


Managing Global Data Privacy Laws and Communication Regulations in Financial Services





If you search for a definition of “data privacy,” you’re likely to find inconsistent answers. For an individual consumer, data privacy could mean having control over information relating to their internet searches, their health, education, purchasing activities, location, finances or any other personal data. The right to privacy—to protecting that data from third parties that may use it for unauthorized purposes—has been made explicit by emerging laws and regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States.

Somewhat paradoxically, financial industry regulations imposed by the SEC, FCA and FINRA require firms to collect and store all business-related electronic communications data. The scope of that data has expanded widely and sometimes collides with tools commonly used by individuals for their own personal purposes. While the objective of compliance regulations is to hold financial firms accountable and protect consumers, using that data for purposes other than those outlined by regulatory guidelines can lead to fines, litigation and a loss of customer trust.

Data privacy laws are expanding throughout the world and will be increasingly important as more of our lives take place online. The initial thrust of many data protection laws is to protect the rights of personal data and firms faced with industry-specific regulatory compliance obligations are not exempt. They need to be aware of how they can meet their obligation to collect and store business communications while adhering to data privacy mandates in all markets they operate within.

In this guide, we’ll cover:

- Landmark privacy laws GDPR and CCPA, as well as other regional and country-specific privacy regulations
- How data privacy and retention and oversight requirements can work together
- Steps to stay prepared for current and evolving data privacy regulations
- How Smarsh helps organizations stay on top of both data privacy and retention and oversight requirements
- Data privacy resources

Pioneering Data Privacy Laws

General Data Protection Regulation

The General Data Protection Regulation (GDPR) in the European Union protects personal data—any information relating to an identified or identifiable data subject—for EU citizens, no matter where they currently reside. It was adopted in 2016 and put into effect as of 2018.

According to DLA Piper, the reasoning behind the regulation's enactment was that, "privacy issues arising from an exponential growth in consumer and mobile technologies, an increasingly connected planet and mass cross border data flows have pushed the EU to entirely rethink its data protection legislation to ensure that these fundamental rights are fully protected in today's digital economy."

Whether organizations are defined as data controllers or data processors, they must take accountability measures such as (but not limited to):

- Adopting and implementing data protection policies
- Maintaining appropriate security measures
- Recording and reporting personal data breaches
- Responding to Right of Access requests
- Enabling a Right of Erasure, when applicable

GDPR set the stage for modern data privacy laws. Since its inception, countries and regions around the world have followed suit with their own versions.

The less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. The more severe infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.



In the first year
of GDPR there were
281,088
cases logged

<https://bit.ly/GDPR-violations-year-one>



€72 million+
in levied fines
in the first nine months
of 2020

<https://www.itgovernance.co.uk/dpa-and-gdpr-penalties>

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) was passed in 2017 and went into effect in 2020. It was modified in October 2020 to become the California Privacy Rights and Enforcement Act of 2020 to further extend enforcement. It applies to all for-profit organizations that do business in the state of California, and meet one or all of these parameters:

- Revenue of at least \$25 million
- Have data that belongs to 50,000+ California consumers
- Get at least 50% of their revenue from selling consumer data

CCPA is frequently referred to as “California’s GDPR” as it contains many similar rights and responsibilities. However, there are a few key differences, namely:

- CCPA’s narrower definition of whose data is covered (e.g. California residents and those temporarily residing outside of the state versus “data processors” or “data controllers” under GDPR)
- CCPA’s broader definition of “personal data” to include information that can be associated with specific individuals (such as devices and pseudo-anonymized data)
- A “look back” requirement that would require firms to respond to requests within 45 days, where requests can reach back 12 months prior to the request (versus GDPR which mandates a response within 30 days with an extension of two months in certain circumstances) and no defined limitation as per how far back the data request can go



