WHITEPAPER

COMPARING GDPR TO U.S. STATE COMPLIANCE REGULATIONS

GDPR vs. CCPA and NY SHIELD Act

BeyondTrust

CONTENTS

GDPR vs. Local & State Laws

The General Data Protection Regulation (GDPR) is a European Union law that was implemented May 25, 2018, and requires organizations to safeguard personal data and uphold the privacy rights of EU citizens and anyone residing in EU territory. The GDPR unifies the EU under a single data protection mandate. GDPR is designed to unify data privacy laws across all of its members countries, while also providing greater protection and rights to individuals. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines. The GDPR replaced the 1995 Data Protection Directive, which created a country-by-country patchwork of data protection laws.

The EU General Data Protection Regulation (GDPR) has been designed to better protect how personally identifiable information (PII) of EU citizens and residents is collected, processed, and stored. Any company with customers in the EU or that serves EU citizens, regardless of where in the world they are located, is subject to the GDPR mandate in regard to the personal data collected and stored

While GDPR applies to all countries in the European Union, there is not a similar comprehensive mandate in the United States. In the US, organizations are subject to a variety of compliance mandates that depend on industry, location, and other factors. Some states have released their own guidelines, adding to the compliance considerations for companies serving customers in those states. Two state initiatives currently in place are the California Consumer Privacy Act (CCPA) and the New York State “Stop Hacks and Improve Electronic Data Security Act” (SHIELD Act).

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) has been quoted as the beginning of America's GDPR-type data privacy laws. CCPA was signed into law on June 28, 2018 and went into effect on January 1, 2020.

Similar to the GDPR, the CCPA requires organizations to focus first on consumer data in 2020 and then personal data shared between businesses in 2021. It is a state-wide law that regulates how personal information of California residents is allowed to be used and shared by businesses.

To be regarded as a business under the CCPA rules, a company has to meet one of the three following attributes:

- Annual gross revenue exceeding $25 million
- Derive 50% or more of its annual revenues from selling consumers' personal information
- Buy, receive, sell, or share the personal information of 50 or more California residents, households or devices a year.

This means that regardless of where a company is based around the world, , if that company buys or sells the personal information of at least 50 California residents, it is liable for CCPA compliance.

See the table in this document to compare GDPR and CCPA requirements.

New York State SHIELD Act

The NY SHIELD (Stop Hacks and Improve Electronic Data Security) Act went into effect on March 21, 2020. New York's law requires the implementation of a cybersecurity program, including reasonable protective measures, such as risk assessments, workforce training, and incident response planning and testing. New York's law covers all employers, individuals, and organizations, regardless of size or location, which collect private information on New York State residents.

The law broadly requires that "any person or business" that owns or licenses computerized data which includes private information of a New York State resident "shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information." To achieve compliance, an organization must implement a data security program that includes reasonable administrative, technical, and physical safeguards.

All organizations that collect private information about New York state residents must independently satisfy the SHIELD Act three-part standard for protecting sensitive individual information. However, regulated organizations that are covered by and in compliance with the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and/or the New York State Department of Financial Services cybersecurity regulations shall be deemed in compliance with the SHIELD Act.

Failure to implement a compliant information security program is enforced by the New York State Attorney General and may result in injunctive relief and civil penalties of up to $5,000 imposed against an organization and individual employees for "each violation." Depending on how the Attorney General seeks to apply this provision, this could potentially lead to significant monetary penalties for entities and their employees who fail to take required protective measures, including when those failures lead to a data breach.

See the table in this document to compare GDPR and NY SHIELD Act requirements.

