virtustream

Whitepaper

Virtustream and the General Data Protection Regulation (GDPR)

This document is purely for general guidance purposes and does not constitute legal advice or legal analysis.

This white paper is an informative piece about the GDPR and describes what the regulation encompasses, what types of data the GDPR affects, how it will affect organizations, and what Virtustream, a Dell Technologies business, is doing to help customers meet GDPR compliance.

Executive Summary:

The European Union (EU) General Data Protection Regulation (GDPR) is a new regulation ([EU] 2016/679) intended to strengthen and unify data privacy rights for EU data subjects.

Virtustream closely partners with Dell's Global Privacy Office to protect the privacy of its customers located around the world. Dell's global privacy program is focused on ensuring the proper use and disclosure of our customers' personal data, as well as fostering a culture that values privacy through awareness. Virtustream cloud services and software complies with the GDPR as of the effective date, May 25, 2018.

Virtustream also provides services and software to assist customers with their GDPR obligations, such as Data Security and Incident Management and the Accountability Principle, supporting customers' goals to manage risk and privacy more effectively and efficiently.

The European Union (EU) General Data Protection Regulation (GDPR) is a new regulation ([EU] 2016/679) intended to strengthen and unify data privacy rights for European Union data subjects. Virtustream cloud services and software complies with the GDPR as of the effective date, May 25, 2018.

What is the GDPR?

The EU GDPR ([EU] 2016/679) replaces the EU Data Protection Directive (95/46/EC), and includes much of what was in the former Directive, but with many new requirements and a broader application than existing EU privacy laws.

The GDPR is a big shake-up for data protection:

- Internationally enforced
- 99 articles, 400+ provisions
- Unlike a Directive, Regulations are binding on all nations
- Applies to any data related to EU citizens
- Fines up to 4% of annual worldwide revenue

According to Article 1 of the GDPR, one of the main objectives of this regulation is to protect the fundamental rights and freedoms of EU data subjects, in particular their right to the protection of personal data.[1] In 2016, the GDPR was approved and adopted by the EU Parliament, with the regulation planned to take effect after a two-year transition period. Unlike a Directive, it does not require any enabling legislation to be passed by government; meaning it will be enforced starting May 2018.

The GDPR addresses requirements for how personal data is stored, updated, accessed, transferred, and deleted by data controllers – those who determine how and what data gets processed – and data processors – those who

[1] Intersoft Consulting, "Art. 1 GDPR Subject-matter and objectives" accessed May 10, 2018. https://gdpr-info.eu/art-1-gdpr/

provide services to actually process the data. To obtain further detail about what the GDPR entails, organizations can review a summary of the legislation.

Who is Affected by the GDPR?

The GDPR applies to any organization (whether a controller or a processor) that controls and/or processes personal data of EU data subjects (people whose personal data is processed by a controller or processor), regardless of whether the processing actually takes place in the EU or not. This applies to organizations located within and outside of the EU, if they offer goods or services to, or monitor the behavior (i.e. social media, online tracking, data analytics) of EU data subjects.

For example, if an EU-based company is collecting personal data from EU data subjects, then they would fall under the GDPR. Additionally, if a US-based company, which does its data processing in the US, is processing personal data from EU data subjects, they would also fall under the GDPR due to the global reach of the regulation's applicability for all EU data subjects.

The scope of the GDPR is global, and includes the possibility of penalties and direct enforcement actions if an organization is non-compliant. Because of this, it is important for organizations to have a good grasp of their IT controls in regards to personal data.

Controller vs. Processor

By researching the differences between controllers and processors, executives can better understand how their organization is defined within the context of the new regulation. This will help answer questions such as: What is the difference between a controller and a processor? Is my organization a controller or a processor? Are cloud service providers like Virtustream a controller or a processor? How does this affect me?

Article 4 of the GDPR outlines the exact definitions of controllers and processors. In short, the key differentiation between a controller and a processor is that a controller **'determines the purposes and means of the processing of personal data'.**

An organization can collect personal data and still be either a controller or a processor. However, if they are the ones **determining the means and purpose** for processing the personal data, then the organization is a controller. A processor is an organization taking part in processing the personal data on behalf of the controller. In the GDPR, any organization can be deemed a processor if they match this definition, as processors in the GDPR are not exclusively service providers.

Is Virtustream a Controller or a Processor?

