The Simple Guide to GDPR Data Protection:

Key Requirements and Considerations for Compliant Email and File Sharing

AUTHOR: Tim Edgar, Senior fellow at Brown University's Watson Institute for International and Public Affairs

virtru

What is GDPR?

The European Union's General Data Protection Regulation (GDPR), is the basic framework for protection of personal information of EU citizens. The GDPR lays out detailed requirements governing the collection, use, sharing and protection of personal information.

GDPR replaces the EU's existing data protection rules, which were already among the strictest in the world. Previous EU data protection rules were provided in a directive, which means that EU member states were required to pass legislation to make those rules binding. GDPR is a regulation, which means it is directly effective and applies uniformly throughout the EU and in three other nations that are part of the European Economic Area: Norway, Liechtenstein and Iceland.

GDPR was adopted in April 2016 and entered into force on May 25, 2018.

While GDPR covers a broad range of data protection and privacy concerns, this paper is specifically concerned with encryption and access control provisions of the regulation.

Who is affected by GDPR?

GDPR affects all companies or entities who offer goods and services in the EU (whether or not for payment), who monitor behavior in the EU, or who offer goods and services or monitor behavior in Norway, Liechtenstein and Iceland.

Note that GDPR affects many more organizations than existing EU data protection rules. Previously, EU data protection rules depended on whether an entity had an "establishment" in the EU. GDPR applies worldwide.

GDPR applies to both data "controllers" and data "processors." A data controller is the entity (such as a business) that determines the purposes, conditions and means of processing personal data, while a data processor is the entity that actually processes the personal data (such as a cloud provider or other third party service). The same organization may be both a controller and a processor.

If I do not do business in Europe or handle the personal data of EU citizens, should my organization care about GDPR?

Yes. The European Union's data protection rules are influential worldwide. The EU makes it easier to transfer personal data outside EU countries if it determines that those nations provide privacy protections that are "essentially equivalent" to those provided by the EU. As a result, many other countries have adopted similar rules to protect the personal information of their nationals:

- **The UK government announced in June 2016 that it will adopt legislation that implements GDPR even after the UK leaves the EU.**

- More than 100 countries have adopted data protection legislation that is modeled in whole or in part on EU data protection rules. Many of them are likely to update their legislation in light of the EU's adoption of GDPR.

What does GDPR consider to be personal data?

Some examples include:

- Name
- Photo
- Email address
- IP address
- Banking or other personal information
- Medical information
- Social networking posts
- Any other data that can used to identify a person

What happens if I ignore GDPR?

For the most serious violations, organizations can be fined up to a maximum of €20 million or 4% of annual worldwide turnover, whichever is greater. (This is much greater than previous penalties for violating EU data protection rules.)

What are the Technical Requirements? How Does Virtru Help?

Virtru's encryption and access management solutions facilitate GDPR compliance in four ways:

- Strong, easy-to-use client side encryption for emails and files.
- Complete control of customer encryption keys.
- Powerful access control tools that allow organizations to maintain control of their data, regardless of where the emails and files are created, stored, or shared.
- Audit tools that facilitate insight and reporting on when and where email and files have been accessed or shared.

Encryption

GDPR includes strict security requirements, including encryption, as part of an overall risk-based approach to cybersecurity. Organizations must assess the risk of data loss and data breach, and must consider technical measures to mitigate those risks, including pseudonymization and encryption. Any breaches that do occur must be reported to regulators within 72 hours, and data subjects must be notified "without undue delay"—unless the organization can demonstrate that the data were encrypted.

GDPR includes an explicit duty to consider encrypting personal data as part of an overall obligation to use "state of the art" security measures. As a result, for many organizations and uses, encryption is effectively mandatory. Because encryption is a common security measure and cybersecurity risks are increasing, it is likely that regulators and courts will find that in many if not most situations a decision to forgo encryption is a violation of GDPR.

In a report published in 2014 on privacy and data protection by design, the European Union Agency for Information and Network Security (ENISA) examined both client-side and end-to-end encryption. Client-side encryption is generally used by cloud service providers to protect data in transit to and from the cloud provider. End-to-end encryption means that data is stored in the cloud in encrypted form, without the ability of the cloud provider to access it.

Significantly, the ENISA report states that services such as "electronic mail" that mediate communications between end users "should prefer to encrypt the communications between users in an end-to-end fashion, meaning the encryption is added at one user end-point and is only stripped at the other end-user end-point, making the content of communications unintelligible to any third parties including the service providers."

