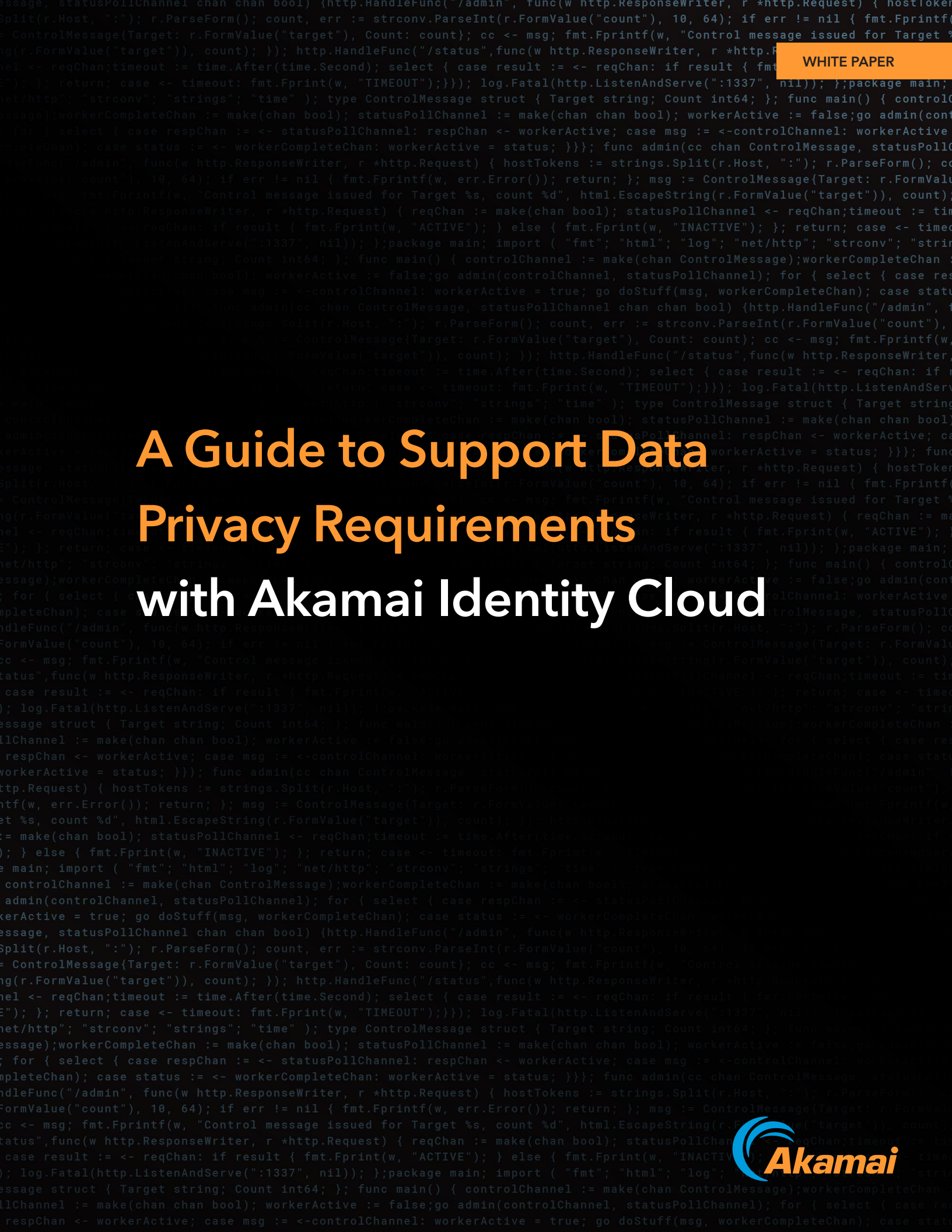
WHITE PAPER

A Guide to Support Data Privacy Requirements with Akamai Identity Cloud



How Can Akamai Identity Cloud Help with Compliance?

