White Paper

IBM Cloud Secure Virtualization: **Your Key to Simplifying GDPR**

Introduction

Time is running out for firms to comply with the European Union's General Data Protection Regulation (GDPR), Europe's most significant update to data privacy regulation in decades. Any company that handles the personal data of European citizens or residents and that is not in compliance by May 25, 2018, could face lawsuits or stiff penalties, including massive fines.

Achieving full GDPR compliance could take anywhere from a few months to a year, depending on your organization's size, the complexity of its data flows, and current privacy maturity level. With a compliance deadline right around the corner, organizations need to get started today, if they have not already.

GDPR: What it means to you

The GDPR replaces the 20-year-old European Directive 95/4/EU, and is intended to strengthen and unify data protection and data privacy for individuals within the European Union. Because the GDPR is a regulation and not a directive, GDPR is directly applicable throughout the EU. When it goes into effect, it will apply to all EU member states as a single law. However, GDPR has various opening clauses that leave room for member state interpretation and implementation, in particular with regard to employment. EU member states can choose to extend the law, but are not entitled to water down its protections. Many member states have demonstrated they will take advantage of the latitude they are afforded by GDPR. Several have already drafted related bills but so far, Germany has been the only member state which formally adopted such a law .

The GDPR isn't just any regulation. It's a regulation with teeth by means of enforcement. Controllers [2] or processors [3] found in violation of GDPR could be fined up to 20M euros or 4% of their worldwide revenue—whichever is greater. Amongst its many requirements is a stringent 72-hour breach notification time if the breach is likely to result in a risk to the rights and freedoms of natural persons, and it allows individuals in the EU to challenge companies to prove data privacy and security of their "personal data". Notably, the term "personally identifiable information (PII)", as it is commonly used in the United States, refers to a relatively narrow range of data such as name, address, birth date, social security number or credit card numbers. However "personal data", in the context of GDPR, covers a much wider range of information that can include social media posts, photographs, lifestyle preferences and transaction histories and even IP addresses [4].

This paper takes a close look at the GDPR requirements and how HyTrust, Intel®, and IBM, in partnership as IBM Cloud Secure Virtualization, can simplify your compliance efforts.

[1] https://www.bvdnet.de/wp-content/uploads/2017/08/BMI_%C3%9Cbersetzung_DSAnpUG-EU_mit_BDSG-neu.pdf

[2] 'Controller' is defined as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data..." (Regulation (EU)2016/679, Article 4, Definitions).

[3] 'Processor' is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." (Regulation (EU) 2016/679, Article 4, Definitions)

[4] 'Personal Data' is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier[...]" (Regulation (EU)2016/679, Article 4, Definitions). PII inter alia includes name, address, telephone number, date of birth, email address, NI/ social security number, banking information, and credit card information. In other words, all PII is personal data but not all personal data is PII.

White Paper

Achieving GDPR compliance can be a significant endeavor wrought with challenges. Organizations that are compliant with the Payment Card Industry Data Security Standard (PCI-DSS), NIST 800-53, or ISO 27001 are on the right path to adherence. However they must still address protection, auditing and reporting with regard to personal data, as well as data storage, and user rights. There's no single solution that will do it all, but organizations can simplify their efforts by choosing compliance solutions that address multiple GDPR requirements.

HyTrust, Intel & IBM Cloud: A Single Solution for Simplifying GDPR Compliance

The GDPR codifies both the concepts of privacy by design and privacy by default. Article 25 depicts the concept of considering privacy risks when designing a new system or business process to help ensure that privacy is "built into" the system or business process from the beginning and on a consistent basis. Considerations for reducing privacy risks include transforming personal data into non-personal data through technical means such as psuedonymization, anonymization and encryption. There are also requirements to retain personal data only for the time period needed for defined business or legal purposes.

HyTrust workload security solutions reduce risk by automating compliance and enforcing security-based policies across private and public clouds. As an integral part of IBM Cloud Secure Virtualization, HyTrust helps remove the security and compliance barriers that often prevent companies from accelerating their cloud adoption.

IBM Cloud Secure Virtualization utilizes infrastructure automation jointly developed by IBM and VMware, and services automation developed by IBM, to deploy and integrate the Intel and HyTrust technologies with the VMware unified software defined data center platform on IBM Cloud bare metal servers. IBM is the first global cloud provider to automate the deployment and integration of Intel® Xeon® processor-based servers with Intel® Trusted Execution Technology (Intel® TXT) and HyTrust CloudControl and DataControl software with VMware Cloud Foundation. VMware Cloud Foundation is a complete cloud offering of compute, network and storage and includes ESXi, vSAN, NSX and vSphere.

Intel developed Intel Trusted Execution Technology (Intel TXT) and Intel®AES NI some years ago to create a root of trust and accelerated encryption capability. What HyTrust and IBM have achieved by enabling them, is to create the value that is described in this document and take security to the lowest level in the cloud infrastructure. Thus, this provides a deeper security capability that is far superior to most other offerings in the Cloud Services market and helps to meet the GDPR's privacy by design and privacy by default requirements.

