ManageEngine
ADSolutions

E-BOOK

Data privacy regulations and their impact:

An overview

Table of contents

Data is the key to successful digital transformation, and it has often been observed that companies that effectively handle and process data stand above the rest. With a data-driven approach, businesses gain the ability to deal with challenges in a more subjective and informed manner. Accurate data analysis can also change the business strategies from being merely reactive to being predictive. Over 2.5 quintillion bytes of data is generated everyday, and it is estimated that 90% of the world's data has been collected just in the last couple of years.

According to McKinsey Global Institute, data-driven organizations are 23 times more likely to acquire customers, 600% more likely to retain customers, and 19 times more likely to be profitable. Leveraging data efficiently enables organizations to make informed decisions and improve the customer experience. Eventually, this results in satisfied customers who keep coming back for more.

01 Rising privacy concerns across the world

For a long time, companies have been collecting data from their customers without their complete knowledge and consent. Since the true purpose of such data collection is kept hidden from consumers and tucked deep inside the terms and conditions, many consumers click the “agree to terms and conditions” check box without understanding its impact. They have handed over so much of their information to companies without even realizing it.

User data has a huge market value, resulting in companies pooling and selling the personal data of individuals on a large scale. Websites all over the world collect and store this data in many forms:

- Personal data, including an individual's name, gender, IP address, and location
- Engagement data, like text messages, emails, mobile apps, and social media pages
- Behavioral data, like purchase history and product usage information
- Behavioral data metrics, such as consumer satisfaction, purchase criteria, and product desirability

Global tech giants have been found to keep more information about users than what they require, and they often claim to use this data to personalize content and improve the user experience. But the fact is that these companies sell this data to advertisers, publishers, and other third parties.

For instance, ad performance with respect to a particular user is shared with advertisers, who then customize their ads based on the user's behavior to hyper-target them for conversion. Users' location information is also commonly shared and used to display personalized local ads. In response, 86% of Americans have made attempts to erase their digital footprints and secure their personal information that's available online because of privacy concerns.

Data refers to any information that could personally identify someone. Data privacy refers to protecting data in terms of data collection, use, and distribution.

The aim is to secure multiple types of data, like first-party data (information that brands and creators collect directly from their consumers), second-party data (information acquired from the company that collected it), and third-party data (information purchased from other sources, ideally including data from different sources aggregated in one place).

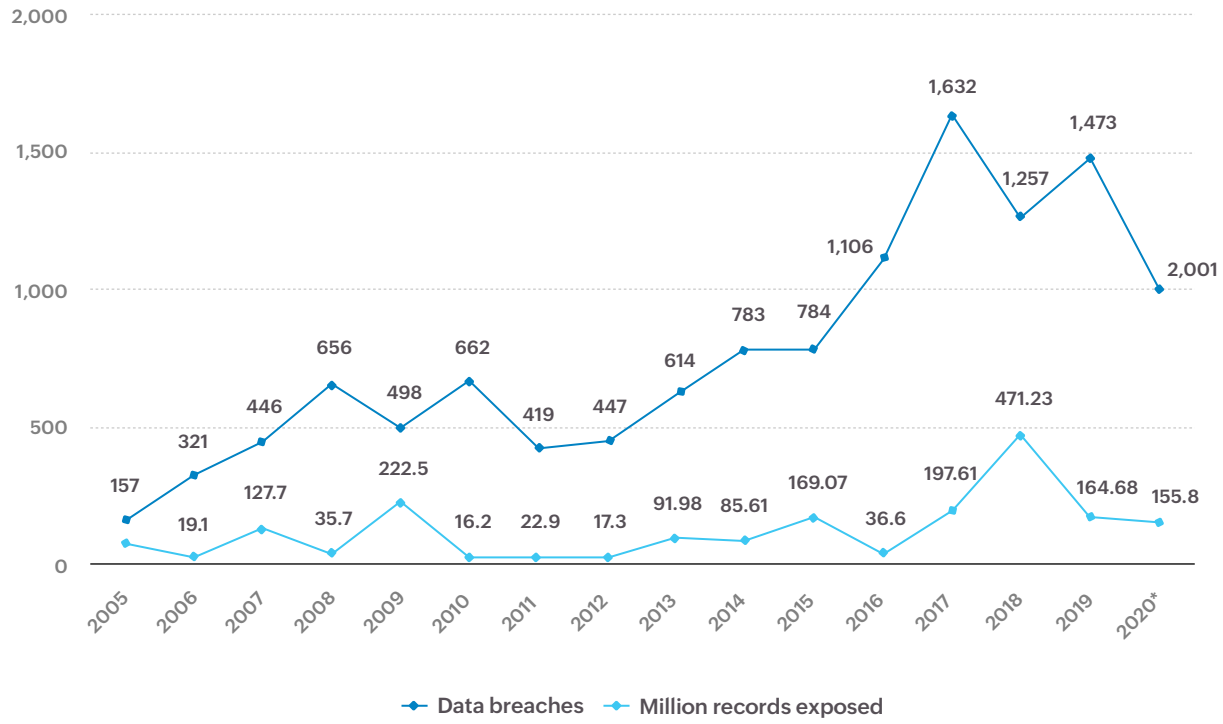
As consumers become more knowledgeable about their data rights and how their data is used, they will demand that it be secured. Seventy-nine percent of Americans have expressed concerns about the way their personal information is used by companies. With rising concern from the general population over the misuse of data, there is a need for global data regulations that focus on strengthening consumer privacy and data protection.