Laws and regulations related to personal information (PI) are continuously being enacted around the world as data breaches and abuses persist. Understanding the variations among the many different privacy and data protection laws can be challenging for organizations — from the European Union's General Data Protection Regulation (GDPR) to the California Consumer Privacy Act (CCPA) in the United States, Australia's Privacy Act (APA), Japan's Act on the Protection of Personal Information (APPI), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) — each regulation has its own nuances.

Our customers often ask about specific privacy law sections and about the ways Akamai supports compliance. To help you protect data privacy, we've compiled a list of general requirements that can be found across many data protection and privacy regulations around the world. We describe each obligation briefly, then explain how our customer identity and access management (CIAM) solution, Akamai Identity Cloud, can help to address them.

CIAM is a systematic approach paired with dedicated software solutions that has been critical in helping brands collect and manage customers' personal data in a way that ensures security and compliance with regulatory measures. CIAM enables organizations to utilize customer data within their marketing automation and content management systems so that brands can continue to create highly personalized customer experiences while simultaneously satisfying regulatory requirements and their customers' growing desire for data privacy.

Following is a guide to using Akamai Identity Cloud to support compliance with 11 common data protection obligations from the various privacy laws and regulations around the world.

Table of Contents

Obtaining and Managing Consent

For certain activities performed by organizations, the underlying data usage is based on the individual's prior consent. Requirements for obtaining valid consent and the circumstances when it is required for data usage varies among the regulations. Managing consent and honoring the individual's choice to grant or withdraw consent is essential under global data protection laws, but can be challenging to implement.

How Identity Cloud Can Help

Identity Cloud allows organizations to collect consent and provides a preference center self-service portal for users to view, modify, and revoke it.

User experiences and forms are customizable to support both opt-in and opt-out scenarios and can request consent at the time of account registration, after login, or at any stage of the customer journey. You can also grant users the ability to manage their consent on a self-service basis at any time.

Consents and preferences are stored in an auditable fashion alongside user data as part of the customer data record. All user data is encrypted in motion and at rest. Access logs provide evidence of the actions taken by a user for transparency and accountability.

OBLIGATION	Obtaining and Managing Consent
EU GDPR	Art 4 (11), 7 (3)
CALIFORNIA CCPA	Section 1798.120
CANADA PIPEDA	Schedule 1 Clause 4.3
MEXICO LFPDPPP	Art 8 and 9 of the Law
AUSTRALIA APA	APP Guidelines Chapter B.34
JAPAN APPI	Art 16
SINGAPORE PDPA	Art 13 and 16
BRAZIL LGPD	Art 7 (1) and Art 8
ARGENTINA LPDP	Section 5
INDIA PDP BILL 2019	Clause 11

Right to Object

The right to object entitles an individual to deny the use of personal data for certain types of data processing, such as direct marketing or statistical analysis.

How Identity Cloud Can Help

Identity Cloud provides a customizable preference center that allows users to select or deselect what types of data processing they approve.

This user interface and design is integrated with the registration and login experience, where users can select the types of data processing they accept, as well as take other actions on their profile. Preferences are stored alongside user data as part of the customer record, and data is encrypted in motion and at rest. Preference settings can also be updated via API from any client-hosted page.

OBLIGATION	Right to Object to Any Processing Activity
EU GDPR	Art 21
CALIFORNIA CCPA	Section 1798.120
CANADA PIPEDA	Schedule 1 Clause 4.3.8
MEXICO LFPDPPP	Art 22, Art 27 ff
AUSTRALIA APA	Not explicitly covered
JAPAN APPI	Art 30 APII
SINGAPORE PDPA	Not explicitly covered
BRAZIL LGPD	Art 18 VIII
ARGENTINA LPDP	Art 16 and Art 30
INDIA PDP BILL 2019	Clauses 7 (d), 11 (e)

Parental Consent for Children

Requires an individual to be a certain age for consent to be valid. For individuals below the applicable age threshold, a legal guardian can provide valid consent on their behalf. Please note that the age threshold for valid consent varies by country.

