunity for brands

Brands have a short window of opportunity to use personal data privacy as and competitive advantage and to build a trusted relationship with their customers. Instead of simply paying lip service to being customer-centric, organizations have the chance to become genuinely more customerfocused by giving consumers what they've been asking for - greater control of their personal data.

This means understanding the spirit of the law and not just the letter of the law. Instead of simply trying to avoid fines, organizations can seize the chance to think – and behave – in truly empathetic fashion about the consumer experience.

Apple is leading the way here, actively promoting how its technology, platforms, and ecosystem are designed to protect customer privacy and data. It is successfully making data security a compelling selling proposition; users' data is theirs and theirs alone, is never sold to third parties, and is totally safe and secure. This is true whether users chose to store data locally or encrypted in the cloud. Security and privacy are very much part of the DNA of Tim Cook's Apple. The pay-off, of course, is that optimal security is only available to those who put their faith – and their dollars – in Apple's own walled garden. iCloud, iTunes, Apple Music, and soon Apple TV+. See for example apple.com/privacy.

Many companies are not prepared to go to the lengths Apple has and take advantage of this opportunity and in this way build customer trust. Nevertheless, in a time when data protection and privacy face increasing regulatory pressure, here are seven actions U.S. companies should consider taking to address these issues.

1. **Review the customer experience**, understand which touchpoints are most critical, and consider the data required to optimize those touchpoints.

2. **Engage in a dialogue with your consumers** to better understand the value exchange they are willing to have with your brand and the current level of trust in your handling of their data.

3. **Actively communicate data privacy policies** to consumers clearly and plain English.

4. **Audit the existing data flow** to confirm how data is captured, procured, processed, and utilized within the experience ecosystem.

5. **Appoint a marketing and/or business lead for data privacy** and compliance activities. This area needs to be more than just a legal focus.

6. **Establish a sustainable structure for compliance** that leverages leading data protection software and automated testing.

7. **Shift to greater use of 1st-party data for marketing activities.** This change may require further changes to an organization's data architecture as well as how they capture and connect data sets.

In summary

The status of GDPR compliance by U.S. organizations is an important bellwether of the work required for companies to achieve compliance with the California Consumer Privacy Act and other potential state and federal legislation.

The nature and extent of work undertaken to date indicates many organizations still have plenty to do. Many companies have only done the bare minimum to deliver legal compliance. But there is an opportunity for companies to get ahead of the laws and show consumers how they value and protect personal data and privacy. This will require significant effort to build trusted relationships, improve data collection/integration, and change media

---

About the Digital Analytics Association (DAA)

The DAA is a not-for-profit, volunteer-powered association whose mission is to make analytics professionals more effective and valuable through professional development and community. Its vision is advancing the profession of using data to improve business. The DAA was founded as the Web Analytics Association in 2004. The organization has almost 5,000 members around the world, representing a broad spectrum of expertise. For more information about the DAA, or to become a member, visit the DAA website at digitalanalyticsassociation.org.

Note

The authors of this report are marketers and not lawyers, so the information in this article should be used for informational and contextual purposes. We recommend that brands should consult legal counsel for specific guidance regarding compliance with GDPR, CCPA, and any other privacy legislation.

---

ebiquity

We are a leading independent marketing and media consultancy

Our ambition is to help brands harness the power of data, analytics, and technology to improve marketing outcomes

With 18 offices globally, we offer full coverage of the world's largest advertising markets:

- Working with 70 of the world's top 100 advertisers
- 650+ employees in 14 global markets including London, Paris, Madrid, New York, Sydney, Shanghai and Singapore
- Listed on the London Stock Exchange (AIM:EBQ)

Our consultants and experts work with market-leading local and global brands across three key areas:

- Media
  Achieve higher media performance through best-in-class media management and transparency
- Analytics
  Build evidence-based marketing programmes rooted in data and analytics
- Tech
  Design the right technology ecosystem to drive higher value from digital investments

ebiquity

ebiquity.com
@ebiquityglobal
linkedin.com/company/ebiquity-plc