Guidehouse

A Roadmap to Global Data Privacy Regulation

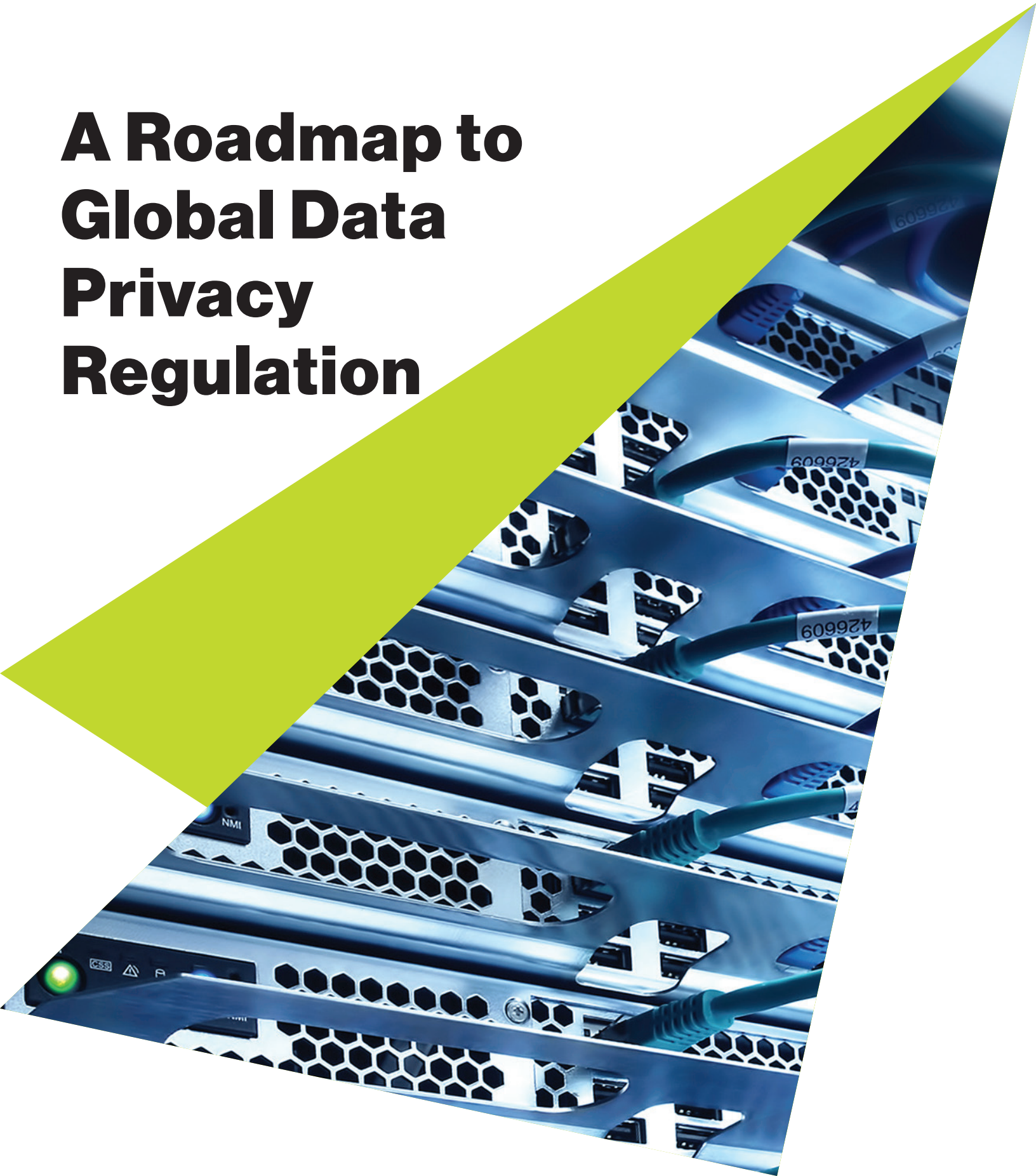

Table of contents

A Roadmap to Global DATA Privacy Regulation

GDPR and CCPA Key Features and considerations

Introduction

Highly publicized data breaches and revelations about the various ways consumer data is collected, stored, and used have recently spotlighted companies' data privacy policies and the regulations that govern them. Recent developments showcasing the extent to which this data is also sold or otherwise disclosed to third parties, with users left unaware, have further highlighted the need for more transparency in this area. Two major data privacy laws passed in the European Union (EU) and the state of California have the ability to shape how many companies need to approach the issue, with other laws in the works both globally and domestically. Internationally, Brazil has recently approved the General Data Privacy Law, and Argentina and India have proposed their own laws or drafted frameworks. Domestically, Colorado enacted a law to amend the state's data breach notification requirements, including reporting timelines, and New Jersey and Washington have recently taken steps toward advancing their own data privacy legislation. With the draft Consumer Data Protection Act of 2018, federal efforts are also gaining traction. These actions further underscore the need for companies to examine their data privacy frameworks.

The General Data Protection Regulation (GDPR) became effective on May 25, 2018, and is applicable to organizations within the EU that use personal data, as well as international organizations that provide goods and services to individuals in the EU or monitor their behavior. While most organizations have completed initial assessments and some form of remediation, very few have developed the necessary downstream procedures to operationalize the program and demonstrate compliance with the GDPR requirements.

Shortly after the effective date of the GDPR, the state of California passed the California Consumer Privacy Act of 2018 (CCPA) on June 28, 2018. While the CCPA only provides data privacy rights to California state residents, considering there are currently minimal federal laws or regulations in the United States governing data privacy and use, particularly outside of financial and health matters, California's law has the potential to set the standard for the entire country due to the size of the state and the breadth of what the statute aims to cover.

The objective of this document is to provide an overview of some of the key features of the GDPR and the CCPA as well as comparisons between the two and key considerations.

Key Regulatory Features

Effective Date

GDPR	May 25, 2018
CCPA	January 1, 2020
Key Considerations/ Comparisons	The CCPA specifies users may request up to 12 months' worth of available data, so impacted organizations that retain data for 12 months or longer need to be prepared to provide data going back to January 1, 2019.

