Aligning GDPR Requirements with Today's Hybrid Cloud Realities

7 Requirements for Compliance

DATASTAX

CONTENTS

EXECUTIVE SUMMARY

The enactment of the European Union's General Data Protection Regulation (GDPR) represents a significant milestone for virtually every international business. Under the standard, organizations will need to comply with an extensive set of requirements—or potentially face significant fines for failing to do so. This paper examines the regulation's security standards, and it then looks at the capabilities security teams need to address GDPR across their IT environments, which continue to grow increasingly hybrid in nature, encompassing both on-premises and multiple cloud services.

INTRODUCTION: ALIGNING GDPR WITH EVOLVING ENVIRONMENTS

Since it was formally adopted by the European Parliament and the Council of the European Union in 2016, the GDPR has had a massive impact on firms globally. The regulation applies to any organization that processes the personal data of EU citizens—regardless of where the organization is headquartered. This in effect means that the GDPR has emerged as a standard that virtually every international organization must adhere to.

While much has been written about the fines associated with non-compliance, which can run as high as four percent of a company's annual revenues, the costs for compliance are also looking to be quite steep. The International Association of Privacy Professionals estimates that Fortune's Global 500 companies will spend roughly $7.8 billion on GDPR compliance. Another study showed that Fortune 500 companies expect to pay an average of $1 million on technology alone to become compliant.

As IT and security teams set out to align their security and data governance practices with GDPR, they must institute these changes in an IT ecosystem that is also seeing fundamental change. One of the most important changes is associated with the increasingly diverse nature of computing models employed, and the reality that many organizations are now running a hybrid mix of legacy on-premises systems, private clouds, public clouds and more.

The following sections offer a look at the GDPR's requirements pertaining to data security, and they examine the key capabilities that are paramount in enabling GDPR compliance in hybrid environments.

OVERVIEW OF GDPR SECURITY REQUIREMENTS

Much of the GDPR is dedicated to detailing requirements around data security practices. Following are a few examples of the specific requirements.

Article 5: Principles Relating to Processing of Personal Data

This article includes the requirement that personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')." Establishing a strong, resilient and auditable security framework that addresses these requirements will represent a foundational component of GDPR compliance.

Article 17: Right to Erasure (Right to be Forgotten)

Article 17 outlines circumstances in which citizens can require that data controllers erase their personal data, cease further dissemination and potentially halt third-party processing of their data. To comply, organizations will need to take proper steps to ensure the permanent deletion of personal data when requested.

Article 25: Data Protection by Design and Default

This article establishes requirements around the safeguards that are employed. It explains that controls must be put in place to ensure that organizations only use the data that is required for a given process. It also mandates that safeguards must be aligned with risk. Addressing these requirements will necessitate three key groupings of controls:

- Assessment. This includes the evaluation of processes, profiles and risks.
- Preventative measures. Controls such as encryption and fine-grained access control will be important in aligning safeguards and risks and addressing the requirement that, "by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Detective. Organizations will need to be able to demonstrate compliance, which will require capabilities for auditing, activity monitoring, alerting and reporting.

Article 32: Security of Processing

This portion of the standard is focused on ensuring processors "implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk." One of the key mechanisms outlined for addressing this requirement is through the "pseudonymisation and encryption of personal data." Organizations also need to institute a "process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing." And controls need to be employed that safeguard against the "unauthorised disclosure of, or access to, personal data."

Article 33 and 34: Breach Notification

In the event of a breach of personal data, article 33 mandates that organizations must notify the supervisory authority within 72 hours of discovering the breach. Article 34 specifies that data subjects must also be notified of breaches. Article 34 also states that organizations are exempted from this notification requirement if they have implemented appropriate protection measures that "render the personal data unintelligible to any person who is not authorised to access it, such as encryption."

ADDRESSING GDPR REQUIREMENTS: KEY CAPABILITIES

For years, organizations have been compelled to comply with a range of regional and industry mandates, which have served to shape security investments and strategies. The GDPR standard represents an example of how these standards continue to get more stringent and comprehensive in scope.