Let's take a closer look at some of the challenges introduced by GDPR and how IBM Cloud Secure Virtualization can help address them.

HyTrust in Action

GDPR legislation is focused on data security, consent, legitimate use, and other aspects of data protection. It has major significance with stricter, more specific obligations for both data controllers and data processors. While the legislators have avoided identifying specific controls, they clearly mandate that both controllers and processors "implement appropriate technical and organizational measures" (Article 32). This means that state-of-the-art, best practice industry standards shall be applied and be reviewed regularly to meet the security requirements. Many of HyTrust's solutions are already designed to simplify and automate such practices.

Challenge: Data Mapping

Although data inventory and data mapping is not explicitly mentioned in GDPR, it is widely acknowledged that Article 30 of GDPR requires a company to create a data inventory and do a data mapping exercise. Under GDPR, organizations are no longer required to notify and register their processing activities with local data protection authorities but rather are required to maintain a record of all their organization's processing activities internally, and to make them available to supervisory authorities upon request.

White Paper

A critical first step in the GDPR readiness journey is to establish a complete, accurate picture of where personal data resides (Data Mapping). Controllers (and, if applicable, also, processors) have to comply with various new privacy requirements under GDPR, and Data Mapping can help to do so. Those requirements include:

- Maintaining detailed records of your company's data processing activities; and being able to present these records to supervisory authorities on request (Article 30 GDPR);
- Being able to demonstrate that your company's processing activities are performed in compliance with GDPR (Article 5(2) GDPR, Accountability); and
- Implementing data protection by design and by default (Article 25 GDPR).

Data Mapping also helps your company to assess the risks of your data processing activities with regard to the rights and freedoms of individuals. In a nutshell, this is the only way to ensure that all personal data is secured. However, given the complexity of today's IT ecosystems, this is not a simple task. To establish visibility, organizations need to assess:

- Who has access to the data
- How access and other activities will be tracked and assigned to specific individuals
- The different locations and environments in which data resides
- The different data types that must be secure
- Where data is transmitted

An organization must have complete answers to these questions in order to claim they adhere to sound practices and have established a solid foundational for GDPR. For example: Article 30, Records of Processing Activities.

HyTrust CloudAdvisor enables organizations to search, discover, and visualize the personal data in their environment. Data visibility capabilities allow admins to create a forensic trail to meet data compliance, retention, regulatory, and recovery objectives. Organizations can discover where data resides, understand its composition, and know who is using it and how. CloudAdvisor also protects VMs with threat detection and incident response capabilities. This helps companies meet their obligations with regard to data minimization (only collecting data that is needed for a stated purpose), storage limitation (only keeping that data for as long as required for a stated purpose) (Article 5(I) GDPR), data breach notification (Articles 33, 34 GDPR), data breach handling, and other conditions establishing lawfulness of processing (Article 6 GDPR).

Challenge: Controlling Access to Personal Data and Systems

Article 5 of the GDPR specifies that "personal data must be processed in a manner that ensures appropriate security of the personal data, including preventing unauthorized access to use of personal data and the equipment used for the processing." Article 32 of the GDPR provides further details on how to secure processing. Once you know where personal data is stored, then you must restrict access to only those who have a legitimate reason to process or use it. Strong authentication and access control management solutions are vital to ensure that personal data access is controlled and minimized. This problem is most challenging when it comes to controlling the access of privileged individuals. In particular the vAdmins (virtualization administrators) that normally have broad authority over the management of the virtual infrastructure that is the backbone of the data center.

HyTrust CloudControl helps organizations manage the complexity of authentication and access to workloads by vAdmins. These include two-factor authentication, advanced role- and object-based access controls, secondary approvals (two-person rule), audit quality logging, and hypervisor configuration hardening. These key capabilities allow organizations to mitigate the risks associated with the accidental or intentional misuse of privileged user access and compromised credentials.

White Paper

Challenge: Protecting Personal Data from Data Breaches

Encryption and key management are increasingly seen as a security imperative, and GDPR will only serve to firmly establish that fact. Encryption and key management represent an essential means of establishing data confidentially and integrity (Article 32). Furthermore, Article 34(3) of the GDPR states that "communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it."

Encryption and key management therefore play vital roles in complying with GDPR, as they can eliminate the need for breach notification. If a breach occurs when data is encrypted and keys are protected, a cyber attacker will very likely be unable to decrypt the data and access the information. Just as critical as encryption is the proper management of the encryption keys. They have become a principal virtual asset and are a critical requirement of any encryption implementation. Quite simply, if the keys are vulnerable to loss or compromise, the security benefits of encryption are negated, and the organization can be exposed to the loss of sensitive and valuable data.