Impacted Organizations

GDPR	Organizations established in the EU or organizations that have personal data of individuals in the EU for the purpose of offering goods/services or monitoring their behavior.
CCPA	For-profit organizations with $25M in revenue, organizations that generate 50% or more of their revenue from selling personal information, or organizations that have data on 50,000 California consumers, households, or devices.
Key Considerations/ Comparisons	Both regulations target organizations that have information on residents and not just organizations physically located within their geographies.

Scope of Data

GDPR	Personal data processed Any information: (a) "Relating to an identified or identifiable natural person." (b) "An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."
CCPA	Personal data collected Any data that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with particular consumer or household." A "consumer" is a California resident. The definition is developed through examples, exclusions, and cross-references to other laws. For example, data subject to HIPAA is exempted from the CCPA, but data subject to FCRA and GLBA is excluded only to the extent those statutes conflict with the CCPA.
Key Considerations/ Comparisons	The definitions both expand the term Personal Data to cover any information that alone or in conjunction with other sources could make an individual identifiable. The GDPR will apply to more internal activities and transfers of data and, therefore, the burden may be more extensive in terms of the number of obligations placed on an organization; however, the CCPA can be more expansive because of the use of "household" in the definition.

Data Subject Rights

GDPR

- Right to be informed
- Right to access
- Right to rectification
- Right of erasure ("right to be forgotten")
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making (e.g., profiling)
- Right to lodge a complaint with the supervisory authority

CCPA

- Right to request that a business disclose the categories and specific pieces of personal information collected
- Right to request deletion of any personal information collected ("right to be forgotten")
- Right to request that a business disclose the categories of personal information sold/disclosed to a third party
- Right to opt out of sale of personal information
- Right to equal service and price

Key Considerations/ Comparisons

Similar data privacy protections are required, though there are some differences between the two regulations. Examples include the detailed implementation requirements for data request portals and the associated data intake requirement related to the right to correction specified under the GDPR, and the explicit right to equal services and price provided for under the CCPA.

