IDERA® | SQL Server Whitepaper

HOW TO HANDLE THE COMPLEXITIES OF REGULATORY COMPLIANCE

CONTENTS

PREFACE	3
WHY IS DATA PRIVACY IMPORTANT?	4
REGULATORY AGENCIES TAKE ACTION	4
PROTECTING PRIVATE DATA	5
RESPONDING WITH REGULATORY COMPLIANCE MANAGEMENT	6
THE COST OF NON-COMPLIANCE	7
COMPLEX REGULATORY COMPLIANCE DEMANDS SOPHISTICATED TOOLS	8

PREFACE

The reliance on digitally stored information continues to grow and now dominates society in the 21st Century. The use of the Internet for business and information exchange shows no signs of slowing down or returning to the good old days of cash transactions handled through physical contact. Social media has become an intrinsic part of the lives of many individuals which is evident by the panic that sets in when a smartphone is misplaced or runs out of power unexpectedly.

On one level, the unparalleled convenience afforded by e-commerce and electronic communication is very attractive to a majority of the population. But from the beginning of the digital age, there have been concerns that revolve around the privacy of personal and sensitive information. The apprehension over how society's collected data is used has spawned governmental regulations that purport to protect the rights of individuals to control access over their personal and sensitive information. Businesses need to comply with these regulations.

WHY IS DATA PRIVACY IMPORTANT?

An incredible amount of digital information is generated every day, with an estimated 1.7 MB of data being created every second for every person on earth. Not all of this data can be directly linked to individuals, but much of it can be used by corporations to create user profiles that can be used to predict purchasing habits or future online activities. In other cases, healthcare facilities and financial institutions retain personal and sensitive information that can have disastrous consequences when used unscrupulously.

There are different degrees of inappropriate use of personal information. It can be done by the organizations that collected the data or by other groups taking advantage of inadequate protective measures used in its storage. Unwelcome advertising and spam are at one end of the spectrum and, while annoying, do not present serious risks to the individual whose data is being used. More consequential and long-term damage can be caused by data breaches that make personal information available to hackers.

News organizations regularly report on data breaches whose number continues to grow annually. In the first half of 2019, over four billion records had been compromised due to problems in the way personal data was inadequately protected in the United States. The affected organizations range from large banks to smaller companies that perform collections for healthcare providers. A constant in all cases is that millions of pieces of personally identifying data are potentially in the hands of criminal entities that can cause irreparable harm to the affected individuals.

REGULATORY AGENCIES TAKE ACTION

The intrusions into personal privacy ushered in by the digital age have not gone unnoticed by the affected citizens. As the population vocalized their concerns, regulations began to be crafted to address how personal data is collected and used. The European Union (EU) issued its first data protection directive in 1995. It broadly defined personal data and laid out guidelines for processing it within the EU. The rules were strengthened in 2012 as a precursor to the extensive set of regulations introduced in 2018 with the adoption of the current General Data Protection Regulations (GDPR).

The regulations enforced by the GDPR impact any entity that collects data from EU citizens. It was designed to eliminate the complexities of complying with standards developed by individual nations within the union. It is an extensive document that defines personal data and the ways in which individuals can exert control over how it is used. The GDPR directly addresses the issues of electronic commerce and data collection by holding any processor of data collected from EU citizens subject to the directive regardless of the physical location in which the information is processed. Thus, any company conducting business in the EU needs to comply with the GDPR.

There is no question that the EU's directive is currently the most comprehensive set of data privacy regulations in the world. In the United States there are no comparable overriding standards in place. While many federal and state guidelines cover some of the same ground, it would be difficult to implement a similar policy in the U.S. Clashes between federalists and states' rights proponents make passing national legislation a difficult undertaking. There are some calls by industry leaders for a U.S. equivalent to the GDPR, but they appear to be a long way from fruition at this time.

Many other nations around the world have instituted their own data privacy laws. In some cases, such as in Brazil, the guidelines closely follow the example of the GDPR and pertain to the nation as a whole. Other countries, like Australia, follow the U.S. model of data privacy and protection with a mix of federal, state, and territorial laws. The differences in other types of international laws illustrate the difficulty in getting concurrence from the world's diverse nations. It would appear that there will not be a global privacy directive anytime soon.

PROTECTING PRIVATE DATA

Data subject to privacy laws is collected and used by organizations in many ways. This presents obstacles to keeping it safe and out of the reach of unauthorized users. Here are the key principles that an enterprise needs to consider when protecting private data.

- Understand the personal and sensitive information that is contained in its systems. This is a necessary first step toward keeping it protected. For example, a knowledge of which databases store personal information may inform the way in which those systems need to be secured.
- Restrict the collection and retention of data to what is required for business purposes. There may be no valid reason to obtain certain personal information on customers when conducting business.
- Protect the information that is collected and stored. This involves a wide variety of strategies and tactics that run the gamut from encrypting data when it is in transit and at rest to enforcing strict password standards. It includes keeping networks secure from unauthorized intrusion and training employees on the correct data handling procedures.
- Dispose of data properly when it is no longer needed. Keeping sensitive data around after its shelf-life has been exceeded poses unnecessary risks that can easily be avoided. Use robust data deletion techniques that fully eradicate information from databases and storage media.
- Create a response plan for data security incidents. In the unfortunate event that sensitive information is compromised, having a plan in place to minimize the effects can prove priceless. This includes notifying the affected parties and regulatory bodies fully and promptly concerning the extent of the data breach.

