A System Admin's Guide to Data Privacy Regulations

FILECLOUD

WWW.GETFILECLOUD.COM

Executive Summary

The wave of regulation that begun in Europe with the General Data Protection Regulation (GDPR) has managed to spread across the globe. Governments are now ardent on establishing regulatory environments that support data-driven economic growth while solidifying their trust in technology. Several countries are now considering data privacy laws for the first time, while others are looking to reappraise their current approaches.

In today's digital, global economy, an organization's use of personal data can no longer be regulated or contained in isolation within a single country. The coming frameworks that enable businesses, governments, and most importantly individuals to reap the benefits of the data revolution, have to respect national cultures, traditions and laws.

At this point, businesses have to be aware of the potential intrinsic risks of storing and managing customer data. Several high-level, publicized breaches have exposed the dire consequences of data mismanagement. These attacks have impacted major organizations in virtually every industry, affected millions of customers and cost companies billions of dollar, while further promoting cybercriminal activity.

Companies that have a solid grasp on the nature of the data they possess and a conscientious management policy should not be worried about the tightening regulations. However, they have to also homogenize around the emerging unanimity that data privacy laws are enacted to protect the privacy of individuals while facilitating data flows and innovation that are crucial to the digital economy.

Since most modern startups begin their journey in the cloud, compliance should be relatively unexacting whenever new legislations are enacted. These companies are most likely already using a secure content management system, or can quickly adopt one if they are not. And more often than not, despite that fact that it's not the main focus of the system administrators, it typically falls upon them to manage these 'secure content management systems'.

FileCloud enables data infrastructure modernization scenarios, thanks to its flexible cloud implementation, backup and disaster recovery support

Gartner magic quadrant report

FileCloud is deployable in a private cloud (FileCloud Server), a public cloud (FileCloud Online) and hybrid architectures. Organizations can choose to implement FileCloud on public cloud infrastructure, such as that of AWS and Microsoft Azure, or private data centers.

Gartner magic quadrant report

Understanding Data Privacy

Data privacy is a composite part of data security that specifically deals with the proper management of data – regulatory obligations, notice, and consent. More specifically, practical data privacy relates to how data is shared with third parties, how it's legally stored after collection, and any regulatory restrictions like CCPA, HIPAA, or GDPR.

Data remains one of the most valuable assets a company can have in their procession. With the rise of the digital economy, organizations find huge value in the collection, sharing and use of data. While data protection can exist without data privacy, you can't have data privacy without protection.

Guaranteeing data privacy basically means that you are not the menacing company greedily collecting all of your customer's personal information – whether passively or actively. According to a McAfee survey, more than 40 percent of people globally feel that they lack adequate control over their personal information. This is one of the major driving forces behind the establishment of regulations to enhance information privacy. And as data protection regulations grow globally, privacy requirements will also evolve and expand.

A Closer Look at Data Privacy and Protection Laws

Lawmakers have acknowledged the importance of establishing data privacy regulations and the need to hold organizations responsible for end-user data. Most data protection and privacy enactments are put in place to protect the personal information of the country's citizens. These laws typically govern the ability of individuals and entities to 'process' the data of other people, and they come into play whenever information is processed, collected, stored or communicated to or from the country.

Given the rising use of mobile devices for enterprise purposes, a Mexican national working in Canada whose data is stored by a cloud vendor in Brazil would likely set off specific privacy law provisions within all the three countries'. In order to avoid the infringement of these laws, businesses have to be able to track their employees' electronic cooperate data as it traverses borders.

The main focus of most data privacy laws is consent –for an employer to process an employee's personal data, the employer ('data user') must first obtain the employee's (data owner's) consent to do so. Accordingly, the business will have to know when and how you have to acquire consent from customer or employee data owners. Some data privacy laws include an exception from acquiring consent when collecting or processing personal data in relation to judicial proceedings for the purpose of meeting legal obligations.

New dimensions of the technology and business landscape are emanating, that will compound the issues involving securing personal information. Big data and its enormous datasets will present unique issues for management and controls. Transferring data internationally has become a staple occurrence and calls for new security measures in internet infrastructure and networks.

Tighter consent requirements are on the horizon, as individuals seek to have increased controls how their personal data is used. It falls on the organizations IT security teams – lead by sysadmins, to adopt a comprehensive compliance system that can conform with, and meet data privacy regulations.