Under the provisions of the GDPR, Virtustream may be a data processor when processing personal data as a cloud provider on behalf of a current customer that's considered a data controller under the GDPR. Virtustream may also be a controller when acquiring personal data from EU data subjects for the purpose of marketing and selling goods and services to them (e.g., cloud services and software).

For example, if a hospital providing services to EU data subjects has selected the Virtustream Healthcare Cloud to maintain the security of their clients' personal data, in the form of protected health information (PHI). As new clients come to the hospital, the hospital staff collects the healthcare data needed, and uses Virtustream Healthcare Cloud to store, update, and access the personal data.

In this example, both Virtustream and the hospital have assumed responsibility for the clients' personal data – meaning they both fall under the GDPR. The hospital is determining the means and purpose for processing the personal data, but, although they are collecting the data, they are not processing it themselves – making them the **controller**. Virtustream in this scenario is the **processor**, because it is processing personal data on behalf of the controller.

What is Considered 'Personal Data'?

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.[2]

[2] European Commission, "What is personal data?" accessed May 10, 2018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Personal data may include, but is not limited to:

- Name
- Home address
- Work address
- Landline number
- Mobile number
- Email address
- Personal identification number
- Passport number
- Social Security number
- Driver's license
- Credit/debit card number
- Cultural/social identity
- Health information (i.e. genetic, mental, physical, or physiological data)
- Financial information
- Bank details/account numbers
- Tax file number
- Computer IP address (EU region)
- Location/GPS data
- Social media posts
- Cookies

How Can GDPR Affect Organizations?

The GDPR is intended to protect personal data and the rights of individuals, and goes beyond previous EU law by establishing more comprehensive data protection standards. However, the big question most executives have, both within and outside the EU, is how this regulation will directly impact their organizations.

Personal data protection is mandatory with the GDPR, and will compel organizations that are responsible for personal data to move forward with privacy as a top priority. In order to comply and avoid severe penalties, organizations must build privacy into all of their processes, products, and systems that will process personal data.

The GDPR changes how organizations both inside and outside of the EU handle personal data. When compared to the previous Directive, the GDPR encompasses many more overseas organizations. In particular, US technology companies that are responsible for the personal data of EU data subjects must now take more care in how they handle customers' data.

International Data Transfers

Along with privacy driven developments, the GDPR has strict rules governing international data transfers that can directly affect organizations. Under the GDPR, transfers of EU data subjects' personal data to countries outside of the EU are only permitted where the conditions defined in the GDPR are met.

The intricate details of the GDPR require both controllers and processors to thoroughly understand the specifics of handling international personal data transfers under the GDPR conditions. By referencing resources, such as the European Commission, organizations can gain a deeper understanding and prevent the possibility of future penalties.

An example of an International Data Transfer condition, per Article 45 of the GDPR is:

"A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization."[3]

In this condition, there is an established onus to ensure an **adequate level of protection** when transferring personal data internationally. By understanding Articles 44 through 50 of the GDPR, organizations can determine how the Commission determines an adequate level of protection for an international transfer of personal data.

Penalties for Non-compliance

Organizations that do not comply with the GDPR can face severe penalties that will directly affect business workflow and value. If an organization is found to not fully comply with the GDPR, an EU supervisory authority can issue warnings, reprimands, suspensions of data transfers, bans on processing, and orders to correct infringement. An EU supervisory authority can also issue **substantial fines up to 4% of total global annual turnover** (i.e. annual revenue) in any instance of non-compliance that includes all revenue from all customers, not just revenue associated with EU nations or EU data subjects.

[3] Intersoft Consulting, "Art. 45 GDPR Transfers on the basis of an adequacy decision" accessed May 10, 2018. https://gdpr-info.eu/art-45-gdpr/

Breaches

With enhanced regulation on security and privacy for personal data, the GDPR also has a protocol for breaches, which is critical for all organizations. The GDPR breach notification requirement obliges controllers and data processors to report certain data breaches within 72 hours. Controllers may be required to notify a regulator, and possibly data subjects. Processors are required to notify the controllers about any covered breach.

Virtustream Helps Customers Better Manage Security and Privacy Risk

Virtustream closely partners with Dell's Global Privacy Office to protect the privacy of its customers located around the world. Dell's global privacy program is focused on ensuring the proper use and disclosure of our customers' personal data, as well as fostering a culture that values privacy through awareness. Virtustream cloud services and software complies with the GDPR as of the effective date, May 25, 2018.