RESPONDING WITH REGULATORY COMPLIANCE MANAGEMENT

The Internet and e-commerce have removed many of the barriers that historically limited international trade with individual citizens of foreign countries. Now, anyone with an Internet connection can interact with companies and organizations located anywhere in the world. Conversely, this means that businesses need to be cognizant of the regulations that are in effect in all of the countries in which their customers are located. Due to the diversity of competing privacy standards, this can prove to be extremely challenging.

Organizations operating in these locales may be subject to varying constraints regarding how the personal data of the population can be collected and used. In some cases, modifications to corporate policies may need to be made on a country by country or even state by state basis to maintain compliance with these varying guidelines. Failure to follow this strategy exposes a company to penalties from each sector in which it has done business.

Here are some measures that companies can take to minimize their chance of failing to comply with privacy regulations.

- Keep updated on regulatory changes in all markets. This includes monitoring blogs and regulatory websites that provide information regarding any new initiatives or modifications that are being made to current compliance standards.
- Conduct regular data audits to determine where sensitive data is being stored as well as how it is being used and who has access to it. In a dynamic IT environment, these issues can change rapidly and demand the timely execution of appropriate actions to maintain data protection and regulatory compliance.
- Remove unnecessary customer and employee data from systems as soon as possible. Performing this task can be quite complex, as outdated sensitive information can be resident in backups as well as operational systems. Retaining unneeded personal information is an avoidable disaster waiting to happen.
- Ensure that all systems are updated and patched. Running obsolete software or neglecting security patches is a dangerous game that organizations should strive to avoid. Data breaches that are shown to have been caused by lax system maintenance procedures will end up being much more expensive than addressing the problem with more robust internal processes.

Some of these activities may necessitate developing new teams or reallocating human resources. The costs associated with remaining compliant may seem prohibitive to some organizations, but pale compared to the price of ignoring the regulations in effect.

THE COST OF NON-COMPLIANCE

Non-compliance with modern privacy regulations carries with it substantial penalties levied against the offending entities. The GDPR specifies that the most egregious failures to protect personal data can cost an organization 20 million euros or 4% of their previous year's turnover, whichever is higher. Less severe failures can be penalized at reduced levels that can still cause major negative impacts to the affected companies. To date, over $125 million in fines have been imposed on companies, with hundreds of millions more expected in the near future.

Non-compliance with GDPR standards can be revealed through investigations by data protection authorities, investigative journalism, or concerned employees or customers who bring protective lapses to the attention of governing bodies. Though there is no organization equivalent to the EU's Information Commissioner's Office which oversees compliance and determines fines, failing to comply with any locality's regulations can result in large monetary fines and commensurate loss of consumer confidence.

In the United States, the decentralized regulatory landscape results in fines being initiated from various sources. One of the strongest US laws is California's Consumer Privacy Act (CCPA) which went into effect on January 1, 2020. It is similar to the GDPR but does not go as far as the EU's directive. Its focus is on larger companies that do business in the state and includes explicit opt-out language that returns some control over data use to consumers. Offended companies will be liable for $7,500 per violation and $750 for each affected user. Basing the fines on the number of users impacted by a data breach can make non-compliance very expensive.

In addition to the financial penalties that directly impact non-compliant organizations, there are lasting public relations ramifications to running afoul of privacy regulations. The publicity surrounding a data breach can result in lost customers and limits the ability of an enterprise to attract new ones. These effects may dwarf the monetary penalties and offer another compelling reason to be vigilant regarding compliance.

COMPLEX REGULATORY COMPLIANCE

As the world's data privacy and protection standards evolve, so too will the methods businesses need to employ to remain compliant with them. Staying abreast of new regulatory developments may require full-time staff for companies that have customers in multiple regulatory jurisdictions. An internal audit team may be required to vigilantly test systems to determine their compliance as conditions change within the computing environment. New procedures will need to be developed to dispose of unnecessary sensitive data and fully protect the personal data required for continued business operations.

Employing the right software tools and human resources are critical components of a strategy designed to ensure regulatory compliance. Monitoring applications that alert an organization to unauthorized attempts to access sensitive data are essential when forming a first line of defense against data breaches. They can be the difference between a widespread loss of personal data or a swift response that nips the attack in its early stages before the information is compromised.

Historical records that indicate compliance are indispensable when confronted with consumer complaints or investigations initiated by regulatory agencies. They can be obtained through the audits conducted within an enterprise that demonstrate activities meant to implement compliance and changes made to address findings resulting from those examinations.

There are many moving parts involved in keeping an organization compliant with privacy regulations. While it may be seen by some as a burden, regulatory compliance management is an inescapable part of doing business in the digital age. Ignoring the demands for data privacy will not make them go away, but threatens organizations with onerous financial penalties and the prospect of losing their customers to more enlightened and prepared companies. It's time for enterprises to do whatever is necessary to deal with this complex reality.

IDERA'S SOLUTION

SQL Compliance Manager

Monitor, audit, and alert on user activity and data changes in SQL Server databases.

Simplify your SQL Server audits. SQL Compliance Manager is a comprehensive auditing solution that monitors and tracks changes to SQL Server objects and data, and sends alerts on suspicious activity. Obtain detailed visibility to determine who did "what", "when", "where", and "how", whether the event is initiated by privileged users or hackers. SQL Compliance Manager also helps ensure compliance with industry regulatory and data security requirements. SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of all data access, selects, updates, schema modifications and permission changes to SQL Server databases.

Start a free, fully-functional, 14-day trial today!

Start for FREE