Guide to Privacy and Compliance
Introduction

In the wake of a growing portfolio of new privacy and data protection regulations across the globe, we are witnessing a worldwide trend requiring companies to adopt a multiregional compliance strategy for consumer privacy and personal data security. Among the regulations that global players need to comply with are the European Union’s General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), and many others.

Global 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 much larger fines – eventually leading up to the staggering GDPR 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 to protect their valued privacy, sales and marketing power will suffer. Businesses today need express consent in order to process personal data. Without trust, there is no consent and therefore no data. And that results in ineffective sales and marketing campaigns.

Privacy and identity governance help global businesses form trusted relationships with users and customers, resulting in higher customer loyalty – and ultimately higher business revenue.
The Need for a Multiregional Compliance Strategy

According to data from the United Nations, 107 countries have put in place legislation to secure the protection of data and privacy. Currently, 68% of all countries have existing or pending privacy legislation.

While the scope of individual country and state regulations vary, the largest economies tend to have the strictest regulations. But the common thread is that companies doing business around the world need the ability to cope with a large variety of privacy laws that are similar in many aspects, but at a detailed level incorporate many important differences.

In the case of regulations, the details matter. Most regulations require different customer identity implementations. From a practical standpoint, it does not make sense to try to comply with each regional requirement via deployment of individual local IT solutions. After all, most global companies want a centralized database with a single 360-degree view of the customer.

Some companies are contemplating a strategy based on implementing the most stringent data privacy provisions and then applying them across the globe. However, that won’t work either, because some data privacy requirements are mutually exclusive. For example, while both GDPR and CCPA require companies to obtain consent before collecting personal data, the specifics differ. A common static user consent screen simply won’t work.

Under GDPR, organizations cannot 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. Such differentiation can cause headaches for global players faced with the prospect of addressing multiple major markets with solutions that need to display different registration forms.

What’s more, some of the new regulations 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 not allowed. This means businesses have to rethink and redesign their user experiences and eliminate all data fields on registration pages and other forms that could be considered excessive. In regions where there are no such restrictions, marketing teams might still want to collect additional data.

What’s needed is a centralized customer identity solution that has the flexibility to adapt to individual, regional regulations – a system that can deliver different user interfaces and handle personal data differently depending on the location of the consumer.

Meeting the Global Challenge

To meet global regulations, protect customer data, and maintain consumer trust, global companies need to implement flexible customer identity and access management (CIAM) solutions to secure user data and credentials with strong encryption and scoped access control. Rather than trying to address the regulations one at a time as they arise – and then having to reinvent the wheel each time – the prudent approach is to deploy a solution flexible enough to meet current and future regulations.

Whether building such a CIAM solution in-house, or deploying a professional-grade commercial solution, organizations must ensure that their identity management solution is able to address key regulatory issues such as consent, right to object, right to access and delete data, data portability, security, and more.

Consent

A common aspect of the various regional regulations is the mandate that organizations must obtain consent prior to collecting and processing personal data. Requirements for obtaining valid consent and when such consent is required vary among applicable regulations. Therefore, companies should deploy a solution that supports user experiences (like web forms) and design patterns to ask for consent at the time of account registration, as well as after account login at any stage of the customer journey. User experiences need to be fully customizable to support both opt-in and opt-out scenarios.
Right to Object
Consumers must be able to object to the use of their personal data for certain types of processing, such as direct marketing or statistical analysis. This requires a solution with a customizable preference center that will allow consumers to select or deselect what types of data processing they approve.

Right to Access
Many laws provide the consumer 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. This again requires a customizable identity management preference center that allows consumers to request access to their data. Companies can then act on the request and pull data from a central database or other systems that hold customer data.

Right to Delete Data
Often referred to as the “right to be forgotten,” GDPR, CCPA, and other regulations include the right for consumers to have all or parts of their personal data erased and have it no longer disseminated to third parties or exposed to third-party processing. Companies must ensure that their CIAM solution allows secure, nonrestorable deletion of data records – including deletion from backups – to help prevent the accidental sprawl of toxic data.

Data Portability
Compliance regulations state that consumers must be provided with copies of their data in a commonly used, machine-readable format, allowing users to transfer their data to another organization without hindrance. Companies must therefore implement solutions that allow such requests and are able to pull data from a centralized database or other systems that hold customer data, and export it into common data formats such as JSON.

Security and Breach Notification
Companies must implement appropriate data security safeguards to protect the personal data they process and the privacy of the affected consumers. Included are safeguards that are specifically noted in certain regulations, such as encryption of personal data in transit and at rest. In addition, organizations must notify consumers of any data breaches within a certain time after first becoming aware of the situation. These important security measures must be fully addressed by the identity management solution.
Scoped Access

Whether developed in-house or obtained from a commercial vendor, the CIAM solution should provide highly granular permission levels to ensure full control over which people and applications can access and manipulate customer data — all based on roles and responsibilities. Fine-grained access control should be applied all the way down to data columns, rows, and fields. For example, it should be possible to define roles that allow developers to perform application administration tasks without allowing them to gain access to any customer data.

Conclusion

Beyond meeting multiregional customer identity compliance regulations, privacy and security assurances are crucial for global organizations that want to build deep and trusted digital relationships with their customers. Consumers have increasingly high expectations that their personal data will be kept private and secure.

The growing portfolio of regional laws and regulations — not to mention the many publicized cases of data abuse, breaches, and identity theft — have massively raised the bar for global enterprises to be considered 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 very difficult to restore.

Rather than trying to build trust by addressing new regional regulations on a case-by-case basis, now is the time to deploy global, flexible, enterprise-grade identity management solutions to meet the needs of today and the future.

For more information, read our new white paper GDPR, CCPA, and Beyond: How Identity Governance Helps Companies Comply and Improve Customer Trust for information.

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 2/20.