In many organizations, the reality is that compliance initiatives have represented a mad scramble to check the required boxes before a rapidly impending deadline. Given the extensive, far-reaching nature of the GDPR standard, security teams will be well served by approaching the regulation in a holistic fashion, and going beyond tactical checklists to ensure the investments and initiatives undertaken ultimately serve to strengthen the organization's security. It is important to institute GDPR controls in the context of holistic, strong security framework, one that helps ensure that personal data as well as other corporate data assets are secured. This strategy will be particularly critical moving forward, particularly as organization's IT environments continue to grow increasingly complex, interrelated and dynamic.

Toward that end, security teams should look to employ a layered, defense-in-depth approach, incorporating complementary, synergistic controls that help ensure that a single vulnerability, error or breach doesn't jeopardize the availability and security of sensitive data and systems. Another key strategy will be to adopt a "privacy by design" philosophy. This will entail factoring data protection in at the outset of the design of new products and systems, rather than trying to tack security mechanisms onto these systems after the item is complete.

As organizations set out to establish compliance with GDPR and align strong security policies across their modern hybrid cloud and big data implementations, they'll need a key set of capabilities. The following sections offer an overview of the elements required.

Internal and External Authentication

To address GDPR requirements and security best practices, security teams need to establish strong controls around who can access sensitive data. This will require strong authentication mechanisms that can be used not only for employees, but third-party contractors, partners and customers. For optimal flexibility and efficiency, authentication platforms should support integration with a range of protocols, including Active Directory, Kerberos and Lightweight Directory Access Protocol (LDAP). The systems used for managing authentication should deliver a robust set of controls, including capabilities for segregating administrative duties.

At the same time, these strong authentication mechanisms need to be aligned with the objective of delivering a positive and rewarding user experience. Consequently, pursuing initiatives aimed at identity federation and single sign-on will be increasingly essential. Further, these capabilities need to offer unified support of both traditional on-premises environments as well as private and public cloud environments.

Fine-grained Access Control

Within many areas of the GDPR standard, requirements are detailed that underscore the need to restrict access to sensitive data, so that the only people that can access or modify it are those that have a legitimate need to do so. Addressing these requirements requires the ability to establish granular access controls, and to apply these controls uniformly across multiple clouds and data centers. Within database tables, this includes the need to apply policies down to individual rows of data. In addition, within multi-tenant environments, such as public cloud implementations, strong, persistent controls need to be applied to specific data sets, restricting access of both users and administrators.

Encryption for Data in Transit and at Rest

Strong, granular and flexible encryption capabilities are a key requirement for preventing unauthorized access to private data. By encrypting specific data sets, organizations can ensure that no matter where the encrypted data may be transported or copied, it will remain consistently safeguarded by established policies.

Within larger enterprises, there will typically need to be a mix of encryption mechanisms employed in order to most effectively address the organization's mix of risks, technologies and environments. A typical security team may now need tools that encrypt data at the application, database and storage level. In addition, tokenization may be another technology that is employed to minimize the potential for unauthorized data access. Where possible, encryption should be implemented in a way that doesn't require changes at the application level.

Strong Key Management

As the reliance upon encryption continues to grow, so does the need for robust key management. To establish the highest levels of security, keys should be stored in hardened, tamper-resistant appliances that have been certified to be compliant with such standards as FIPS and Common Criteria.

In addition, it's critical to establish key management capabilities that are aligned with on premises and hybrid, multi-cloud environments. For example, key management capabilities should work across such public clouds as Amazon Web Services, Microsoft Azure and Google Cloud. Security teams should look to employ platforms that enable them to bring their own keys to a range of cloud services, including infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) environments.

In today's modern environments, it's vital to ensure that the mechanisms employed support data mobility. Toward that end, rather than using vendor-proprietary encryption and key management, organizations should leverage third-party tools that enable the migration of data across multiple clouds, without requiring the decryption of data. This can yield a number of advantages, including accelerating workload migrations and eliminating unnecessary CPU costs associated with decryption and encryption, not to mention helping ensure data remains safe during migration.

