New Privacy Regulations: GDPR, CCPA, PIPEDA, POPI, LGPD, HIPAA, PCI-DSS, and More

September 17, 2019 | Topics: Cloud Volumes ONTAP, Cloud Data Sense, Data Protection, Advanced

Whether we like it or not, our personal data is constantly being gathered and—often stored—electronically. The recent scandal around Facebook and Cambridge Analytica highlights just how vulnerable our personal data is and the importance of it being handled and used responsibly.

Three notable examples of laws and regulations have been put in place by governments and by industry to protect personal data are HIPAA, GDPR, and PCI-DSS. But regulations that have followed in the footsteps of the GDPR such as CCPA, PIPEDA, POPI, and LGPD are also major concerns for enterprises. This blog will look at all these data security and privacy regulations and how NetApp's Cloud Volumes ONTAP can help supporting their compliance.

This is part of an extensive series of guides about compliance management.

GDPR Data Protection

The General Data Protection Regulation (GDPR) was enacted by the

European Union to deepen and harmonize personal data protection regulations. Now in effect as of May 25, 2018, it is a comprehensive and clear set of guidelines that acknowledges that different "flavors"

and clear set of guidelines that acknowledges that different "flavors" of personal data require different levels of protection. Sensitive data, such as health, biometrics, genetic, or criminal history are subject to the highest levels of protection. The quantity of data also counts, with companies that regularly collect and process large volumes of personal data having to register with government-appointed Data Protection Authorities.

GDPR applies to all companies, no matter where they are based, who collect and process personal data on EU residents. Non-EU companies have to appoint a GDPR representative and will be liable for all fines and sanctions.

Some of the key requirements of the GDPR are:

- Consent: Organizations must get consent to collect personal data, with the level of consent varying according to the type of personal data being collected.
- Data minimization: Responding to years of gratuitous collection of personal data by apps, with no clear purpose in mind, the GDPR stipulates that organizations can only collect personal data that is clearly related to a well-defined business objective. If an organization gathers personal data for one purpose but then decides it wants to use it for another purposes (such as consumer profiling), that could be considered non-compliance.
- Individual rights: Another key feature of the GDPR is the very clear rights that it gives data subjects (i.e., the individuals whose personal data is being collected) to understand why their data is being collected and how it is being processed. They have the right to object, to correct—and they have the right to be erased/forgotten. They also have the right to be notified (individually) if their personal data has been breached in a way that could endanger their freedoms and rights.

One of the most unique aspects of the GDPR is its "teeth"—very stiff penalties for non-compliance (up to €10 million or 2% of worldwide annual turnover, whichever is higher) and breaches (up to €20 million or 4% of worldwide annual turnover, whichever is higher). Just as painful is the right of Data Protection Authorities to prevent a company from collecting or processing personal data while a suspected non-compliance or breach is being investigated.

CCPA: The California Consumer Privacy Act

The California Consumer Privacy Act (CCPA) focuses on consumer privacy rights. In effect as of January 1, 2020, and enforced by the Attorney General of the State of California, CCPA will regulate data

More about Data Privacy

Data Protection in the Cloud: The Basics and 7 Best Practices

Data Protection Officer vs Chief Privacy Officer: A Comparison of Two Compliance-Related Roles

belonging to individuals, such as internet activity, cookies, IP addresses, and biometric data, as well as “household data” generated by IoT devices in the home, for example.

Under CCPA, consumers will have the right to know what personal data is collected or sold, and for what purpose, including disclosures of previous sales dating back to January 1, 2019. They will have the right to access the data, to request its deletion, and to opt-out of it being collected or sold. Those who exercise these privacy rights will still be entitled to equal services at the same cost. Consumers will also have the right to sue companies for data breaches and for privacy failures.

Any organization that could potentially possess the data of a California resident could be subject to CCPA regulations, and non-adherence could lead to penalties of up to $7500 per violation. In addition, consumers will be able to sue companies for data breaches for damages of $100 to $750 per record.

PIPEDA: Personal Information Protection and Electronic Documents

The Personal Information Protection and Electronic Documents Act (PIPEDA), which received royal assent on April 13, 2000, is the Canadian federal privacy law for private-sector organizations. Its original purpose was to evoke trust in electronic commerce by regulating businesses that handle personal information. This regulation applies to any Canadian-based private enterprise that collects consumer data in the course of commercial activities, as well as international companies that target Canadian customers. PIPEDA applies to data collected about an identifiable individual, such as name, age, ethnicity, medical history, opinions, comments, and marital status.

PIPEDA is based upon ten fair information principles, according to which businesses must obtain their customers’ consent prior to data collection. In addition, they must uphold transparent personal data policies, and limit data collection to clear and specific purposes. Individuals have the right to access their data and to challenge its accuracy. PIPEDA also holds organizations accountable for data loss or theft. As of November 1, 2018, organizations subject to PIPEDA are obliged to disclose security breaches of personal information to the Privacy Commissioner of Canada, and to individuals affected by the breach. Failing to do so, could result in fines as high as CAD$100,000.