Comparing GDPR to CCPA and NY SHIELD Act

Governance	GDPR	CCPA	NY SHIELD Act
Scope	All personal data collected for European Union citizens and residents	All California residents whose personal data is collected after January 2020 and for business-to-business data, starting January 2021	All entities that store and transmit residential New York state residents' private data and consumer sensitive information. Full enforcement was required in March 2020
Responsibility	GDPR requires ownership for sensitive data within the organization and the location, storage, and processing of personal information. This includes an assignment of a Data Protection Officer	CCPA does not require an individual be assigned an owner for compliance purposes	NY SHIELD requires an individual have cybersecurity responsibilities within an organization
Implementation of Safeguards	GDPR does not provide specific details and technology recommendations for the safeguarding of personal information.	CCPA has safeguards to protect minors under 13 years of age, a "Do not sell my information" right, a public method for submitting data requests, and requires a 12-month delay for any opt-ins after an opt-out. There are no technical or physical safeguard recommendations	NY SHIELD requires very specific physical and technical safeguards be implemented and monitored to ensure the security of personal information

Governance	GDPR	CCPA	NY SHIELD Act
Personal Identifiable Information	GDPR is not restricted to personally identifiable information, but rather what information is generally stored about a person, how it is processed, how it is shared, and when it should be erased	CCPA defines personal information as data that could be associated with a particular consumer or household, including real name, alias, postal address, unique personal identifiers, email address, social security number, driver's license number, passport number, and many other unique identifiers	NY SHIELD explicitly defines personal information as passwords, biometrics, driver's license number, social security number, and many others to avoid any ambiguity
Organizational Size	Any organization or entity that collects data or processes data for European Union residents	CCPA is enforceable for any entity that has gross revenue over $25 million, buys, sells, or processes over 50k records for individuals or household, or earns more than half their revenue from the sale of personal information	Small businesses below 50 employees, $3Million in revenue, and $5 million in assets may modify the safeguards to meet their business requirements
Right to Access	An individual has the right to review all European Union personal data processed for an individual	An individual has the right to access personal data in scope collected for the last 12 months, with restrictions imposed on whether the data was stored, sold, or transferred between organizations	An individual has no right to request the deletion of personal information stored by a business or entity.

Governance	GDPR	CCPA	NY SHIELD Act
Right to Portability	Data must be able to be imported and exported in a user-friendly format. This is similar to United States HIPAA regulations	All individual access requests must be exportable in a user-friendly format, but there is no requirement for importing data	An individual has no right to export the personal information being stored by a business
Right to Remediate	An individual reserves the right to correct and verify any personal data European Union data that has been collected	CCPA lacks a corrective actions provision for personal data	NY SHIELD lacks a corrective actions provision for personal data
Right to Halt Processing	An individual has the right to withdraw consent or stop processing, within an entity, of personally collected data	An individual has the right to “opt-out” of selling personal data and businesses must provide an opt-out link or procedure on their website or through a similar data collection vehicle	An individual does not have any rights to “opt-out” for the sale and processing of personal information
Right to Stop Automation	An individual has the right to enforce a human decision in an automated process that may have a legal effect for the inquiring party	CCPA has no provisions to stop automated decision-making	NY SHIELD has no provisions to stop automated decision-making

Governance	GDPR	CCPA	NY SHIELD Act
Right to Stop Information Sharing	An individual has the right to request the halting of third-party data transfers based on a specific category of data	An individual has the right to “opt-out” of selling their personal information to third parties	NY SHIELD has no provisions to stop information sharing, however sensitive personal information, which is explicitly defined, must be secured appropriately
Right to Information Erasure	A European Union citizen can request the right to erase personal data if specific conditions are met	An individual has the right to erase personally collected data only under specific conditions	NY SHIELD has no provisions to erase personal information within a business or entity
Individual Damages	No limits to pursue damages based on actions	Each consumer breach is limited to a minimum of $100 and a maximum of $750 per data breach event	An individual does not have the right to sue a business or entity for a breach under NY SHIELD
Enforcement Penalties	Global annual revenue is capped at 4%	Regulator penalties are limited to $2,500 for unintentional violations and $7,500 for intentional violations	Organizations face civil penalties of up to $5,000 per violation and no penalty caps for failing to notify authorities when a breach occurs

How BeyondTrust Can Help Your Organization Meet Compliance Requirements

BeyondTrust's Privileged Access Management (PAM) solutions enable businesses to control, monitor, and manage access to critical systems and data, while ensuring that people remain productive and are not impeded in their day-to-day job tasks. BeyondTrust solutions secure and manage privileges across every user, session, and asset.