Auditing and Central Visibility Across Disparate Environments

GDPR requirements will place increased emphasis on visibility, auditability and accountability. Within this context, application-level auditing will represent an important requirement. With this capability, security teams can establish a full audit trail for all activity within the application, including all updating, selection and deletion of private data.

Security auditing will also be essential in tracking all sensitive administrative activities, including encryption/decryption requests, key rotation and so on. It will also be a growing imperative for organizations to establish a more unified view of all user data. This requires a single, connected and contextual view of the customer across disparate environments as well as visibility into all customer interactions through all channels and touch points.

Simplified Data Deletion

Within many organizations, the ability to delete sensitive data, permanently and with certainty, when no longer needed has presented challenges—and those challenges are set to be compounded significantly as operations teams seek to comply with customers' right-to-be-forgotten requests under the GDPR. To address these challenges, it will be vital to gain capabilities for efficiently controlling and scheduling removal of information. In addition, central key management can be another asset in this area. By establishing central control over cryptographic keys, organizations can retain central control over encrypted data. In response to a right to be forgotten request, an organization that has implemented granular encryption mechanisms could delete the key or keys used to encrypt the records associated with a given customer, and so ensure that data could never be decrypted.

Within data management environments, look for capabilities that support "time to live" management for specific records. These capabilities make it easier to manage deletion of data on a scheduled basis. These capabilities should be highly granular in nature, for example enabling policies to be applied to specific columns in a database.

Data Autonomy and Sovereignty

GDPR makes clear that the organizations that collect personal data are responsible for that data. These responsibilities apply as data is migrated across borders. Specifically, article 56 explains that supervisory authorities are responsible for overseeing controllers' cross-border processing of personal data.

GDPR will therefore place an increased emphasis on data sovereignty and autonomy. Within data management environments, it will be important to establish controls at the keyspace and schema level that specify which data centers data should be replicated to. This is particularly critical in hybrid, multi-cloud environments, helping ensure data isn't transported to locations it shouldn't be.

These capabilities can help support data residency policies across multiple cloud and data center locations, ensuring each customer's data can be stored in the geographic locations consistent with existing compliance requirements. For example, when running multiple cloud services across country borders, teams need capabilities for ensuring that data for German citizens is only held in data centers in Germany.

SAMPLE USE CASE: MULTINATIONAL FINANCIAL SERVICES COMPANY

Challenge

With the GDPR taking effect soon, the security and IT operations teams at an international financial services firm were under significant pressure. In order to address GDPR right-to-be-forgotten requirements, they needed to broaden and strengthen their visibility and controls around many of the disparate repositories that held customer data, including both on-premises and cloud environments. At the same time, the company was competing in a financial services market being disrupted by technology upstarts and well-financed incumbents. Therefore, it was vital that any security mechanisms employed didn't compromise internal operations or the customer experience.