How Identity Cloud Can Help

Identity Cloud has age-gating functionality to protect against acceptance of personal data from children who cannot provide valid consent under applicable laws because of their age.

OBLIGATION	Parental Consent for Children
EU GDPR	Art 8
CALIFORNIA CCPA	Section 1798.120 (c)
CANADA PIPEDA	Schedule 1 Clause 4.3
MEXICO LFPDPPP	Art 89 III of the Regulation and the Guide page 11 and 12
AUSTRALIA APA	APP Guidelines Chapter B.47, 52 and 53
JAPAN APPI	Not explicitly covered
SINGAPORE PDPA	Advisory Guidelines on Selected Topics by the PDPA, revised August 31, 2018
BRAZIL LGPD	Art 14 § 1
ARGENTINA LPDP	Art 18
INDIA PDP BILL 2019	Clause 16 (2)

Right to Access by the Data Subject

Allows individuals to access the personal data being processed including, in some cases, the right to seek additional information about the uses and disclosures of such data.

How Identity Cloud Can Help

Identity Cloud provides a customizable preference center, which allows users to access their data anytime from anywhere. The self-service portal allows users to control data preferences by easily checking the scope and accuracy of the information provided without the need for customer support services.

OBLIGATION	Right of Access by the Data Subject
EU GDPR	Art 15, 20
CALIFORNIA CCPA	Section 1798.100
CANADA PIPEDA	Schedule 1 Clause 4.9
MEXICO LFPDPPP	Art 22-23 and 29-35 of the Law and Art 101 of the Regulation
AUSTRALIA APA	APP 12 and APP Guidelines Chapter 12
JAPAN APPI	Art 19
SINGAPORE PDPA	Art 21
BRAZIL LGPD	Art 9 and Art 18 (2)
ARGENTINA LPDP	Art 27
INDIA PDP BILL 2019	Clause 17 (3)

Right to Rectification

Provides individuals with the right to correct the personal data being processed.

How Identity Cloud Can Help

Identity Cloud allows users and service representatives to edit data records anytime from anywhere to ensure the data elements are current and accurate. Rectification activities are logged and auditable and can serve as evidence for data control by users.

OBLIGATION	Right to Rectification
EU GDPR	Art 5 (1) d, 16
CALIFORNIA CCPA	Section 1789.100 (a)
CANADA PIPEDA	Schedule 1 Clause 4.9.5
MEXICO LFPDPPP	Art 11 (2), 22 and 24, 28-31 and 35 of the Law
AUSTRALIA APA	APP 13 and APP Guidelines Part 13
JAPAN APPI	Art 19
SINGAPORE PDPA	Art 22
BRAZIL LGPD	Art 8 and Art 18 (III)
ARGENTINA LPDP	Art 29
INDIA PDP BILL 2019	Clause 18

Right to Erase or Delete Personal Data ("Right to Be Forgotten")

Many laws include the right for individuals to have their personal data erased and no longer disseminated to third parties or exposed to third-party processing, also known as the "right to be forgotten."

How Identity Cloud Can Help

Identity Cloud allows secure (non-restorable) deletion of data records, including deletion from backups, to help prevent the accidental sprawl of data. The right to be forgotten can be performed by users or service representatives easily anytime from anywhere.