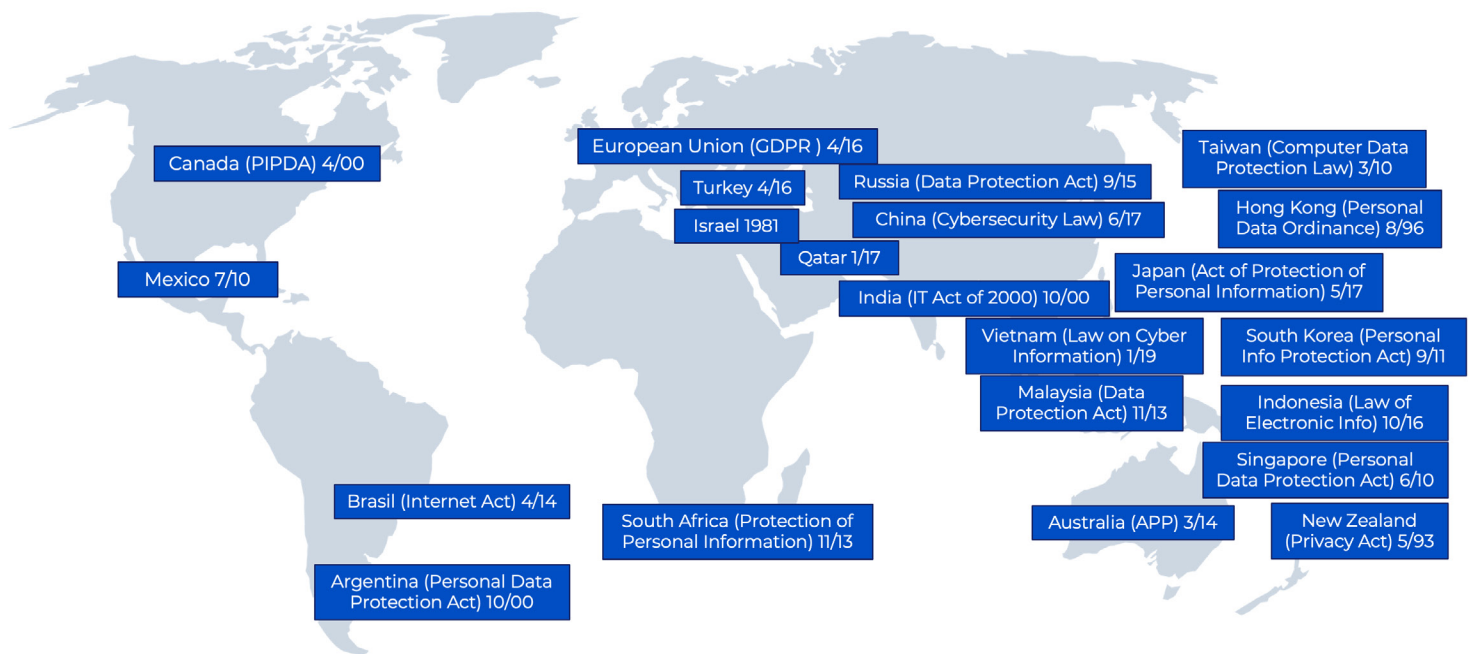
Civil penalties for violations of the CCPA are \$2,500 per violation and \$7,500 if proven to be intentional.

Organizations must be able to square consumer rights with their organizational responsibilities. It’s recommended to:

- Update privacy notices
- Disclose business purpose for collecting data in the privacy notice
- Notify users about the right to opt-out of the sale of their information
- Respond to requests for disclosure in a readily usable format within 45 days
- Enable right of erasure

Data Privacy in the World Beyond GDPR and CCPA

Global organizations with operations in multiple jurisdictions must consider any and all applicable regulations and laws. Some specific privacy mandates include the following:



Brazil

Passed in August 2018, the [General Law for Data Protection](#), or Lei Geral de Proteção de Dados Pessoais (LGPD) was implemented in September 2020, with enforcement scheduled to begin in August 2021.