What Exactly is Personal Data?

Successful businesses in a global digital economy heavily depend on analytics to derive actionable insights from data. Most of this data is personal information that relates to identifiable individuals. New technologies, business models and capabilities like big data analytics, Internet of Things (IoT), and artificial intelligence (AI) typically rely on massive volumes of personal data and hence have the potential to greatly impact people's privacy. As data becomes more valuable, organizations are finding it difficult to maneuver the increasingly complex regulatory landscape.

In a nutshell, personal data refers to any information that relates to an identified or an identifiable living person, whether directly or indirectly – in particular by reference to an identifier like an Id number, address, name, or more factors specific to the economic, mental, genetic, physiological, social or cultural identity of that individual. The definition of personal data should ideally be broad enough to encapsulate any information from which an individual can reasonably be identified.

Anonymized data is by definition, not personal data. Pseudonymized data from which a natural person can be potentially identified, for example, where the same company possesses a data set that allows for re-identification of the data, may be considered to be personal data. Personal information may also be inclusive of special categories of criminal offenses and conviction data.

Government regulation usually lags behind problems that have already materialized in a country's economy. Data privacy regulation for the private sector has developed in a different way. Given the expansive data protection regimes already passed in the EU and many other jurisdictions, the question of what types of data-related injuries people have to be protected against must be studied carefully, and some real-world answers have to be provided.

Acknowledging that real data privacy dangers exist doesn't cut it, organizations must endeavor to establish systems of 'digital governance' whose focus is the identification and prevention of harmful data practices.

Why Sys Admins Should Be Concerned

System administrators play a crucial role in developing and maintaining solid infrastructure in any IT environment, especially where security is concerned. Whether implementing policies, performing analysis on trends, actively working to prevent threats or engaging with SaaS vendors to make sure that they are not allowing any lapses in the security policy, it's the system admin that helps protect the integrity of the IT environment by facilitating close collaboration with security teams.

Data privacy regulations are typical technology-neutral or system independent. They typically contain broad terms that require system administrators to only apply the law but also interpret it. Despite being 'open to interpretation', regulations usually have clear data protection safeguards that have to be integrated into services and products, with privacy as a default option. From a security perspective, administrative or shared identities are typically the most powerful IDs on any since they are needed to access multiple security and system functions.

The sysadmin performs all the configurations for employee privileges and roles; they should, therefore, evaluate all their users and the assets they have access to. To mitigate any legal risks, system administrators have to embrace the strictest possible security, organizational, and technical measures.

Staying Ahead of the Curb

The rules that govern the use of personal data significantly vary – from technology to technology, from sector to sector, and from country to country. This may seem confusing to people who rightly expect the same protection regardless of who is collecting their data or how it's being processed.

Additionally, laws can quickly become outdated in a dynamic, rapidly changing digital ecosystem. In order to get ahead of regulations and reduce their impact on the organization, system administrators can conduct regular data audits, extensive security evaluation, use stronger passwords, adopt the right customer and employee data deletion mechanisms, and keeping technology and certifications up-to-date.

a) Extensive Security Evaluation

Prevention is, and will always be the most ideal approach to handling data breaches as opposed to fixing it. System administrators should leverage the tools at their disposal to detect and fix security vulnerabilities. Continuously monitoring your passwords and network vulnerabilities are crucial to achieving and maintaining regulatory compliance. By using penetration tests – ad-hoc tactics to try to exploit a system, on-premise, and cloud vulnerability scanners, system administrators can proactively identify vulnerabilities and acquire recommendations on how to enhance your general security position. Documenting discovered vulnerabilities and the measures taken to mitigate them will be useful in the event an organization is required to prove the existence of 'appropriate technical measures' to regulatory authorities. Given the rising number and frequency of cyberattacks in recent years, a proactive approach to data security makes more sense than ever.

b) Routine Data Audits

As a system admin, you should always have a solid grasp on where data is being stored and who has access to it. Auditing your data gives you a record of security-related system events, allowing for more targeted safeguards to secure it. A data audit will also help an organization determine if it's following external rules, laws, and regulations or internal guidelines like corporate controls, policies, procedures, and bylaws. There are several touchpoints that could cause a data breach. For example, poor data capture solutions, unrestrained access to data and lose documents can all contribute to increased risk. Taking the time to be thorough and perform data audits is crucial to understanding where your data protections lie and where they should be improved.