OBLIGATION	Right to Erasure ("Right to Be Forgotten")
EU GDPR	Art 17
CALIFORNIA CCPA	Section 1798.105 Exemptions: 1798.145 (g)(3)
CANADA PIPEDA	Schedule 1 Clause 4.9.5
MEXICO LFPDPPP	Art 11 (3), 22, 28-32 and 35 of the Law
AUSTRALIA APA	APP 4, APP Guidelines Chapter 4.2 and APP 13 and APP Guidelines Chapter 13
JAPAN APPI	Art 19 APPI
SINGAPORE PDPA	Art 25
BRAZIL LGPD	LGPD Art 18 (VI)
ARGENTINA LPDP	Art 31
INDIA PDP BILL 2019	Clauses 18, 20

Data Portability

Requires organizations to provide individuals with copies of their data in a commonly used, machine-readable format, allowing them to transfer their data to another organization without hindrance.

How Identity Cloud Can Help

Identity Cloud provides a customizable preference center, which allows users to request a download of their data. Organizations can easily act on a data portability request and download the data from Identity Cloud and any other systems that hold user data. It is possible to have Identity Cloud trigger an event to start the process of collecting and delivering the data needed to satisfy the regulatory requirement. Identity Cloud user data can be provided in JSON, an open-standard file format that is both human- and machine-readable.

OBLIGATION	Right to Data Portability
EU GDPR	Art 20
CALIFORNIA CCPA	Section 1798.100
CANADA PIPEDA	Not explicitly covered
MEXICO LFPDPPP	Not explicitly covered
AUSTRALIA APA	Consumer Data Right Bill 2019 (applicable to consumers only)
JAPAN APPI	Not explicitly covered
SINGAPORE PDPA	Right is still in consultation
BRAZIL LGPD	Art 11, 17, 18 and 40
ARGENTINA LPDP	Art 33
INDIA PDP BILL 2019	Clause 19

Vendor Risk Management

Organizations must ensure data protection and security, independent of whether they are processing personal data themselves or having a third-party service provider process the data on their behalf. For this reason, vendor risk management is a key part of overall compliance.

How Identity Cloud Can Help

Akamai is a trusted service provider, ensuring data protection and security of the personal data it processes on behalf of its customers by the technical and organizational measures implemented. The certifications and attestation covering Akamai Identity Cloud are evidence of the appropriateness of these measures, serving as effective risk mitigation.

Identity Cloud provides strong user authentication and sophisticated protection mechanisms against network-based threats – all secured behind the Akamai Kona Site Defender web application firewall. In addition, it enables organizations to maintain access controls on a need-to-know basis. Identity Cloud maintains and is audited or assessed for certification and compliance with major security assurance programs, including:

- ISO 27001:2013
- ISO 27018:2014 (PII protection in the cloud)
- SOC 2 Type 2 (all five Trust Service Principles: Common Criteria/Security, Availability, Confidentiality, Processing Integrity, and Privacy)
- HIPAA/HITECH (protection of healthcare information at rest and in transit) Security Rule Compliant
- EU-US Privacy Shield Framework

OBLIGATION	Vendor Risk Management
EU GDPR	Art 32
CALIFORNIA CCPA	Section 1798.81.5
CANADA PIPEDA	Schedule 1 Clause 4.7
MEXICO LFPDPPP	Art 19
AUSTRALIA APA	APP 11
JAPAN APPI	Art 20
SINGAPORE PDPA	Art 24
BRAZIL LGPD	Art 46 ff
ARGENTINA LPDP	Art 19
INDIA PDP BILL 2019	Clause 24

Breach Notification

Organizations must report data breaches within a certain period after first becoming aware of the situation. In general, the notification includes a description of the organization that was breached, type(s) of data accessed, approximate number of impacted individuals, expected or actual damage to individuals, and mitigation measures. The details of what to report, in what period, and to whom differ by country.

How Identity Cloud Can Help

Akamai has implemented an Information Security Event Management Policy with procedures and a related Communication Policy to support organizations with any data breach notification obligation. These policies and procedures are part of our ISO 27001:2013–certified Identity Cloud Information Security Management System.