The legislation contains requirements that are very similar to those of the GDPR, such as breach notification, data protection impact assessments and data subject rights. According to [Forrester's Global Map of Privacy Rights and Regulations](#), its scope of protection is considered broad against all covered entities, yet it does not meet the EU's "adequacy" [comparative standard](#) for data protection and privacy. Transfer of personal data must comply with LGPD provisions, unless, among other exceptions, the transfer is necessary for compliance with legal or regulatory obligation. Fines are structured gradually, from 2% of revenues up to a maximum of 50 million BRL (approx. \$10M USD) per infraction. Enforcement guidelines and frameworks from the Brazilian Protection Authority (ANPD) remain in development as of late 2020. According to [DLA Piper's Data Protection Laws of the World](#), Brazil is rated "Moderate" in terms of regulatory rigor and enforcement.

(DLA Piper's rating scale assesses the amount of effort required to meet data privacy obligations. Regulatory requirements are rated from most to least rigorous, noted as "Heavy," "Robust," "Moderate," or "Limited.")

China

China possesses a multitude of data protection laws across various regulations, including the 2017 Cybersecurity Law and those administered by the Cyberspace Administration of China (CAC). Among the various draft laws and regulations, the CAC introduced the Measures on Cross-Border Transfer Security Assessment in 2019. It includes numerous provisions governing cross-border transfers, including completion of security assessments, transfer agreements and incident response plans, as well as approval by the People's Bank of China (PBOC) for

transfer of personal financial information. Fines and sanctions vary by law, with violations of the Cybersecurity Law potentially carrying fines of up to 1,000,000 RMB (approx. \$152K USD). DLA Piper rates China as “Heavy” in terms of regulation and enforcement, although it does not have an established enforcement agency or meet EU adequacy standards.

Hong Kong, SAR

Hong Kong first implemented a [Personal Data \(Privacy\) Ordinance \(PDPO\)](#) in 1996. PDPO went through significant revision in 2012/2013 to govern the use of personal data in direct marketing. Administered by the Office of the Privacy Commissioner for Personal Data (PCPD), the PDPO is seen by DLA Piper as “Heavy” in terms of regulation and enforcement. Its broadly defined scope of protections (although not as explicit as GDPR) cover all entities (with some exceptions for employment-related data). It also does not meet EU adequacy standards. The PCPD provides non-binding guidance that prohibits cross-border data transfers unless specific conditions are met, including enforceable data transfer agreements that include model clause input from the PCPD. Violations of the ordinance include fines of up to HK\$50,000 (\$6K USD) for failure to respond to a PCPD enforcement note.

Japan

The [Act of Protection of Personal Information \(APPI\)](#) was enacted in 2003 and last modified in June 2020. It establishes an oversight body, definitions of sensitive information, and defines restrictions on the transfer of personal data to foreign jurisdictions. APPI is administered by the Personal Information Privacy Commission (PPC). PPC has taken a leadership role in promoting stringent privacy standards across the Asia Pacific region as well as establishing data transfer standards with the EU, although it lacks the authority to impose fines. Cross-border data transfers must receive prior consent from data subjects, unless receiving countries are white listed by the APPI (which now includes EU countries) or demonstrate similar data protection standards. Non-compliance with APPI orders to correct violations are subject to fines of up to JPY 300,000 (approx. \$3K). Japan’s privacy regulation and enforcement is “Robust” according to DLA Piper.

Singapore

Singapore’s [Personal Data Protection Act \(PDPA\)](#) was implemented in 2012, with additional data protection provisions taking effect in 2014. The provisions recognize the rights of individuals to protect personal data, while excluding information related to employment with an organization. References within PDPA draw upon privacy regulation laws that are considered “comprehensive,” including the EU, UK, Canada, Hong Kong and Australia. These include nonbinding guidance on cross-border data transfer. Additional regulations pertaining to critical infrastructure industries—including banking—were implemented in the 2019 [Cybersecurity Act \(CSA\)](#), which outlines additional requirements for handling incident response and breach notification. PDPA enforcement includes penalties of up to SGD 1 million (approx. \$747 USD). Singapore’s privacy regulation and enforcement is considered “Robust” by DLA Piper.

