WHITE PAPER

GDPR, CCPA, and Beyond:

How Identity Governance Helps Companies Comply and Improve Customer Trust

Executive Summary

Business-impacting privacy regulations are an ever-expanding global trend. The European Union's much-discussed General Data Protection Regulation (GDPR) went into effect in 2018. And on January 1, 2020, the California Consumer Privacy Act (CCPA) becomes law, affecting companies that conduct business in California, the fifth-largest economy in the world.

But that's just the start. Fueled by well-publicized data breaches, ID theft, and related scandals, privacy and compliance legislation is being enacted across the globe at a rapid pace. In the United States alone, nine states have introduced or passed bills imposing far-reaching obligations on businesses and organizations to provide consumers with more transparency and better control over personally identifiable information (PII).

Businesses cannot afford to ignore these new privacy laws and regulations. From a financial standpoint alone, moderate fines that were levied during the first 12 months of GDPR have now given way to staggering fines in excess of $200 million, which is still far away from the statutory cap of 4% of the annual global turnover. But the cost to global businesses is much more than financial. At risk is consumer trust.

If customers do not trust a company or organization to protect their valued privacy, sales and marketing power will suffer. Businesses today need express consent in order to process personal data. And consent requires trust. Without trust, there is no consent. Without consent, there is no data. And that means hopelessly ineffective sales or marketing campaigns.

Honoring privacy is not just a compliance question, but also a core business advantage. Privacy and identity governance help businesses and organizations form trusted relationships with users and customers, resulting in higher customer loyalty – and ultimately higher business revenue.

This paper presents an overview of GDPR, CCPA, and related global privacy regulations. It offers up the case for building customer trust through regulatory compliance, identity governance, and data protection, and discusses the need for proper identity management solutions. Also presented are examples showing how two leading brands have met their privacy compliance goals.

General Data Protection Regulation

On May 25, 2018, GDPR became a global fact of life. The comprehensive data protection law's stated goal is to harmonize local data protection laws across Europe. The law applies not only to Europe-based companies, but also to any company or organization that does business within the European Union.

GDPR lays out numerous detailed requirements about how to collect, store, and use PII, and how to protect the data against unauthorized access.[1] This involves not only how to identify and secure personal data, but also how to accommodate new transparency requirements, how to detect and report personal data breaches, and how to train privacy personnel.

Noncompliance with GDPR's principles can have a material impact on the financial status of an organization because of GDPR's ability to levy fines. While initial privacy breaches resulted in modest fines, the industry is now sitting up and taking notice, as recent fines levied are making headline news globally. Two major fines – one on a major airline[2] ($230 million) for a data breach that affected 500,000 people and one on a global hospitality company[3] ($123 million) for the hacking of the personal information of 383 million hotel guests – have garnered particular attention from global businesses.

California Consumer Privacy Act

Applying additional pressure on businesses to protect privacy, the final countdown has now begun for the California Consumer Privacy Act (CCPA).[4] On January 1, 2020, most larger companies or organizations that do business in California will be required to comply with the state's strict new privacy legislation that establishes a legal and enforceable right of privacy for every California resident. As with GDPR, these new regulations are not just for businesses based in California; they apply to all companies that do business in the state.

CCPA provides the following protections for the personal data of California consumers:[5]

- **Ownership.** Protects consumers' rights to tell a business not to share or sell personal information
- **Control.** Provides consumer control over the personal information that is collected about them
- **Security.** Holds businesses responsible for safeguarding personal information
- Any business or organization will need to comply with CCPA if they meet just one of the following criteria:
  - Have revenues in excess of $25 million
  - Buy, receive, sell, or share the personal information of 50,000 or more consumers, households, or devices for commercial purposes
  - Receive 50% of annual revenues from selling consumers' personal information

While many companies faced substantial hurdles last year in complying with GDPR, they now need to comply with CCPA as well. With the looming deadline right around the corner, time is running out. Businesses that collect customer identity data in California and build customer profiles for personalized marketing campaigns need to act now or risk the potential for major fines.

How Do GDPR and CCPA Compare?

While CCPA is somewhat different in scope from GDPR, it grants consumers similar rights of controlling and vetoing the use of their data. Both regulations require companies to store data securely, be transparent about the types of personal data collected, and manage consumer requests for deletion of personal

data (often referred to as the "right to be forgotten"), which means being able to delete personal data from all systems throughout the organization.