Data Request Method

GDPR

Via any one method (telephone, email, or website)

CCPA

Via toll-free telephone number and website

Key Considerations/ Comparisons

Mandated response times vary between the two regulations (30 calendar days vs. 45 days, respectively).

Under the GDPR, this includes complete fulfillment of the request and not only the response. Under the CCPA, the data required for responses is restricted to the past 12 months and the number of responses per individual is limited to two in a 12-month period.

In limited cases, this response time may be extended under both laws.

Civil Penalties and Consumer Damages

GDPR	Civil penalties specified as a maximum of €20 million or 4% of global annual revenues. Does not specify any limitations to damages to impacted consumers.
CCPA	Civil penalties specified as up to $7,500 per violation, with no maximum. Imposes a minimum of $100 and a maximum of $750 per impacted consumer per incident.
Key Considerations/ Comparisons	Significant fines and damages are possible under both regulations.

Organizational Data Privacy Standards

GDPR	Requires organizations to appoint a Data Protection Officer in some situations, consider data privacy when undertaking any new initiative (Data Protection by Design), perform risk assessments of their data processing systems, and document the legal basis under which the data is processed.
CCPA	N/A
Key Considerations/ Comparisons	The GDPR mandates organizations adopt data protection standards throughout their operations.

Incident Response

GDPR	Requires organizations to notify personal data breaches to the data protection authorities (DPAs) and, under certain circumstances, to communicate with the people impacted.
CCPA	N/A
Key Considerations/ Comparisons	The GDPR specifies organizations must notify DPAs within 72 hours of becoming aware of a personal data breach.

Transparency

GDPR	Requires organizations to notify data subjects when their personal data is collected, the elements collected, uses of the data and their purpose, retention periods, parties with whom the data is shared, and their rights.
CCPA	Requires organizations to provide notice of the data to be collected related to residents, with a particular emphasis on the purchase or sale of their personal data.
Key Considerations/ Comparisons	The notification requirements are similar, with the CCPA paying particular attention to informing the individuals of any sale or disclosure of their information.

Considerations and Recommendations

To ensure for readiness, financial institutions should conduct assessments or perform compliance testing to identify possible gaps in policies, procedures, processes, and systems that need to be closed/remediated. While this is not an all-encompassing list, we have identified a few areas for consideration and some of our related recommended actions below.

Areas of Consideration	Recommended Actions
Policies and Procedures	Update policies, procedures, job aides, checklists, templates, etc. based on regulatory requirements. Update privacy notices and other disclosures to conform to regulatory requirements.
Processes, Systems, and Controls	Create data inventory/registry of data sources, processes, and key attributes. Develop processes to respond to personal data requests (export, update, erasure, opt out, etc.). Update existing or implement new controls to monitor updated or new processes and systems.
Training	Create/update training programs for new processes, with a timeline for execution, including addition into annual or new employee curriculums. Conduct training sessions to inform employees and evidence regulatory compliance efforts.
Monitoring	Expand first, second, and third-line-of-defense testing to periodically monitor compliance with data privacy requirements. Creation of key performance indicator reports to monitor personal data requests and compliance with required response timelines.

As a leading global advisor, we have helped many of our clients set up and/or update their data privacy operations and understand all aspects of implementing a robust data privacy framework.

Contacts

Kathryn Rock
Director
Banking, Insurance, and Capital Markets
M +1-202-973-6541
E krock@guidehouse.com

Prasun Howli
Associate Director
Banking, Insurance, and Capital Markets
M +1-713-646-5057
E prasun.howli@guidehouse.com

Special thanks to contributors Margaret Shea, Sarah King, and Brandon Criswell

linkedin.com/company/guidehouse

twitter.com/guidehouse

guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Headquartered in Washington DC, the company has more than 7,000 professionals in more than 50 locations. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit: www.guidehouse.com.

Guidehouse