02 An urgent need for data privacy regulations

Over the last few years, data misuse has extended far beyond creepy advertisements that target individual customers. The increased focus on privacy concerns is driven by the numerous cybersecurity attacks that have led to massive breaches of personal data. Data breaches cost organizations time and money. This loss happens in the form of data loss, which can be compensated to some extent, and through irreversible damage to their reputation, which eventually leads to the loss of customers. Customer loyalty is almost impossible to regain.

The global rise in ransomware attacks is a major source of concern for businesses. According to the AICPA, almost half of Americans expect to fall victim to fraud over the next year. Statista estimates that the global average cost of a data breach in 2021 was $4.24 million, a steep 10% rise from 2020. With the most powerful economy in the world, the United States is the main target of cyberattacks and it has the highest average total cost of a data breach: $9.05 million in 2021.

Annual number of data breaches and exposed records in US (in millions)



The above chart tracks the number of data breaches and exposed records in the US from 2005 to 2020. These attacks serve as an urgent reminder of the necessity of global data privacy regulations. Such large-scale data breaches, resulting in the loss of sensitive information, money, and sometimes life, have impacted countries across the world.

Thus, governments are starting to regulate data collection and management by companies. With privacy being declared a fundamental right by the United Nations Universal Declaration of Human Rights, there is an immediate obligation to preserve privacy rights.

03 Data privacy regulations

In order to amp up data privacy and security measures, governments across the world have started passing laws to control the types of data that can be collected about users, how it can be used, and how it must be stored and protected. These regulations are designed to allow consumers to control their data.

One important mandate is to ask for consumers' consent each time their data is collected. The terms and conditions must also be easily understandable for consumers. These laws require companies to allow their users the right to access their data, take it and use it elsewhere, and request that businesses erase their personal data completely from their records.

Over 137 countries have implemented data privacy laws to prevent the misuse of personal data. Here are some of the major data privacy regulations from across the world:

GDPR

i. General Data Protection Regulation (GDPR)

Considered one of the most prominent privacy regulations, the GDPR was passed in 2018. It impacts all the organizations that process personal data and operate within, or sell goods to, the EU. As defined by the GDPR, processing data also covers the possible types of use and processes involved, like data collection, storage, retrieval, alteration, and destruction.

The GDPR also requires Data Protection Impact Assessments for any processing likely to risk the data subject's rights. In order to limit collection at the source itself, the GDPR emphasizes following data minimization, purpose limitation, and storage limitation. Violating the guidelines can result in fines of up to €20 million or up to 4% of the company's total global turnover from the preceding fiscal year, whichever is greater.

ii. California Consumer Privacy Act (CCPA)

The CCPA covers the residents of California and applies to businesses with a gross annual revenue of over $25 million; those that buy, receive, or sell the personal information of 50,000 or more residents, households, or devices; and those that derive 50% or more of their annual revenue from selling residents' personal information.