Where consent is the legal basis for data processing, CCPA differs from GDPR in that it requires the ability for users to opt out, versus requiring explicit consent prior to collecting PII.

Additional Global Regulations

As important as they are, GDPR and CCPA are just the beginning of this global trend. Around the world, numerous privacy and compliance laws are being considered or already enacted. In the United States alone, legislators in nine other states have introduced bills that would impose broad obligations on businesses to provide consumers with more transparency and control over PII.[6]

On the international level, the trend to stricter (and business-impacting) privacy regulations is a global phenomenon that companies and organizations cannot ignore. Listed in the table below are just some of the new and pending regulations, such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA).

Table. Examples of existing, upcoming, or proposed data protection and privacy regulations

AMERICAS	EMEA	ASIA PACIFIC
Argentina: PDPL/Bill No. MEN-2018-147-APN-PTE[7] USA: California: CCPA (AB 375) Canada: PIPEDA[8] Hawaii: SB 418[9] Maryland: SB 0613[10] Massachusetts: SD 341[11] Mississippi: HB 2153[12] New Mexico: SB 176[13] New York: S00224[14] North Dakota: HB 1485[15] Rhode Island: S0234[16] Texas: HB 4518[17]	European Union: GDPR Russia: Federal Law No. 152-FZ[18]	Australia: Privacy Act 1988 / Information Privacy Principles (IPPs)[19] China: Personal Information Security Specification[20] India: Personal Data Protection Bill[21] Japan: APPI[22]

Beyond Regulatory Compliance: Building Trust

With all of these regulations, building consumer trust has become even more important for companies and organizations across the globe. GDPR, CCPA, and related legislation require companies, where applicable, to ask customers for consent before they collect and use their data — and, of course, to keep a record of the consent.

Beyond regulatory compliance, privacy is also crucial for businesses that want to build deep and trusted digital relationships with their customers. Customers have increasingly high expectations that their personal data will be kept private and secure. The many publicized cases of data abuse, breaches, and identity theft have raised the bar for companies to be seen as trustworthy keepers of personal data. When customers store data with an organization, they are entering into a trust contract; if that trust is breached, it tends to be difficult to restore.

People will only give a brand their consent to process their data if the company offers value in return, but also only if they trust the brand. No trust means no consent. No consent means no data, and that means no (or hopelessly inefficient) sales and marketing efforts. Trust has been called the "new currency" for companies that aim to obtain customer data.

The Importance of Consent: Rethinking the User Experience

Under GDPR and CCPA, customers must be able to view, modify, and even revoke their consent at any time. In other words, businesses that provide easy-to-use web forms to collect consent and then purposely make it difficult to revoke consent by requesting that people follow a complicated bureaucratic process will not be in compliance. What's more, companies need to clearly inform people why they are collecting the data and what they are going to use it for.

For marketing organizations, this has quite a few implications. Under GDPR, for example, organizations can no longer use pre-checked boxes on landing pages for gated lead-generation content to obtain consent. Consent must be opt-in rather than opt-out. That is, consumers must check the box to agree. Under CCPA, however, implied consent is still allowed, so a pre-checked box is still compliant. This differentiation can cause headaches for global players faced with the prospect of addressing two major markets with websites and apps that need to display different registration forms. Or even deploying entirely separate websites and apps to address different regions, which multiplies the effort to develop and maintain code.

The new regulations also prohibit excessive data collection. Companies can only collect personal data that is needed for the service or product they offer. Asking for a phone number or gender just to deliver an email newsletter or enable the download of a white paper is no longer allowed. This means that businesses need to rethink and redesign their user experiences and eliminate all data fields on registration pages and other forms that could be considered excessive data collection.

Global Retailer Implements Centralized Solution to Help Simplify Compliance of Today's and Tomorrow's Privacy Laws

A global retail company recently solved its privacy compliance requirements by deploying Akamai Identity Cloud. The solution has enabled the company to provide its customers with transparency and control over their personal data. This has been achieved by minimizing the PII that is captured during registration and by asking for consent before processing any data.