Virtustream provides services and software to assist customers with their GDPR obligations, supporting customers' goals to manage risk and privacy more effectively and efficiently.

The following are some examples of the core GDPR obligations that Virtustream can assist an organization with.

Data Security and Incident Management

The Data security and Incident Management area of the GDPR requires an organization to have appropriate technical and organizational security controls and procedures in place to secure data subjects' personal data that they are processing, as well as notify the affected data subjects and/or an EU supervisory authority in the event of a data breach that is likely to result in a high risk to the rights and freedoms of data subjects.

Virtustream cloud services and software that help organizations address GDPR compliance obligations in this area include:

- **Virtustream Enterprise Cloud / Virtustream Healthcare Cloud**, powered by Virtustream xStream Cloud Management Platform, supports security and compliance with tools that assist with continuous auditing and reporting of data stored in Virtustream cloud infrastructure-as-a-service (IaaS), and includes security information and event management (SIEM) and governance, risk management and compliance (GRC) tools that collect and analyze data. Examples of Virtustream Enterprise Cloud compliance offerings, attestations, and certifications include: SSAE18/ ISAE3402/SOC2, PCI-DSS 3.1, ISO 27001:2013, ISO 9001:2015, ISO 22301:2012, and HIPAA/ HITECH/HITRUST.
- **Virtustream Viewtrust** provides out-of-the-box enterprise risk management (ERM) and continuous monitoring capabilities that enable customers to see a near real-time view of cybersecurity risk across the entire enterprise. In support of the GDPR provisions, it unifies data from numerous complex sources, regardless of location, and integrates that data into a drill-down representation of the customer's organization, business relationships, and systems. The identified risks are quantified, weighted according to impact, and presented from summary data at the executive level down to raw data at the operational level. Viewtrust enables proactive decision-making and remediation of risks, in a manner that is consistent, efficient, and actionable.

Accountability Principle

The Accountability Principle of the GDPR essentially means an organization must comply with the GDPR data protection principles and be able to suitably demonstrate that compliance.

Virtustream cloud services and software that help organizations address GDPR compliance obligations in this area include:

- **Virtustream Enterprise Cloud / Virtustream Healthcare Cloud** have been assessed by a retained independent audit firm to verify that security policies and practices will be consistent with GDPR requirements when it becomes effective. As a general practice, Virtustream provides independent third party security certifications and attestation reports under nondisclosure (NDA) to enable customers to quickly verity the effective operation of specific security controls. Virtustream adheres to the Cloud Infrastructure Service Providers of Europe (CISPE) Code of Conduct for GDPR, which contributes to Virtustream's demonstrated compliance.
- **Virtustream Viewtrust** implements powerful Governance, Risk Management, and Compliance (GRC) capabilities that enable customers to manage and document their compliance efforts related to the provisions of the GDPR.

Virtustream Viewtrust and the GDPR

Viewtrust enables customers to have more secure networks and data, by being more proactive with their enterprise compliance and risk management needs. It facilitates an efficient, collaborative, and consistent audit practice despite continually changing network environments and cyber threats. Customers benefit from a single holistic view and unified management of their enterprise on a continuous basis. Viewtrust also enables simultaneous, real-time collaboration across teams – breaking down silos within the organization and significantly increasing efficiency.

Virtustream Global Infrastructure

Virtustream has a significant data center presence in the EU and can process a Data Controllers workloads solely within the EU. Virtustream's global footprint does offer locations outside the EU as well and can accommodate data transfer requirements if this is the Data Controllers goal.

Data Center Locations

Virtustream offers choices for geographical location in the European Economic Area.

- **Virtustream Enterprise Cloud:** includes the UK, Germany, France, and the Netherlands.

Contact Us

For more information about Virtustream and the GDPR, please contact us at info@virtustream.com or visit us at www.virtustream.com. To see a complete list of our data center locations, visit our global infrastructure locations page.

About Virtustream

Virtustream, a Dell Technologies Business, is the enterprise-class cloud service and software provider trusted by enterprises worldwide to migrate and run their mission-critical applications in the cloud. For enterprises, service providers and government agencies, Virtustream's xStream® Management Platform and Infrastructure-as-a-Service (IaaS) meets the security, compliance, performance, efficiency and consumption-based billing requirements of complex production applications in the cloud - whether private, public or hybrid.