Data Privacy Vs. Data Security: How Are Data Privacy and Data Security Related?

What's In Your Data? Enterprise

Subscribe to our blog ▸

LGPD: The Brazilian General Data Protection Act

The Brazilian General Data Protection Act (LGPD), which will come into effect in 2020, aims to supplement and replace existing legislation with a general data protection law that regulates both the public and private sectors. It is not only intended to protect personal data, but to strengthen Brazil's economy by aligning with international compliance standards set by GDPR. LGPD regulates any organization, be it a small business or a multinational corporation that collects Brazilians' personal information. Data protected encompasses both that of an identifiable individual as well as anonymous data from which identity can be inferred, or used in behavioral profiling.

Entities subject to LGPD must appoint a Data Protection Officer (DPO) that implements best practices and communicates with the ANPD, Brazil's data protection authority. Companies must also ensure that personal data is secure, and must notify the ANPD of any potentially damaging data breaches. In addition, consumers will have the right to know for what purpose their data is being collected, and request its alteration, deletion, or transfer. Companies that fail to comply with these regulations will be subject to pay up to 2% of their total annual revenue in Brazil or up to $50 million Brazilian reals.

Australian Data Privacy Regulations

Australian data privacy regulations originate in the Privacy Act of 1988, which regulated the handling of personal information through a mixture of federal, state, and territory laws. These regulations, enforced by the Office of the Australian Information Commissioner (OAIC), apply to the private sector. Their objective is to protect consumer data by ensuring that Australian entities, with a turnover of over AU$3 million, meet certain compliance standards.

Following the formulation of GDPR and other international regulations, Australia has recently made efforts to update and improve its existing policies. As of February 2018, some Australian companies are obliged, under the Notifiable Data Breaches scheme, to report harmful data breaches to the OAIC. In addition, on November 26, 2017, the Australian government introduced the Consumer Data Right (CDR), which allows consumers in the energy, telecommunications, and banking sectors to access their data, and control who it is shared with and for what purpose. Violating these regulations, enforced by the Australian Competition and Consumer Commission (ACCC), could lead to penalties of up to $10 million.

POPI: The Protection of Personal Information Act

The Protection of Personal Information Act (POPI) was signed into law in South Africa on November 19, 2013, and is expected to come into effect later this year. Its key objective is to protect personal information collected in the public and private spheres. Under POPI, South African institutions must adhere to a set of compliance standards that ensure responsible collecting, storing, processing, and sharing of personal information. POPI applies to all South African companies, though it is aimed specifically at entities that handle vast amounts of consumer information such as banks, medical organizations, and insurance companies. The law not only protect individuals, but extends to any legally recognized entity, including companies and communities.

Under POPI, consumers have access to their data, can request its deletion or modification, and control with whom it is shared. Companies are required to collect data for valid and transparent reasons, retaining it only as long as is strictly needed. Moreover, they must adhere to security compliance standards; ensuring data is not breached or compromised, on their part or on the part of any third parties that may process the data on their behalf. Failing to meet POPI requirements can lead to reputational damage, fines, and imprisonment.

HIPAA Privacy and Security Rules

The main motivation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was to improve health care efficiency and patient care outcomes by encouraging the free flow of health information in the US. At the same time, these HIPAA compliance requirements mandated national standards to secure the privacy of personal health information. Compliance with HIPAA's final Privacy Rule has been compulsory since April 2003, and with its final Security and Enforcement Rules since April 2005.

What Is HIPAA Compliance?

The HIPAA rules and regulations apply to all "covered entities"—health plans, health care providers, and health care clearinghouses who transmit health information in electronic, oral or written form. It also applies to the business associates of covered entities, i.e., individuals or organizations who are contracted to provide services but are not part of the covered entity's workforce.

The Privacy Rule is concerned with the Security Rule is that it

The Privacy Rule is somewhat broader than the Security Rule in that it protects all "individually identifiable health information" that is either transmitted or held by a covered entity or its business associate, in any form or media—electronic, paper, or oral. This protected health information (PHI) includes information related to the individual's physical or mental health or condition, health care provided to the individual, or payment for the provision of health care to the individual. PHI also includes basic identifying information such as a patient's name, their date of birth, SSN, and home address. In order to encourage health care research, the Privacy Rule places no restrictions on the use or transmission of de-identified health information.

The Security Rule focuses solely on PHI that is held or transmitted electronically, or e-PHI. As worded in the Security Rule, covered entities must implement appropriate administrative, physical and technical measures to:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit.
- Identify and protect against reasonably anticipated security threats.
- Protect against reasonably anticipated, impermissible uses or disclosures.
- Ensure compliance by their workforce and business associates.

All these have to be satisfied for HIPAA-compliant cloud storage. The Office For Civil Rights (OCR) oversees HIPAA compliance. It can impose civil monetary penalties (CMP) for non-compliance with the law that range from $100 to $50,000 per affected PHI record, up to a maximum of $1.5 million per incident. In February of this year, for example, Fresenius was fined $3.5 million by the OCR for five incidents in which it failed to comply with HIPAA's risk analysis and risk management rules.