OBLIGATION	Breach Notification
EU GDPR	Art 33
CALIFORNIA CCPA	Section 1798.29 (a) and 1798.82 (a)
CANADA PIPEDA	Clause 10.1 ff.
MEXICO LFPDPPP	Art 20
AUSTRALIA APA	Part IIIC APA
JAPAN APPI	Not explicitly covered
SINGAPORE PDPA	Guidelines on data breaches 2019
BRAZIL LGPD	Art 48
ARGENTINA LPDP	Art 20
INDIA PDP BILL 2019	Clause 25

Organization's Accountability

Each organization that controls personal data is accountable under applicable data protection laws for the protection and security of the data it processes. This requires the organization to know at any time what data it processes, where, for what purposes, and which third parties are accessing the data.

How Identity Cloud Can Help

Identity Cloud assists organizations in establishing accountability for data-processing activities. It maintains an auditable record of the data elements collected, including any edits to the data records.

In addition to protecting the data stored by appropriate technical and organizational measures, Identity Cloud offers fine-grained role- and attribute-based access controls and a log mechanism to provide evidence of any data access. These safeguards demonstrate that organizations that use Identity Cloud to process personal data are acting in an accountable manner.

OBLIGATION	Accountability of an Organization
EU GDPR	Art 5 (2)
CALIFORNIA CCPA	Section 1798.100
CANADA PIPEDA	Schedule 1 Clause 4.1
MEXICO LFPDPPP	Art 14
AUSTRALIA APA	APP 1 and Chapter 1 of the Guidelines
JAPAN APPI	Art 15 ff
SINGAPORE PDPA	Art 3
BRAZIL LGPD	Art 6 (10)
ARGENTINA LPDP	Art 10
INDIA PDP BILL 2019	Clauses 22 ff. and 29

Data Residency and Transfer

Data residency may play an important role in organizations because of internal corporate or statutory requirements. Statutory data residency laws apply; for example, in Russia and China. In many countries, there are no data residency requirements, but data transfer requirements are put in place to ensure the in-country level of data protection is maintained.

How Identity Cloud Can Help

Identity Cloud offers various data residency settings to satisfy related requests by customers, including the China and Russia regions. For China, in accordance with applicable laws, this includes no encryption at rest for personal identifiable information stored in the region.

For Russia, the Identity Cloud Russia solution provides a "write first in Russia" approach, with the application hosting and data storage of customer's PI taking place in a secondary region in the European Union.

Akamai is certified under the Privacy Shield program and agrees with its customers on Standard Contractual Clauses to ensure any in-country data protection level is maintained when data is transferred to other countries.

OBLIGATION	Data Residency/Data Transfer Requirements
EU GDPR	Art 46 ff.
CALIFORNIA CCPA	Not applicable
CANADA PIPEDA	Schedule 1 Clause 4.1.3
MEXICO LFPDPPP	Art 36 ff.
AUSTRALIA APA	APP 8
JAPAN APPI	Art 24
SINGAPORE PDPA	Art 26
BRAZIL LGPD	Art 33 ff.
ARGENTINA LPDP	Art 23 ff.
INDIA PDP BILL 2019	Clauses 33 ff.

Conclusion

Data privacy laws and regulations hold organizations accountable when processing personal data, and allow individuals to retain control over any processing of their personal data by third parties. Akamai Identity Cloud allows individuals to manage their data and provides organizations with a record for transparency and accountability when processing personal data. Identity Cloud offers easy-to-use tools and processes that assist you in maintaining compliance with applicable data protection laws, keeping personal data safe, and fostering customer trust.