The CCPA requires businesses to put out a "notice at collection" message to inform consumers about the collection of their personal information and its purpose. It also has an entire section on regulating the functioning of data brokers. Violating the regulations can result in fines from $2,500 for an unintentional violation to $7,500 for an intentional violation.

iii. California Privacy Rights Act (CPRA)

Introduced in 2020 as a more comprehensive version of the CCPA, the CPRA aims to increase the rights of consumers in terms of data privacy and security. With a new category called sensitive personal information (SPI), the CPRA demands businesses provide additional protection based on the sensitivity of the personal information. It includes updated disclosure requirements, purpose limitation requirements, and opt-in and opt-out requirements.

In addition to expanding the laws in the CCPA, the CPRA introduces four new rights for consumers: the right to correct inaccurate personal information, the right to limit the use and disclosure of SPI, the right to access information about automated decision-making, and the right to opt out of automated decision-making technology. These new rights protect customers against data misuse by AI-driven technologies.

Other than these three regulations, there are several other laws concerning customers' right to privacy and the collection of data. The Health Insurance Portability and Accountability Act (HIPAA) governs the healthcare industry and prevents unlawful collection and sharing of patients' health information without their prior consent. The Gramm-Leach-Bliley Act (GLBA) applies to financial institutions to ensure the security and privacy of customers' financial information pertaining to their loans, financial statuses, transactions, and more.

The Payment Card Industry Data Security Standard (PCI DSS) ensures secure, lawful credit card transactions. The Fair Credit Reporting Act (FCRA) regulates the collection and use of individuals' credit information. To ensure children's safety, the Children's Online Privacy Protection Act (COPPA) governs the collection of information about minors.

04 The impact of data privacy regulations on businesses

Data privacy regulations enable businesses to optimize their data handling practices and ease cross-border digital transactions. But they require businesses to strengthen their data management technologies in order to build strong digital capabilities. The core idea is to create compliant, efficient business models that protect customers' data privacy.

There are two major changes businesses can expect as a result of data privacy regulations. First, privacy will become a fundamental expectation among customers. Second, transparency in privacy policies will no longer be optional. With consumers becoming more aware about data policies and with governments enforcing privacy requirements, companies are learning that implementing data privacy policies can create a business advantage by keeping them ahead of the curve.

On the other hand, from a business standpoint, the cost of compliance will shoot up since organizations might have to allocate separate staff and financial resources just to keep up with these regulations. With high noncompliance penalties and the potential risk of losing their brand value, organizations will be forced to pay to achieve compliance. The other impact on businesses is overregulation of policies. Customers become burdened by endless consent forms for every data process, taking away the ease of use of online platforms.

With the widespread implementation of regulations across the globe, businesses are at risk of noncompliance and increased investment. Many frameworks are being developed to help businesses find the right combination of optimal investment and compliance with regulations. Gartner's data security governance framework describes how businesses can meet legal requirements while dealing with consumer data.

The framework suggests the following steps:

- Identify and focus on data that is impacted by data privacy compliance regulations.
- Develop impact assessments for data protection and administer these periodically while keeping all business stakeholders involved.
- Configure technology controls to lower risk to an acceptable level.
- Review security policies systematically and whenever business risks change.

05 The relationship between data privacy regulations and IAM

Data privacy regulations have fundamentally changed the way businesses process consumers' personal information. Any information that pertains to an individual and can be used to identify them must be protected. The ultimate aim is to avoid the misuse of personal data by monitoring the collection of data and preventing data breaches. With the constant expansion of businesses, it is bound to become difficult to ensure compliance with all laws.

i. Staying compliant with data privacy regulations using IAM

IAM solutions provide businesses with highly reliable security features to help them meet the strict compliance requirements of privacy laws. With IAM, organizations can easily follow the stringent mandates and prevent unlawful processing when handling customers' private data. A centralized IAM solution provides security measures like MFA, PAM, and organization-based access policies. Through these, businesses can ensure only authorized users access sensitive data.

Additionally, features like role-based authentication and least privilege methods strengthen internal access within the company. Federated authentication features aid in providing and revoking access, a feature that comes in handy during onboarding of new employees and temporary workers. The advanced encryption options and threat protection measures provided by IAM solutions can be deployed to safeguard data stored on-premises and in the cloud.