PCI-DSS Requirements

Payment Card Industry Data Security Standards (PCI-DSS) is a set of security standards developed by the major credit card companies to help protect sensitive cardholder data. Unlike HIPAA and GDPR requirements, which are based on governmental regulation, PCI-DSS compliance requirements are contractual commitments maintained and enforced by the Payment Card Industry Security Standards Council (PCI SSC), an independent global body established in 2006.

PCI-DSS applies to all merchants or organizations that accept, transmit or store cardholder data. However, there are different PCI-DSS compliance levels depending on the quantity of payment transactions that a merchant/organization has handled over the previous twelve months. The PCI-DSS describes six categories of control objectives:

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

It is the merchant/organization that is held responsible for the security of the cardholder data that it collects and holds, even if they use a third-party company to handle credit card payments. There are two ways that the merchant/organization is expected to validate its PCI-DSS compliance:

Quarterly vulnerability scans: Any merchant/organization that electronically store cardholder data after a payment is authorized must submit once per quarter to a vulnerability scan run by an Approved Scanning Vendor. The merchant's internet applications and networks are remotely reviewed by a non-intrusive scan. This scan seeks to identify vulnerabilities in operating systems, apps, and devices that could be used to gain unlawful access to the company's network.

Annual assessment: Merchants that process less than six million transactions per year must submit an annual Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC). Merchants that process more than six million transactions per year must be audited on-site by a Qualified Security Assessor (QSA) certified by the PCI SCC.

PCI- DSS regulations non-compliance can result in fines to the acquiring bank of $5,000-100,000 per month, with the banks usually seeking to pass the fine along to the merchant. In addition, the bank could terminate the relationship with the merchant or raise the transaction fees considerably. Should the data breach become public knowledge, the merchant may also have to bear indirect costs related to damage to its reputation.

Data Compliance and NetApp Cloud Volumes

It doesn't matter if it's AWS PCI compliance, AWS HIPAA compliance, Azure PCI compliance, GDPR Azure storage, or AWS GDPR compliance: HIPAA, GDPR, and PCI-DSS are agnostic as to where the personal data is being held. Whether it's in the cloud or on-premises or both, whether the data is in-transit or at-rest, the organization is responsible for preventing security breaches that could result in the disclosure or loss of personal data.

How does HIPAA cloud storage in the cloud affect data compliance? Are companies handling the changes that came with GDPR? As you can see in the results of this survey released by NetApp last year, most companies are still unsure about exactly how to comply with GDPR. That's a situation that is likely to change once fines start being issued.

As an enterprise-grade data management platform built on AWS, Azure, or Google Cloud storage, Cloud Volumes ONTAP gives users many of the features they need to protect their business and their customers' data. A major benefit is the availability of the new Cloud Compliance feature, which automatically scans cloud data to map, identify, and report on sensitive private data that falls under the guidelines of GDPR, CCPA, HIPAA, and other regulations.

Besides its functionality with Cloud Compliance, Cloud Volumes ONTAP supports security requirements through data encryption (both at rest and in transit), RBAC access, multi-tenancy, VPC/VNet and SubNet parameters, and more. It allows users to protect their data efficiently and maintain operations that can handle the worst failures by providing under sixty-second RTO and RPO of zero through the use of its AWS high availability configuration. As such, it gives companies the ability to comply with tight SLA requirements.

Can people attain data compliance without the cloud? Yes. But as the NetApp survey linked above also shows, the largest number of respondents were deploying hybrid cloud architectures, taking advantage of both traditional on-prem and cloud storage systems. To orchestrate and protect data across all of those environments it takes the kind of platform provided by NetApp Cloud Volumes and its easy-to-use GUI management tool, NetApp Cloud Manager.

Understanding Privacy by Design

Privacy by design (PbD) is a concept that calls to incorporate privacy protection into the creation and implementation of systems. The PbD framework outlines seven core principles that help ensure privacy becomes an integral part of continuous design and business practices.

See Additional Guides on Key Compliance Management Topics

Together with our content partners, we have authored in-depth guides on several other topics that can also be useful as you explore the world of compliance management.

PCI Compliance

Authored by Exabeam

- PCI Compliance: A Quick Guide
- Quick PCI Compliance Checklist: Be Ready for Your Next Audit
- PCI Audit: Requirements and 5 Steps to Prepare for Your Audit

PCI Compliant Hosting

Authored by Atlantic

- PCI Hosting Solutions | 12-Point PCI Compliant Hosting Checklist
- PCI DSS Cybersecurity Requirements: A Practical Guide
- Small Business PCI Compliance Guide: What You Need to Know

HIPAA IT Compliance

Authored by Atlantic

- HIPAA IT Compliance Checklist & HIPAA IT Infrastructure Guide 2023
- HIPPA or HIPAA? HIPAA vs. HIPPA - What's the Difference?
- Best HIPAA-Compliant Email Service in 2023

Yifat Perry
Technical Content Manager

-