Key benefits related to compliance include:

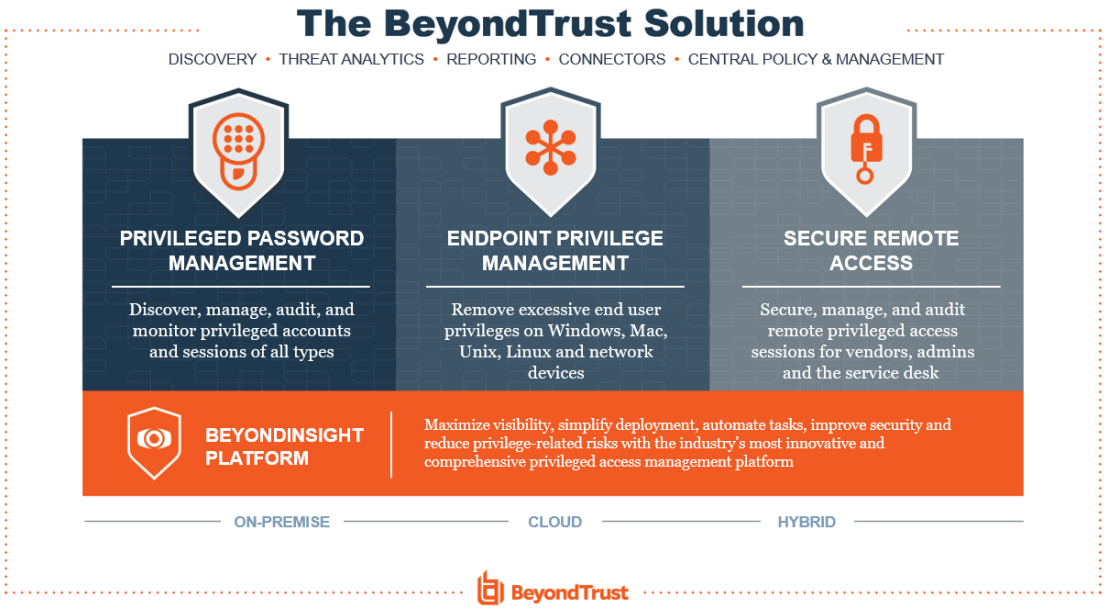
- **Enforce policy of least privilege:** Only give access to data to those who need it, when they need it, with granular levels of access controls that eliminate "all or nothing" access
- **Secure and protect all privileged accounts:** Privileged credentials are stored, rotated, and managed within a secure enterprise password vault, and privileged users are granted access based on their job roles and requirements
- **Create an audit trail:** Every session and all session activity is fully recorded, creating accountability of which specific people accessed a system and what actions were taken, to provide effective attribution
- **Remove all point-to-point pathways:** BeyondTrust's secure architecture breaks any point-to-point access paths into your systems with no descending connections, eliminating the need for VPNs
- **Encrypt communication:** BeyondTrust ensures all privileged access session data in transit or at rest are encrypted using TLS 1.2
- **Enforce data security policies to meet GDPR compliance:** Integrate your identity providers and security policies with BeyondTrust solutions

The BeyondTrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

Conclusion

The General Data Protection Regulation (GDPR) is one of the most important movements in the area of data protection in recent years. While no similar comprehensive mandate exists in the United States that covers all Americans, individual states are expected to continue to consider enacting more localized guidelines.

Complying with these regulations will be essential for many organizations. The BeyondTrust PAM Platform can be quickly deployed to help your organization achieve compliance with a fast time-to-value.

Notes

- This document does not constitute a full guide to GDPR compliance, CCPA compliance, or NY SHIELD Act compliance. BeyondTrust recommends that you consult with a legal specialist in order to manage your compliance with these regulations.

- This document includes information on how products from BeyondTrust can enable customers to meet GDPR requirements. For information on compliance by BeyondTrust with GDPR regarding our own customer data, visit beyondtrust.com/gdpr-statement.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.