South Korea

South Korea’s [Personal Information Protection Act \(PIPA\)](#) was implemented in 2011. PIPA provides a comprehensive framework that is among the most rigorous in the world. Additional sector-specific regulation includes the [Act on Real Name Financial Transactions and Guarantee of Secrecy \(ARNFTGS\)](#). It applies to information obtained by financial institutions’ privacy regulation and enforcement and requires written consent for transfer of personal information associated with financial transactions prior to transfer to third parties. Under ARNFTGS, disclosure of personal information pertaining to financial transactions is subject to imprisonment of up to 5 years or fines of up to KRW 30 million (\$28K USD). South Korea is considered “Heavy” by DLA Piper due to broad scope of protections across all covered entities, prohibitions on cross-border data transfers, established enforcement mechanisms and progress toward meeting EU adequacy standards.

Switzerland

Adopted in September 2020 and scheduled for implementation in 2022, Switzerland's revised [Data Protection Act](#) attempts to update its existing Data Privacy Act (DPA) to better align with provisions of GDPR. While specific provisions remain subject to change through public commentary, its basic tenants remain similar to the existing DPA. In comparison to GDPR, it follows the same general principles of "privacy by design and default," although fines for intentional violations are much less onerous than GDPR, with liability limited to only CHF 250,000 (approx. \$280K USD). Firms should continue to monitor developments on specific provisions and enforcement mechanisms. As it currently exists, Switzerland's data privacy regulations are considered "Heavy" by DLA Piper due to broad scope of protections across all covered entities, prohibitions on cross-border data transfers, and established enforcement mechanisms.

Other US State Laws

Budding state laws are emerging throughout the United States as well. California alone has more than 25 state privacy and data security laws, including CCPA. In Nevada, individuals have included an opt-out provision within their privacy regulations detailing how personal data can be used, and what the individual citizens have the right there to do.

Bills have been introduced in states like Connecticut, Hawaii, Maryland, Massachusetts, Michigan, New York, Pennsylvania, Rhode Island, Texas and Washington and a growing number of states that are adopting similar safeguards regarding the right of access to personal data and the right of deletion.

At the least, consumers should be able to reasonably assume certainty about where their data is stored, that regional policies are being enforced, and that data access is limited to authorized individuals.

Companies must offer certainty that they can fulfill right of access requests within required time periods and ensure that strict data security measures exist. They must also ensure that employees are knowledgeable about privacy rules, and that they or a sanctioned partner can host non-U.S. data in its home region.

Blending Data Privacy and Industry Regulations

At the heart of the matter, data privacy laws and financial industry regulations are based on the same key ideas. Data privacy laws support the right for people to inquire about how companies are using their information. GDPR, for example, mandates that companies only obtain data that has a defensible business purpose, provide individuals their data when requested, and delete that data if an individual has made such a request. The right to deletion is not an absolute right. If there is a legitimate business need, the data can be retained.

At the same time, financial organizations across the world must collect and store communications data they generate for recordkeeping purposes—as a means of transparency for consumers. For example, companies operating in the UK must contend with MiFID II, which requires the capture of all electronic communications. In the U.S., governing bodies like the SEC and regulatory watchdog FINRA also require financial services organizations to collect and archive all business-related communications.

Best Practice Recommendations for Data Privacy Regulation

So, how can financial firms reconcile evolving privacy laws with their existing (and evolving) regulatory obligations? Firms can prepare for an increased focus on data privacy by starting with a few steps:

◆ Understand your data: the sources, features, users

How are you engaging with customers? What are the tools being used by your frontline staff? What personal data can staff collect using those communication tools? In most companies, interactions and engagement take place across a complex web of channels and devices. It's important for privacy executives and compliance teams to understand all the locations where personal information might ultimately reside, and the various dimensions included in the data.

◆ Update policies to reflect all sources used for business purposes

In addition to consent policies, ensuring that internal communications policies are current and reflect how personal data should be managed is central to any privacy mandate. The compliance perimeter needs to expand not just to the IT control systems, but anything that's being used by employees. Having a mechanism to document how tools are being used and for what business purposes can validate that if an inquiry comes up.

◆ Train employees on GDPR and CCPA requirements

Training programs should be built specific to privacy regulations. Related to CCPA, providing users and data managers with an overview of requirements can remove ambiguity of the consequences of potential policy violations.