As data privacy laws are renewed to cover cloud-centric operations, such features will keep businesses on track with minimal disruption to operations. IAM solutions are also designed to combat multiple types of cyberattacks, like phishing, malware, viruses, and DDoS attacks. Thus, businesses with IAM solutions deployed to manage and run their security processes will be able to successfully stay compliant with data privacy laws.

ii. The impact of data privacy regulations on the evolution of IAM solutions

With the introduction of stringent data privacy regulations, IAM solutions need to evolve to match their requirements. One of the reasons why data privacy laws are relevant to the ethical development of IAM solutions is because factors like user credentials are based on users' personal information, such as fingerprints, geographic locations, and personal device features.

If an organization chooses to adopt an IAM solution, it is of absolute necessity that it ensure compliance with all data privacy laws right from the development stage. While features like MFA and PAM provide security at the user level, the protocols running them from the back end must also use advanced algorithms and encryption techniques to remain secure. All the processes and applications should be kept patched and up-to-date.

iii. What an IAM solution must have to stay compliant

As IAM solutions are developed and updated, they must keep in line with the applicable data privacy laws to remain compliant. Here are a few points business should consider to create legally sustainable IAM solutions:

Ensure data privacy and security compliance from the beginning of the development stage and re-evaluate throughout the product's lifetime.

In terms of the collection and management of customers' personal data, collect only what is needed and keep it only as long as is necessary. Secure storage and secure disposal of data are equally important. Ensure such sensitive data can only be accessed by those who need to do so.

Avoid storing sensitive data as much as possible. As an alternative, collect such data only when needed.

Keep a close eye on ML- and AI-driven security solutions and data mining tools. Prevent unauthorized access by reducing permissions and limiting access to resources.

06 Managing changes brought about by data privacy regulations

The common misconception about data privacy regulations is that they only impact the legal department. But the point often missed is that everyone who works with data in a company must be aware of the regulations and stay compliant. Many experts studying these regulations propose that this has less to do with data management and more to do with change management processes. Businesses need to rethink and restructure the way they handle customer data. The best way to implement these privacy regulations into a business is to implement change management.

Investing in analytics and automation technologies should be any company's first step towards building a robust, compliant system that ensures adherence to all privacy regulations. Most data privacy laws mention the customers' access rights, which essentially means that a customer can at any time ask for a copy of all the data that is being gathered on them, or for their data to be deleted.

Businesses will need digital, automated solutions to comply with these requests efficiently. For example, forms that autofill necessary details, desktop guidance tools, or virtual assistants will make the process faster with minimal manual effort. This will in turn reduce the possibility of mishandling data.

The following are some practices organizations should follow to efficiently manage the changes brought by regulations:

- To ensure compliance with all applicable data laws, organizations must have up-to-date knowledge of them. Employing legal counsel for this purpose will provide accountability and allow a rigorous process to be put in place.

- Constantly auditing and assessing the controls of the company is essential to building a system that can withstand complex changes in privacy regulations.

- Every organization is unique, and thus there is no one solution that can be applied to all. It is essential for a business to understand the nature of the data it handles and its duties before trying to seek a solution. What works for a company in one industry may not work for one in another.

- Another important factor that needs to be considered is the location of customers. Each country or jurisdiction has specific local laws, and it is mandatory to comply with those as well.

- Companies must ensure that these privacy regulations are added to their core values. With such a cultural change established, privacy will be considered right from the beginning of each new project and followed through until the end.

- Companies should move away from the traditional data collection approach wherein they try to gather and store as much customer data as possible. With regulations tightening, companies should gather, handle, and store only what is required. The idea of minimalistic data collection must be employed. Also, deletion of data after its expiration or after using it is equally important to complying with privacy regulations.

- Organizations need to be transparent regarding the personal data collected from their customers and manage requests for data deletion in order to ensure legal compliance.

The ever-evolving global data privacy laws will only become more stringent with time. The ideal step for any business to take would be to voluntarily comply with all the privacy laws in the locations where their businesses operate. Additionally, countries and states affected indirectly by their businesses must also be taken into consideration as regulations like the GDPR require. In order to avoid expensive fines, operational interruptions, and the loss of customers, the sooner businesses plan and comply with these laws, the more successful they will be.

About AD360

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console.

For more information about AD360, please visit
https://www.manageengine.com/active-directory-360/

$ Get Quote Download