Solution

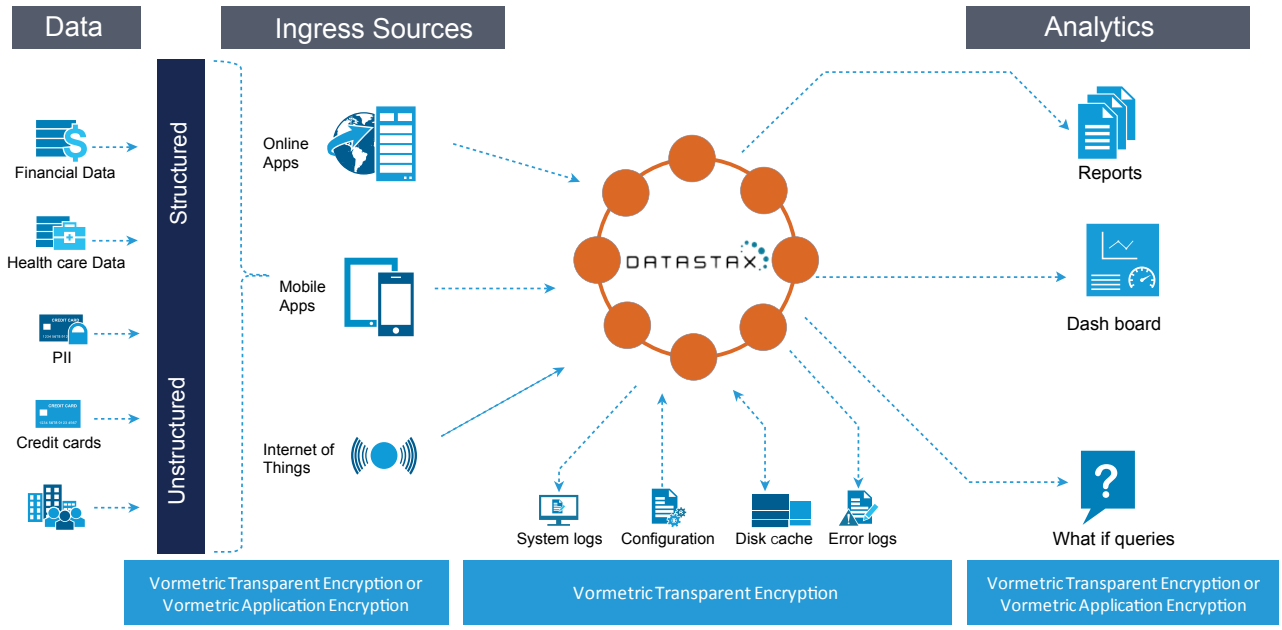
The company's IT operations team implemented a new data model that offered integrated data ingestion and analytics. With this model, operations and business staff were able to gain a unified view of customers from across hybrid cloud environments. The security team also embarked on an initiative to expand their use of encryption. To efficiently support these expanded encryption implementations, the team deployed a key management platform that enabled them to centrally manage keys for all the encryption technologies that they were running.

Benefit

The security team at the financial services institution was able to strengthen the safeguards around its customer data and it gained the controls needed to efficiently comply with customers' right-to-be-forgotten requests. Further, with their unified data model, security teams were able to provide insights that enabled more effective fraud detection. Ultimately, while security was strengthened, they were also better able to support the innovations that helped improve the company's ability to deliver compelling, customer-centric services.

HOW DATASTAX AND THALES ESECURITY CAN HELP

DataStax and Thales eSecurity deliver an advanced set of complementary solutions. Together, these offerings deliver all the required capabilities that organizations need to effectively and efficiently establish the safeguards and controls mandated by the GDPR. These solutions secure data at rest and in transit, and they deliver granular, auditable controls. By leveraging these combined offerings, organizations can establish enhanced security, visibility and control of personal data, including throughout their data centers and across hybrid, multi-cloud environments.



DataStax Enterprise

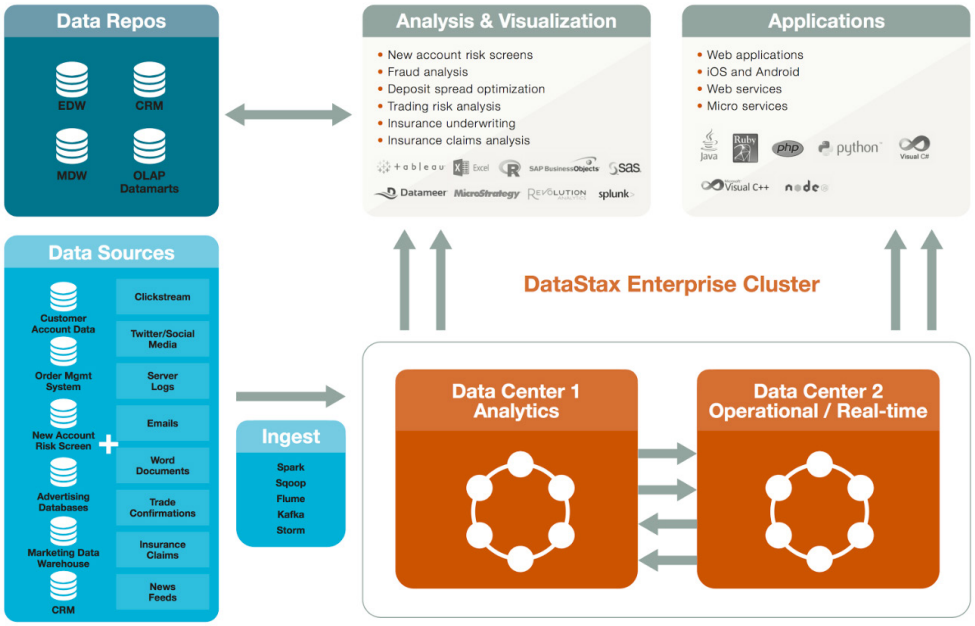
DataStax Enterprise (DSE) is an always-on, distributed cloud database that is designed for hybrid cloud environments. With its leading capabilities, DSE provides the data platform to address GDPR requirements, while achieving the business' customer experience objectives.