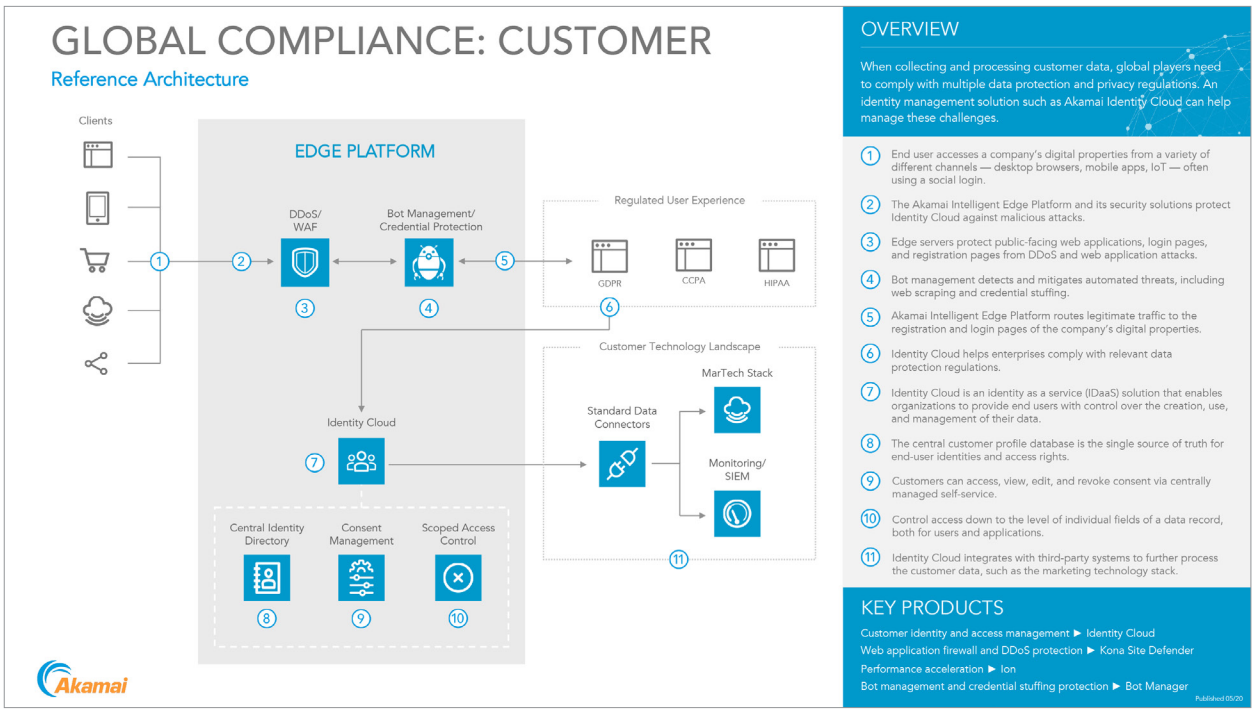
Laws and Regulations Overview

REGION	LAW	LINK
European Union (EU)	General Data Protection Regulation (GDPR)	GDPR
California	California Consumer Privacy Act (CCPA)	CCPA
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	PIPEDA
Mexico	The Federal Law on the Protection of Personal Data held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) 2010 and the related Regulations of 2011	LFPDPPP
Australia	Australian Privacy Act (APA); Privacy Act 1988 / Australian Privacy Principles (APP)	APA APP
Japan	Act on Protection of Personal Information (APPI)	APPI
Singapore	Personal Data Protection Act 2012 (PDPA)	PDPA
Brazil	General Data Privacy Law; Lei Geral de Proteção de Dados Pessoais (LGPD)	LGPD
Argentina	Argentina Personal Data Protection Law; Ley de Protección de Datos Personales (LPDP)	LPDP
India	The Indian Personal Data Protection Bill (PDP Bill 2019) has been introduced by the Indian Parliament and is still in discussion as of May 2020. It has been included in this whitepaper for the sake of completeness.	PDB Bill 2019 (proposal)

Global Compliance Reference Architecture

When collecting and processing customer data, global players need to comply with multiple data protection and privacy regulations. An identity management solution such as Akamai Identity Cloud can help manage these challenges.

Global Compliance: Customer



Find more reference architectures at https://www.akamai.com/us/en/solutions/akamai-architectures.jsp.

Akamai *Experience the Edge*

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 07/20.