Identity Cloud provides the company with fully customizable user experiences for registration and login, and consent forms that can be invoked progressively per purpose. That has made it easy for the company's consumers to understand the purpose of the data they are providing consent to use, as well as where they have opted out. Consumers are able to review, change, and revoke their consent settings at any time.

The company relies on Identity Cloud's scoped access features to restrict access to data records – and specific fields within the records – depending on the role of company personnel who are accessing the identity data. This means that a customer service rep has access rights that are different from those assigned to marketing personnel or developers, for example. This unique capability reduces risks of customer data exposure and provides an unsurpassed level of data security.

By providing one central repository for customer data with fine-grained access control, the solution can mitigate the sprawl of "toxic" identity data (for example, data that is still stored in the database after the customer has revoked consent or requested deletion). The central repository also simplifies the deletion of data in the context of "right to be forgotten" requests.

And finally, all consent settings are stored with the customer profile in an audit-ready form, together with change logs and audit trails of who accessed which resources and when.

Ensuring Data Protection

Compliance goes well beyond privacy concerns. Keeping customer data secure and protected from malicious actors goes hand in hand with ensuring privacy. As personal identity data can easily be abused and exploited, it has become a major target for hacking attacks. The 2018 Cost of a Data Breach Report,[23] conducted by Ponemon Institute and sponsored by IBM Security, found that 48% of surveyed organizations identified the root cause of a data breach as a malicious or criminal attack, with an average cost of approximately $157 per breached identity record.

As breaches frequently involve hundreds of thousands (or even millions) of records, the resulting cost can severely harm a company – and that's before revenue loss associated with reputational damage, loss of customer trust, and potential fines from GDPR and CCPA.

The Need for Identity Governance

Personal identities are valuable assets — not only for the companies that collect and compile PII, but more importantly for the individual consumers who own the information and have a strong desire to protect it and not allow it to be misused.

As more and more areas of consumers' personal lives move into the digital realm, personal data ends up in companies' profile data, ranging from name, address, phone, gender, payment information, and personal preferences, to shopping and browsing histories, and other behavioral data. The need for companies to secure and protect vital data has grown significantly, and regulators worldwide are reacting to this need in the form of increasingly strict regulations.

Regulatory compliance and security are major factors that add tremendously to the complexity and criticality of identity management. However, enterprise-grade identity management solutions can provide customers with transparency and control over their personal data by minimizing the data that is captured during registration and by asking for consent before processing any data.

With proper identity management, businesses can regain consumer trust.

Global Beverage Brand Achieves Rapid GDPR Compliance

A worldwide beverage company faced a daunting two-month timeline to implement GDPR privacy compliance for all of the brand's European customers prior to the GDPR deadline. The company had previously implemented Identity Cloud, but now needed to rapidly ensure compliance with changing consumer privacy regulations.

Compliance was achieved in just two months from start to finish. The company's focus was on obtaining explicit consent from consumers for the use of their data for marketing and personalization in compliance with GDPR requirements. Identity Cloud provided the company with highly customizable, fine-grained consent forms that could be invoked progressively on any digital property — from websites to mobile apps to IoT devices. In addition to enabling GDPR compliance, this powerful capability helped the beverage brand build trust with its customers by making it easy for them to understand and manage their consent preferences.

One of the more challenging areas of the overall deployment was balancing the "right to be forgotten" aspect of GDPR with legal obligations to retain data during the period of a consumer promotion. Identity Cloud provided the capability to ensure that the data was held for the legal term, and then erased at the end of that period — and to be able to communicate that to the customer.

Akamai Identity Cloud

Identity Cloud is Akamai's solution for customer identity and access management. The platform provides everything companies need to enable their customers to create personal accounts and securely login on websites, mobile apps, or IoT-based applications. Identity Cloud provides tools that can be used to significantly reduce privacy compliance efforts, while still providing companies with a highly secure customer profile repository and enabling a 360-degree view of the customer.

Identity Cloud offers specific capabilities and user experiences that can help companies address regulatory requirements. Identity Cloud privacy and protection features include client registration, login, authentication, single sign-on, scoped access control, preference and consent management, and numerous other capabilities needed to collect, manage, and secure personal data.