Granular Access Controls Enable Strong Security Around Personal Data

DSE includes advanced security functionality to control who has access to data as well as security technologies like encryption to secure that data against unauthorized access. DSE also includes a range of audit and logging features to make it easier to put together a full audit trail around customer data sets. With DSE, organizations can establish access controls at the row level. With these capabilities, security teams can enforce granular controls, even in multi-tenant environments. The DSE platform enables you to leverage your existing Active Directory, Kerberos and LDAP directories, so you can federate identities and enable single sign-on to all the enterprise's data domains.

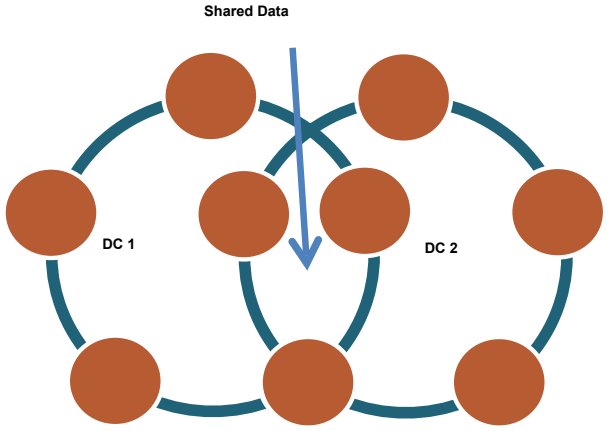
Unified Visibility Fuels Powerful Insights and Efficient Control

DSE delivers unified and contextual views of customer records from across multiple applications, offering capabilities known as Customer 360. Customer 360 is powered by DSE Graph, an optional add-on to DSE that provides entity resolution capabilities and real-time analytics. With DSE Graph, organizations can harness powerful customer insights, and address right-to-be-forgotten requests with optimal efficiency. In addition, organizations can gain vital insights that fuel enhanced services and security. For example, DSE Graph makes it easy for controllers to link data that is seemingly unrelated to find patterns that indicate fraudulent or malicious activities.