c) Keep the Technology Updated

The growth of technology is changing the world, are regulations are trying to keep up. Due to this, they are likely to become more stringent with time. Keeping up with software updates and patching existing software whenever vulnerabilities are detected is crucial to curbing data breaches. The NotPetya and WannaCry ransomware attacks are a good example of the serious implications of missing important patches since fixes were availed for both before the attacks occurred. Setting up an effective patch management solution helps to fully automate the patch-management life-cycle. Presently, even minor software bugs can cause major headaches so the importance of implementing a continuous patching schedule cannot be underestimated.

d) Establishing Suitable Data Deletion Policies

A hallmark of data privacy regulations is that organizations collecting and processing personal data are only allowed to retain it as long as there is a legitimate basis for doing so. Reducing the amount of data you store subsequently reduces the potential areas cybercriminals can attack and exploit.

Getting rid of old data provides your employees with a better sense of what information they require most and should use on a regular basis. In order to remain compliant with data privacy regulations, system administrators should not only protect the personal data stored in their systems but also ensure that the personal data is deleted in a secure manner once there is no permissible basis for retaining it.

A Break down of Regulations Per Country

Privacy laws have never been more important as they currently are, now that personal data traverses the globe via borderless networks. The General Data Protection Regulation (GDPR) was not the beginning and it certainly will not be the last. Stringent data privacy regulations are popping up in more and more economies across the world.

According to the United Nations Conference on Trade and Development (UNCTAD) 107 countries – 66 of which are transitioning or developing economies, have established some form of data privacy legislation.
While these protection laws are often good news for people who have their data stored, it does not bode the same to those who have to carefully navigate the complexities of inconsistent regulations.

System administrators at organizations that operate on a global scale have no choice but to adopt a cross-regulatory compliance strategy in order to keep up and adopt a wide range of regulations, typically with varying restrictions and requirements.

United States

There isn't a single overarching data privacy legislation in the US. Data privacy is not that highly regulated on a federal level. Instead, the country follows an industry approach to data privacy, depending on a patchwork of state laws and sector-specific laws, which results in a confusing set of rules and regulations that organizations have to navigate.

Some federal laws that touch on data privacy laws include the Health Insurance Portability and Accountability (HIPPA), which primarily handles health-related information, and the Children's Online Privacy Protection Rule (COPPA), that applies to organizations that collect data from children under the age of 13.

Some states have stricter laws than others. California for example, has 25 privacy-related laws, such as the California Online Privacy Protection Act (CalOPPA) and California Consumer Privacy Act (CCPA). Since the enactment of CCPA, lawmakers on both the federal and state level have introduced a flurry of similar data privacy proposals and bills. Whether or not any of these bills will eventually become law still remains to be seen, but momentum is certainly building

United Kingdom

Data privacy in the U.K is currently regulated by the Data Protection Act, which not only incorporates, but also supplements the provisions of the EU's GDPR. The DPA's rules are very concise and contain regulatory requirements around data security, and sharing data.

The Data Protection Act calls for fair processing of personal data, which basically means that organizations must have a transparent reason for collecting personal data and how they intend to utilize it.

The law also stipulates that if a website uses browser cookies, the owners have to clearly explain what they do, their eventual use, and gain the informed consent of users. Information rights in the public interest are upheld by the Information Commissioner's Office (ICO). Organizations that don't follow the rules established by DPA risk prosecution by ICO, where fines can reach up to £500,000 and even imprisonment.

India

India doesn't have any specific data privacy and protection legislation, It's data privacy laws are a composite of multiple acts and laws. The Information Technology Act contains provisions that stipulate that every business must have a privacy policy published on their site, whether or not they handle personally identifiable information.

The privacy policy has to describe the data they collect, it's intended purposes, the security practices used to keep it safe, and any third parties it might be disclosed to.

India currently has a draft bill for a new, comprehensive data protection law that has been heavily influenced by the EU's General Data Protection Regulation, the new bill will provide Indian data subjects with expansive data protection rights while imposing strict limitations on the collection and processing of sensitive personal data. The bill recent came under fire from the tech community since its data localization policy would require any company processing the personal data of an Indian national to store a copy of the data on Indian territory.