Identity Cloud provides the following capabilities that aid enterprises in meeting privacy compliance regulations:

- Checkbox consent mechanisms for explicit consent
- Centralized governance for access control
- Progressive permissioning, registration, and profiling
- Easy data record access mechanisms
- Data correction and integrity mechanisms
- Data portability
- Data erasure/deletion
- Scoped access for users and integrations
- Data pseudonymization
- Age gating

By implementing Identity Cloud, businesses and organizations can implement enterprise-grade identity management in a fast, flexible way. Engineered with a cloud-native architecture, the solution intelligently scales with capacity needs to accommodate spikes in traffic and deliver performant user experiences to hundreds of millions of users. Akamai Identity Cloud is designed to help organizations comply with international privacy regulations, build trust in their brand, manage client data, and mitigate risks by making the data securely available across all regions and applications.

To learn more about Akamai Identity Cloud, visit akamai.com/identitycloud.

Conclusion

GDPR, CCPA, and related privacy regulatory compliance — as well as security assurance — are critical factors for any business or organization that wants to develop and retain trusted relationships with its customers. Consumers expect transparency and demand that their valued personal data be kept private and secure. Recent data breaches, identity thefts, and related global events underscore the pressing need for businesses to be recognized as faithful keepers of PII.

When customers allow their private information to be collected and stored with an organization, they are essentially entering into a trust contract. If that trust is broken, it becomes very difficult to restore. Taking and storing consumer data — and processing customer credentials and personal information — is a duty of care that companies today cannot afford to breach or compromise. If trust is broken, it can easily put brand reputation, customer loyalty — and ultimately, ongoing revenue and business success — at risk.

Appendix: Overview of Privacy Regulatory Requirements

This appendix presents an overview of the general types of requirements that can be found in GDPR, CCPA, and many of the major data protection and privacy regulations around the world: consent, right to object, right to access, right to be forgotten, data portability, security, and breach notification. The implementation of these rights vary among the different privacy and data protection laws being enacted — so you should consult your own legal counsel to determine how different laws apply to you.

For information on how Akamai Identity Cloud may help address these regulatory compliance requirements, please read our blog post.

Consent	Organizations often must obtain consent from end users prior to collecting and processing their personal data for certain purposes. Requirements for obtaining valid consent and when such consent is required vary among applicable regulations.
Right to object	Requirements entitle a data subject to object to the use of their personal data for certain types of data processing, such as direct marketing or statistical analysis.
Right to access	Many laws provide the data subject with the right to access, review, and correct the personal data being processed and, in some cases, seek additional information about the uses and disclosures of such data.

Right to erase or delete personal data	Many laws include the "right to be forgotten" for consumers to have their personal data erased and have it no longer disseminated to third parties or exposed to third-party processing.
Data portability	Companies are required to provide data subjects with copies of their data in a commonly used, machine-readable format, allowing users to transfer their data to another organization without hindrance.
Security	Companies must implement data security safeguards appropriate to the risk to ensure that data is not inadvertently or wrongfully accessed, modified, lost, destroyed, or disclosed.
Breach notification	Organizations must notify end users of any data breaches within a certain time frame after first becoming aware of the situation.

SOURCES

1) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
3) https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
4) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
5) https://www.caprivacy.org/
6) https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf
8) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
9) https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=418&year=2019
10) http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=01&id=sb0613&tab=subject3&ys=2019rs
11) https://malegislature.gov/Bills/191/SD341
12) http://billstatus.ls.state.ms.us/documents/2019/html/HB/1200-1299/HB1253IN.htm
13) https://www.nmlegis.gov/Legislation/Legislation?chamber=S&legType=B&legNo=176&year=19
14) https://assembly.state.ny.us/leg/?default_fld=&bn=S00224&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y
15) https://www.legis.nd.gov/assembly/66-2019/bill-index/bi1485.html
16) http://webserver.rilin.state.ri.us/billtext19/senatetext19/S0234.htm
17) https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04518I.htm
18) https://pd.rkn.gov.ru/authority/p146/p164/
19) https://pd.rkn.gov.ru/authority/p146/p164/
20) https://www.tc260.org.cn/front/postDetail.html?id=20190201173320
21) https://meity.gov.in/content/personal-data-protection-bill-2018
22) https://www.ppc.go.jp/en/
23) https://www.ibm.com/security/data-breach