HyTrust DataControl's data encryption and integrated key management capabilities address a number of GDPR Articles (5, 6, 24, 25, 28, and 32) by encrypting data at rest and rendering it illegible. HyTrust DataControl encrypts entire virtual workloads, including the operating system, applications, and data, using block-level technology. Workloads and their data are secure throughout their lifecycle – from their deployment, operation, and migration, until their sanctioned decommissioning. HyTrust DataControl also authorizes workloads to start only under approved conditions and within sanctioned locations. Before running or accessing data, workloads are automatically compelled to check with HyTrust DataControl's policy engine on when and where decryption of the workload is allowed. HyTrust DataControl integrates with HyTrust CloudControl to leverage Intel TXT to provide proof of a host's security state. This enables administrators to set a policy and determine what to do if a workload is moved onto a host that doesn't have the required level of security or is outside the desired geographic region.

In these ways, HyTrust DataControl helps you to comply with GDPR's requirements concerning lawful processing, privacy by design and by default and to meet the general principles relating to data processing as controller and processer, including technical security obligations. See GDPR Articles 5, 6, 24, 25, 28, and 32.

Challenge: Data Sovereignty

Under GDPR, organizations must consider the geographic requirements of their data processing operations (see Article 44), and under what conditions they should run workloads in private, public, or hybrid cloud environments. Even when leveraging a data center of a cloud service provider, its physical location must be taken into account. Understanding, monitoring, and controlling where data resides will be core to maintaining GDPR compliance. IBM has 16 fully operational cloud data centers across Europe, representing the largest and most comprehensive European cloud data center network. IBM operates 55 cloud data centers in 19 countries across 6 continents, ensuring that their clients' data is kept in the EU and no preconditions for third-country transfers have to be met.

Article 44, General Principle for Transfers, states that data transferred outside the European Union remains subject to the law of the EU not only for their transfer, but also for any processing and subsequent transfer. A transfer can only take place to third countries and international organizations if in compliance with this rule by the controller or processor. Additionally, Articles 45 et seq. set forth that an adequate level of data protection must be guaranteed for data transfers outside the EU (e.g. by EU Model Clauses, Privacy Shield, Binding Corporate Rules or an adequacy decision by the Commission). By providing workload placement and location-aware decryption capabilities, HyTrust BoundaryControl, along with Intel TXT, can help organizations meet the technical conditions implied by these requirements. .

White Paper

HyTrust BoundaryControl is effective for data sovereignty as well as protection against VM theft. It enables admins to set policies so that workloads can only run on proven, trusted hosts that are physically located within defined parameters. The foundation for BoundaryControl is rooted in Intel TXT and provides processor level-attestation of the hardware, BIOS and hypervisor, allowing sensitive workloads to run on a trusted platform. Leveraging Intel TXT hardware, BoundaryControl enables you to assign labels that bind a workload to a predefined location, enabling you to create rules like, "German VMs can only run on hosts located in Germany." Encryption policies can also be applied to ensure data on virtual disks can never be decrypted on hosts outside of Germany, for example.

Conclusion

Within a matter of months, companies must have the people, policies, and technologies in place to comply with GDPR's 99 Articles and also with the member states' local related laws. To reduce the risk of noncompliance, organizations should choose technology solutions that help them address multiple articles easily and efficiently. IBM Secure Virtualization, an integrated solution developed in partnership by HyTrust, IBM and Intel, helps simplify and expedite GDPR compliance.

In addition to expediting their GDPR compliance efforts, organizations that leverage IBM Cloud Secure Virtualization can reduce the operational overhead imposed by the regulation. Infrastructure and services automation help improve productivity and efficiency, while addressing security concerns that previously prevented organizations from taking advantage of the agility, efficiency and scalability of the cloud.

With IBM Secure Virtualization, you always know where your data is and can thus better address and meet the following obligations:

- **Review Lawfulness of Processing** – Collection and use of personal data is only lawful under the six defined conditions of Article 6 GDPR
- **Governance and Accountability** – Maintain documentation of the implementation of technical and organizational measures required by GDPR, such as policies, procedures, staff training, and internal audits
- **Determine whether special data is affected and implement compliant processes** – Protect data of children, and other sensitive data
- **Handle Individual Rights** – Control data access, data rectification, data erasure, data portability, and restrict processing
- **Breach Notification** – Identify affected PII and data subjects
- **Cross-Border Data Transfer or Access** – Maintain restrictions on the transfer or access of personal data outside the EU not amplified by cloud use as servers are located in EU

To learn more about IBM Cloud Secure Virtualization visit www.ibm.com/cloud/secure-virtualization or www.hytrust.com.

HyTrust
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
1-844-681-8100 (US) | 1-650-681-8100 (Intl.)

HyTrust, IBM and Intel are separate companies and each is responsible for its own products and services. Neither HyTrust, IBM nor Intel makes any warranties, express or implied, concerning the others' products or services