



COMPLYING WITH GDPR

FOR BUSINESS IMPROVEMENT



INTRODUCTION

The General Data Protection Regulation (GDPR) of the European Union (EU) came into effect from May 2018 onwards. The GDPR emphasizes protecting the privacy and security of personal data, assigning accountability to data processors and controllers, and ensuring the rights of individuals. To achieve GDPR compliance, organizations are strengthening their security infrastructure and aligning their processes to protect the consumer data from attacks and breaches. Leading technology vendors are offering advanced security solutions to support these organizations to solidify their security infrastructure and meet the GDPR requirements.

FileFlex Enterprise™ uses decentralized cloud or edge cloud technology that leverages the storage and CPU power of edge devices to allow users to access, share, stream, and collaborate data from source locations without using a traditional centralized cloud repository. This inherently supports and augments an organization's GDPR compliance endeavors.

This paper covers key aspects of the GDPR, its impact on business environment, and technologies/solutions useful for achieving the GDPR compliance.

EVOLUTION AND APPLICABILITY OF GDPR

The GDPR became a law in the EU in May 2016 and effective from May 2018 onwards, after a 2-year preparatory time frame. The GDPR has replaced the Data Protection Directive that was in place since 1995. The EU mandates each of its member states to deploy the EU directives in their national laws, which resulted in uneven privacy laws across the EU in the past. Over the last few years, there have been increasing incidents of privacy breaches and information thefts. The fast pace of technology development is also posing new and diverse security risks. The recently implemented the GDPR is designed to address these issues and establish a uniform regulatory framework across the EU.

APART FROM EUROPEAN ENTERPRISES, THE GDPR IS APPLICABLE TO THE FOLLOWING ORGANIZATIONS:

- Enterprises present outside the EU but selling products/services in the EU
- Enterprises monitoring the behavior of individuals in the EU
- Enterprises storing, transferring, or processing data of EU citizens

LEVERAGING GDPR FOR BUSINESSES

While the GDPR is a necessity for the organizations listed above, achieving the GDPR compliance can prove to be a significant facilitator to improve processes. Some of the key benefits are given below:

- **Improved Data Organization and Mapping:** Infrastructure to ensure consumer rights, and stronger data controls and simpler consumer opt-out processes would drive enterprises to have a comprehensive data map and better data tracking. It, in turn, would offer well-organized, clean, and relevant data to organizations.
- **Enhanced Customer Targeting:** Enriched data quality would enable organizations to get better clarity about their customers and improve customer analysis. It would result in enhanced customer communication and targeted messaging, aligned with core customers. Hence, organizations can improve their Return on Investment (ROI) for marketing and communication investments.
- **Superior Customer Experience:** Improved quality of customer data would enable organizations to capture a 360° view of customers. Therefore, enterprises can design services and solutions to deliver a personalized and enriched customer experience.
- **Improved Efficiency and Innovation Focus:** Improved data quality and data organization would be instrumental in minimizing non-value-added process components, leading to higher efficiency. A better understanding of customers would also empower organizations to adopt the latest technologies and foster an innovative culture.

- **Enhanced Risk Mitigation:** Complying with the GDPR leads to stronger data management/protection practices, leading to a solid data protection infrastructure and ultimately a robust risk mitigation infrastructure. Improved data organization and quality is also helpful in enhancing the risk mitigation capabilities of organizations.

KEY ASPECTS OF GDPR

While there have been regulations across the EU to ensure data protection, the GDPR brings new priorities and focus areas, which are common for all EU countries. The key aspects of the GDPR include:

- **Focus on Personal Data:** The GDPR has a strong focus on protecting personal data. Although the GDPR has broadly defined personal data, it has still left room to expand the definition of personal data further in the future. The GDPR protects the privacy of the following data types:
 - Primary identity information (name, address, ID numbers, etc.)
 - Web data (IP address, cookie data, RFID tags, location, etc.)
 - Biometric, health, and genetic information
 - Racial/ethnic data, political opinions, and sexual orientation
- **Rights of Individuals:** The GDPR puts a greater emphasis on enabling individuals with more rights to manage their data. Some of the key rights given to individuals include Right to be Informed, Right of Access, Right to Rectification, Right to Erasure, Right to Restrict Processing, Right to Object, etc. Right to be Informed and Right to Erasure are of prime importance.
 - **Right to be Informed:** The GDPR ensures that individuals understand who is collecting their information, what type of information is being collected, and why it is being collected. Hence, it improves the clarity of individuals about the data collection process.
 - **Right to Erasure:** It empowers individuals to request deletion of their data when they offer appropriate reasons for erasing their information. Businesses are required to delete the requested information within a month of receiving the request.
- **Data Protection Impact Assessment:** Businesses are required to conduct continuous data protection impact assessment to mitigate risks posed to the rights of individuals covered under the GDPR. Controllers are obliged to report any breach of personal data to the Data Protection Supervisory Authority within 72 hours of a data breach.
- **Role of Data Protection Officers:** Enterprises are required to appoint a Data Protection Officer (DPO) to enable them to comply with the GDPR. DPOs would help both processors and controllers in continuously monitoring processes to meet the GDPR requirements.
- **Shared Responsibility of Data Protection:** Unlike the Data Protection Act 1998, the GDPR has made sure that both controllers and processors share the burden of data protection and implement security measures. In case of a data breach, both controllers and processors can be held responsible and penalized. Regular audits of data processors would help significantly improve risk mitigation capabilities.

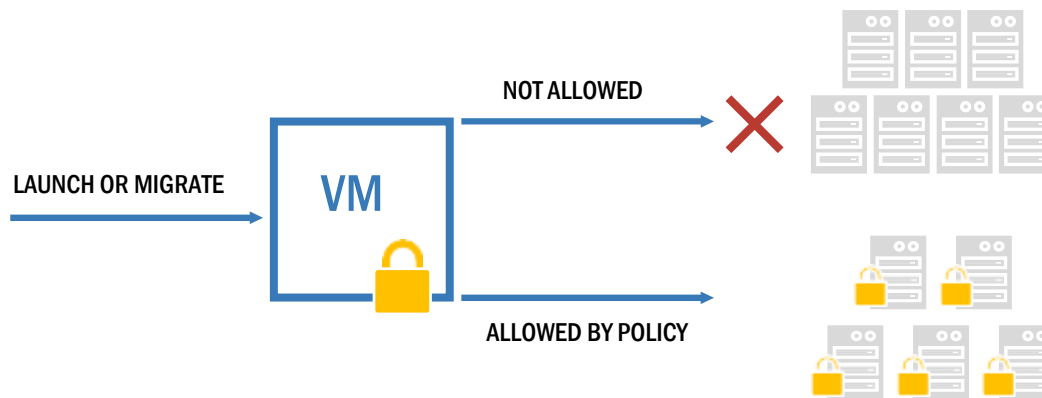
A few examples of processors supporting controllers for storing and processing data include:

- Software-as-a-service providers
- Cloud service providers
- TPV offering account and payroll services, billing services, analytic services, etc.

GETTING READY FOR GDPR COMPLIANCE

To meet the GDPR compliance, security architects need to design controls to ensure that the information is secure within their organizations and that information is not transferred to locations/organizations lacking sufficient security controls. Some of the key security technologies useful for stronger security controls are given below:

- **Policy-driven Workload Distribution:** As shown in the diagram below, the policy-driven workload distribution is useful to ensure strong control to protect and manage private information across private, virtual, and cloud environments. This technique is helpful to prevent unauthorized transfer of data. The security policy is applied to each workload to strengthen security and improve visibility.




- **Ubiquitous Encryption:** Encryption is considered one of the strongest security mechanisms to protect information critical for businesses. Recently developed techniques, such as AES encryption, are especially useful to protect data when the information is transferred from an IT environment to a CSP environment. Innovative encryption solutions result in the enhanced key generation and matrix manipulation, offering stronger protection. Strong encryption solutions reduce application performance issues caused by side-channel attacks, and protect data at rest, in use, and in motion.
- **Micro-segmentation:** Micro-segmentation helps design secure zones to isolate workloads from each other and offer a high level of granular security. It helps customize security to manage different types of data traffic. Micro-segmentation supports the deployment of a centralized network segment policy.
- **Pseudonymization:** This technique reduces the risks posed to personal data by replacing the identifier fields with coded identifiers/tokens. Pseudonyms combined with appropriate identity and access management controls ensure robust protection of business-critical information, especially in case of hybrid clouds. This technique is useful to protect the data already available without obtaining explicit permissions from users while ensuring complete data security.