Keyspace and Schema Level Controls Address Data Sovereignty Requirements

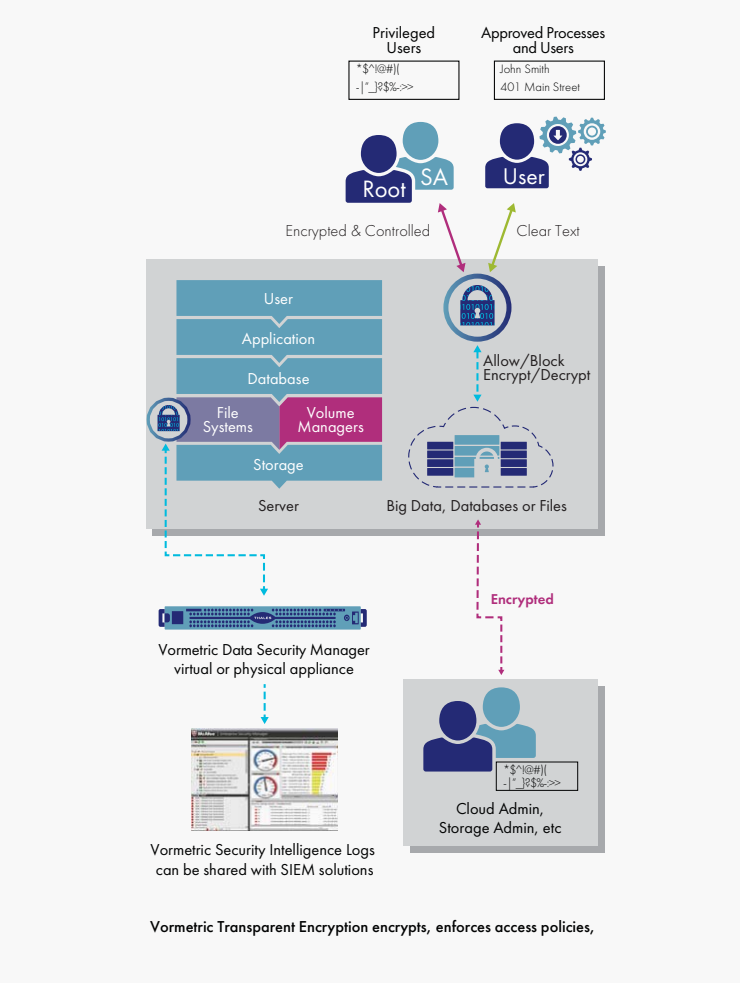
With DSE, organizations can institute controls at the keyspace and schema level to determine which data centers data can be replicated to. As a result, security teams can ensure that regulated data isn't copied to locations it shouldn't be, making it efficient to address GDPR and regional data sovereignty requirements.



Thales eSecurity

Thales eSecurity solutions enhance the enterprise-class security features found in the distributed database technology from DataStax. Thales eSecurity offers the Vormetric Data Security Platform, a solution that delivers robust data-at-rest protection, including transparent encryption, application layer encryption, enhanced access controls, key management and security intelligence.

With the Vormetric Data Security Platform, security teams can institute data-at-rest encryption that delivers additional layers of security in DataStax environments. With the solution, security teams can employ strong controls around sensitive data in big data and hybrid cloud environments. Teams can enforce security policies at the file system level and within data stores at the field or column level. Vormetric Data Security Platform can secure sensitive data throughout DSE environments, including data stores, system logs and configurations.



CONCLUSION

While safeguarding the personal data entrusted to them has always been important for organizations, the GDPR is creating an added sense of urgency in this arena. For many organizations, complying with this regulation will require significant enhancements in how personal data is managed and secured. With DataStax and Thales eSecurity, organizations can leverage complementary solutions that enable stronger, more efficient control over personal data. At the same time, these solutions leave companies better equipped to achieve their customer experience and business objectives.

ABOUT DATASTAX

DataStax powers the Right-Now Enterprise with the always-on, distributed cloud database built on Apache Cassandra™ and designed for hybrid cloud. The foundation for real-time applications at massive scale, our flagship product, DataStax Enterprise, makes it possible for companies to exceed expectations through consumer and enterprise applications that provide responsive and meaningful engagement to each customer wherever they go. Our product also gives businesses full data autonomy, allowing them to retain control and strategic ownership of their most valuable asset in a hybrid cloud world. DataStax helps more than 400 of the world's leading brands like Capital One, Cisco, Comcast, eBay, McDonald's, Microsoft, Safeway, Sony, UBS, and Walmart transform their businesses through right-now applications focused on enterprise optimization and customer experience. For more information, visit DataStax.com and follow us on @DataStax.

DataStax is a registered trademark of DataStax, Inc. and its subsidiaries in the United States and/or other countries. Apache Cassandra is a trademark of the Apache Software Foundation or its subsidiaries in Canada, the United States, and/or other countries.

ABOUT THALES ESECURITY

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment—on- premises, in the cloud, in data centers or big data environments—without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives—digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance—through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Aligning GDPR Requirements with Today's Hybrid Cloud Realities

7 Requirements for Compliance