◆ Tune oversight processes to reflect higher risk areas

It's not just email anymore. Collaboration platforms and encrypted tools must be addressed. Ongoing inspection of content for personal information should not only focus on IT controlled systems, but those where rules and oversight may not have been extended yet (for example, newly deployed collaborative tools like Slack or Microsoft Teams or encrypted tools like WhatsApp and WeChat).

◆ Leverage AI/surveillance to uncover dark data locations

Without AI-enabled surveillance and compliance tools, companies may find it difficult to address the risks that lie within new and various communication channels. Advanced analytics and surveillance technology can help extend oversight processes into areas that cannot be uncovered by policies or lexicons.

HOW SMARSH CAN HELP



Smarsh solutions allow the capture and support of 80 different communication networks, including collaboration tools, mobile applications, social media, email and others. Our archives allow users to handle right of access requirements, processing limitations, data retention specifications and more. Specifically:

- **Role-based access controls** limit access to retained data to authorized staff, with fully customizable role definitions to meet global and local demands. All data access actions (search, review, hold, export, etc.) are logged and fully auditable.
- **Unified identity management** capabilities allow for the creation of a global identity that ties users to all their content sources to provide a complete view of each user, and can be leveraged to create specific policies associated with that user's citizenship status or location.
- **Mediation and data curation** capabilities allow firms to enforce restrictions on processing, including the ability to enforce policy controls on specific communications network, such as enabling in-stream moderation or disabling of specific features.
- **Superior data throughput** to enable the high-speed search, review, and retrieval of any quantity of archived data in order to fulfill Right of Access requests well within required regulatory response times.
- **Data privacy by design and default** including multi-tiered data, application and network security capabilities, backed by ISO 27001 attestation. Full auditing and reporting capabilities, along with tamper-proof storage allow firms to leverage firms to a system designed to withstand the most rigorous regulatory scrutiny.

We also provide solutions for supervision and e-discovery, and the ability to integrate with third party applications. Surveillance technology gives companies the capability to investigate potential unknown risks and areas where dark data may hide valuable insights. Smarsh provides one integrated platform across all these capabilities.

Data Privacy Resources

GDPR enforcement actions: <https://www.itgovernance.co.uk/dpa-and-gdpr-penalties>

CCPA summary: <https://www.caprivacy.org>

CCPA vs. GDPR: <https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDRP-Chart.pdf>

Brazil Lei Geral de Proteção de Dados Pessoais (LGPD): <http://lawsofbrazil.com/2020/09/18/brazils-data-protection-law/>

China 2017 Cybersecurity Law: <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>

EU General Data Protection Regulation: <https://gdpr-info.eu/>

Hong Kong Personal Data (Privacy) Ordinance (PDPO): <https://www.dataguidance.com/notes/hong-kong-data-protection-overview>

Japan Act of Protection of Personal Information (APPI): <https://www.ppc.go.jp/en/>

Singapore Personal Data Protection Act (PDPA): <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>

South Korea Personal Information Protection Act (PIPA): <http://www.pipc.go.kr/cmt/main/english.do>

Switzerland Data Protection Act (DPA): <https://www.linklaters.com/en/insights/data-protected/data-protected---switzerland>

US State Privacy Law Comparison: <https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison>

Global Data Privacy Laws: <https://dlapiperdataprotection.com>





Smarsh® is the recognized global leader in electronic communications archiving solutions for regulated organizations. The Smarsh Connected Suite provides innovative capture, archiving, e-discovery, and supervision solutions across the industry's widest breadth of communication channels.

Scalable for organizations of all sizes, the Smarsh platform provides customers with compliance built on confidence. It enables them to strategically future-proof as new communication channels are adopted, and to realize more insight and value from the data in their archive. Customers strengthen their compliance and e-discovery initiatives, and benefit from the productive use of email, social media, mobile/text messaging, instant messaging and collaboration, web, and voice channels.

Smarsh serves a global client base that spans the top banks in North America and Europe, along with leading brokerage firms, insurers, and registered investment advisors. Smarsh also enables federal and state government agencies to meet their public records and e-discovery requirements. For more information, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.