Canada

Canada has 28 federal, territorial or provincial statutes governing data protection and privacy. However, at a national level, the Personal Information Protection and Electronic Data Act (PIPEDA) regulates how business collect, store and use information regarding its users.

Under PIPEDA, like the GDPR in the EU – individuals have the right to access personal information held by a business, know who is responsible for collecting it, and the reason for its collection.

A crucial aspect of PIPEDA is the fact that it was tailored to ensure consistency in Canada's notification requirements with the country's trading partners, specifically the EU.

Australia

The key law that governs data privacy both in the private and public sectors in Australia is the Privacy Act 1988. The privacy act is based on 13 APPs (Australian Privacy Principles) which are legally binding principles that set the basic standard for privacy protection regarding sensitive, personal, or health information at the federal level.

The set out requirements about how organizations that are bound by the federal privacy laws may collect, utilize, store, and disclose these types of information. Like the rest of the globe, Australian privacy professionals, politicians and the public are actively engaging in debate about data protection and related laws.

The Federal government has announced a series of crucial amendments to the Privacy Act 1988 which will, among other things, drastically increase the penalties for serious or repeated breaches for all entities covered by the Act. The role of the Australian Competition and Consumer Commission (ACCC) in consumer data law developments has increased. In a preliminary report, the ACCC highlighted the need for organizations to have more transparent data handling practices, and recommended further regulatory reform to mandate this.

Brazil

Brazil's current data protection legislation is a patchwork of multiple individual codes, laws, and frameworks. The Brazilian Internet Act, which was passed in 2014, handles policies on the collection, maintenance, treatment and use of personal data on the internet. In August 2018, the General Data Privacy Law was signed off on.

Following closely on the heels of EU, this new legislation will contain 65 articles and bears several similarities to the GDPR. The law will be effected in early 2020. The LGPD creates a new legal framework for the use of personal data in Brazil, both offline and online, in the public and private sectors.

It's meant to replace or supplement sectoral regulatory frameworks that are sometimes marshy, conflictive, and without legal certainty. Like the GDPR, the LGPD guarantees several rights to its data subjects, while defining multiple lawful bases for processing sensitive personal data and the international transfer of data.

New Zealand

Data privacy in New Zealand is currently regulated by the Privacy Act of 1993, which outlines 12 information privacy principles. Organizations have to collect any non-public personal information directly from the individual, ensure that they are transparent about the intended use of the data, disclose any other parties who might have access to the data, and make sure the individual is fully aware of their rights, in regards to their own data.

The Act was established to tackle concerns associated with rising technological advancements and their potential to be used to access private information. The Privacy Commissioner is the main enforcer; they have the ability to issue codes of practice that modify the operation of the Act vis-à-vis specific industries, activities, agencies, or types of personal information. A Privacy Amendment Bill was recently introduced to New Zealand's parliament.

If passed, it will grant the Privacy Commissioner stronger powers, increase fines, introduce new offenses, and make reporting privacy breaches a mandatory requirement.

Finding Common Ground

The rise in data protection laws across the globe is a testament to the growing importance of data protection on the global agenda. Despite this, there is a lot more that has to be done. In an ideal world, all these laws would be harmonized across continents to ensure a more coherent and comprehensive global policy on the fundamental right to personal data protection, especially when it comes to the extraterritorial application of data.

This would significantly reduce the complexity which other nations can implement data protection requirements and reduce confusion and uncertainty when data protection issues arise between countries.

The GDPR is now arguably the world's strongest data protection regime in the world, leading it to be held up as the new global standard. However, it could be ambitious to assume that others will reach it any time soon, considering that several countries across the globe are yet to establish data protection laws or finalize existing draft legislation. The best way to guarantee compliance with almost any privacy law is to set up a transparent, detailed Privacy Policy and keep it updated.

About Us

FileCloud is used by 1000s of customers around the world including Global 2000 enterprises, government organizations, educational institutions, and managed service providers.

"We liked FileCloud's pricing, comprehensive feature set (branding, encryption) and the responsive support"

Stewart

A privately held software company, headquartered in Austin, Texas, USA. Our company offers two products – Tonido for consumers and FileCloud for businesses – used by millions of customers around the world, ranging from individuals to Global 2000 enterprises, educational institutions, and government organizations, and managed service providers.

To read more about how FileCloud can help keep your information secure as it is shared, visit www.getfilecloud.com