ROLE OF QNEXT ON GDPR

Qnext® has developed FileFlex Enterprise™, which is a hybrid point-to-point, software-only service based on the edge technology. FileFlex supports and augments an organization's GDPR compliance activities, such as data control and discovery, data minimization, usage monitoring, integrity, and confidentiality and accountability. Key capabilities of FileFlex Enterprise towards GDPR compliance are given below:

- **Developed around Intel® Software Guard Extension (Intel SGX):** FileFlex has the option to use Intel® SGX technology at the endpoint. Intel SGX helps security architects protect personal data in use. It is designed to strengthen the security by executing the chosen code and data in the protected selective memory areas. These selective areas are separated cryptographically from the remaining operating environments, ensuring strong data security.

- 
- A decorative header image featuring a network diagram with nodes and lines, and the acronym 'GDPR' prominently displayed in a stylized font on the right side.
- **All requirements of GDPR:** FileFlex supports and augments all compliance of the GDPR, such as
 - **Data transfer and control** – FileFlex provides granular authentication controls over the data and enables organizations to control their unstructured data copies. It also provides secure authentication permission during data sharing.
 - **Controlling data duplication** – FileFlex controls the storage limit of personal data based on requirements of users while making it easier to manage where data resides within the organization.
 - **Data accuracy** – By controlling data duplication, FileFlex enables organizations to keep fewer copies of the same data, thus providing more accurate and up-to-date data, mandated by the GDPR.
 - **Support confidentiality and integrity of data** – FileFlex provides privacy of data by using technologies such as active directory, LDAP integration, and enforcement of file share permissions.
 - **Data accountability** – FileFlex supports data accountability by using the logging integration technology while integrating with LDAP.
 - **Security incidents notifications** – By using detailed auditing and integration with enterprise SIEM technology, FileFlex provides faster response for security incidents.

WAY FORWARD

To comply with the GDPR, organizations need to ensure that the information they possess/process is accurate, updated, and relevant. Processes should be established to make sure that the information is lawfully processed only for intended purposes. To strengthen their security infrastructure, organizations can explore various solutions based on advanced encryption, micro-segmentation, and pseudonymization. Qnext being one of the technology innovators can empower organizations to strengthen their controls across environments to protect data in diverse states. Organizations can leverage Qnext's FileFlex offering to support and augment their GDPR requirements. Now, organizations can share important and confidential information/file anywhere in the world with no loss of quality or security. With the FileFlex Enterprise, organizations that follow stringent data protection and cloud regulations such as the GDPR can realize all the benefits without the risks. They have full control over and knowledge about the whereabouts of their data all times. If their customers request deletion or access, then there is no concern with where it may be in the cloud.

While the GDPR compliance is a necessity, it can act as a catalyst for improving internal data management and protection processes, leading to improved customer experience, targeted messaging, and better risk management. We believe the GDPR can prove to be a blessing in disguise for many organizations, and Qnext can be your partner in this journey to comply with the GDPR and realize its benefits.

ABOUT MARKETSSANDMARKETS™

MarketsandMarkets™ is the world's largest revenue impact company, serving over 7500 customers. 80% of top 2000 companies globally rely on us for identifying new high growth and niche revenue opportunities.

In the face of constant technology innovation and market disruption, we help organizations plan and operationalize their future revenue mix decisions by identifying over 30,000 high growth opportunities ranging from \$1B to \$500B across 90+ industry trends and markets. Organizations choose MarketsandMarkets™ to stay ahead of the curve and accelerate their revenue decisions and implementations by 6 – 12 months, giving them a unique, first-mover advantage.

Our revenue impact methodology provides quantified and actionable insights on converged, granular and connected market eco-systems that result from disruptive technologies and high-growth markets. We provide an extended lens on not only what will impact our client's revenue but also what will impact their clients' revenues, continually uncovering latent opportunities.

We work across all major B2B industries with C-level executives in functions such as Strategy, Marketing, Sales, R&D, Product, and M&A. MarketsandMarkets™ brings exclusive high-growth markets intelligence generated by over 850 SMEs and analysts along with its proprietary Revenue Impact platform (Knowledge Store).

For more information, please visit: www.marketsandmarkets.com

Intel®, Intel Data Guard and Intel vPro are trademarks belonging to Intel Corporation. FileFlex, FileFlex Enterprise and Qnext Corp are trademarks of Qnext Corp.