This is precisely what Virtru provides. Emails and files are encrypted on the client to protect data before it leaves your device. Although many cloud services (such as Gmail) provide encrypted channels for communication between customers and the cloud service provider, the content is still available to the service provider. This makes personal data more vulnerable to compromise, both from data breaches and from government surveillance under laws like the Foreign Intelligence Surveillance Act. However, if a customer uses Virtru, the data stored by the service provider is encrypted end-to-end. This meets the security standard that the ENISA report recommends as the "state of the art" for email.

Key Management

GDPR mandates a risk-based approach to cybersecurity. It requires that organizations use "state of the art" technical measures, including encryption, when necessary. This approach implicitly requires organizations to consider the issue of key management as part of their overall policies for the protection of personal data.

Here, the ENISA report is also instructive. It states:

While the service providers may wish to assist users in authenticating themselves to each other for the purpose of establishing such an end-to-end encrypted channel, it is preferable, from a privacy perspective, that the keys used to subsequently protect the confidentiality and integrity of data never be available to the service providers, but derived on the end-user devices.

Virtru's encryption service always ensures that your cloud service provider (such as Gmail) never has access to the encryption keys used to protect your content. Through its Customer Key Server (CKS) offering, Virtru also provides the ability for customers to host their own encryption keys. Keys may be geo-located and hosted either on premise, in a private cloud, or in the public cloud of the customer's choosing. The CKS provides the enterprise with exclusive control of their encryption keys; no cloud provider or other third party has access to unencrypted key material.

Access Control

GDPR includes many requirements for the handling of personal data that go beyond "state of the art" security, including encryption. GDPR emphasizes data governance and accountability. It requires organizations to take control of the personal data that they manage.

Organizations must show they have adopted policies and procedures to ensure control of personal data. They must use systems that provide "privacy by design," that is, data protection by default, not as an afterthought. They must have systems that are capable providing data subjects with their rights under GDPR—rights such as expiration and erasure.

Virtru provides a host of access control features that enable organizations to meet these requirements. Emails and files are protected from the time they are created throughout their lifetime—no matter where they are shared. Users and administrators decide who can access content, and for how long.

Access can be revoked at any time—even after emails and files have been shared or opened. Virtru also enables automatic expiration after a specific period of time, enabling organizations to enforce retention limits for personal data. Email and file forwarding can be audited, limited, or prevented altogether.

Audit

GDPR emphasizes data accountability and audit. Organizations must keep records to show they are complying with GDPR requirements, and make those records available to regulators. Organizations that process personal data on a large scale, or that process particularly sensitive data, must appoint a high-level "data protection officer" to enforce privacy and data protection policies.

Virtru's features will help organizations show they are taking compliance seriously. Administrators can audit access to protected content in real time. They can see when emails and files have been forwarded or shared, and who has access to them.

Virtru has patented search technology to allow administrators to search archived encrypted content to meet regulatory e-discovery and other legal requirements.

Finally, Virtru has data loss prevention (DLP) tools that allow administrators to set rules to automatically protect sensitive content, including personal information, by warning users, adding encryption, notifying administrators, and more.

GDPR requirements and Virtru: Quick summary

Virtru's data protection software provides capabilities that can help your organization meet these email and file sharing requirements:

Topic	GDPR Requirements	Relevant Virtru Features
Risk-based email and cloud encryption	Controllers and processors must "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk" including "encryption of personal data" along with other security measures. *Art. 32. See also preamble, ¶ 83, p. 51.*	Virtru offers email and cloud encryption, using strong AES-256 bit encryption, in an end-to-end fashion.
State of the art security	Technical measures, including encryption, must take account of "the state of the art," costs, and severity of the risk. *Art. 32*. According to the European Union Agency for Information and Network Security (ENISA), the "state of the art" for email encryption requires end-to-end security.	Virtru's client-side, end-to-end encryption is the state of the art for email encryption.
Key management	GDPR does not include specific rules for key management, but it does require that technical security measures to account of the "state of the art." ENISA has recognized that users may want to take advantage of encryption service providers while recognizing that "it is preferable, from a privacy perspective" that service providers do not have access to keys.	Virtru allows customers to manage their keys through its customer key server (CKS), or customers may choose to use Virtru's secure key server or another cloud provider.

Topic	GDPR Requirements	Relevant Virtru Features
Re-use of personal data for other purposes	If a controller wants to take advantage of exceptions that permit the use of personal data for purposes other than those for which it was collected, the controller must take into account "the existence of appropriate safeguards, which may include encryption or pseudonymisation." *Art. 6(4).*	Virtru's object-based security allows administrators to set rules for sharing information, control forwarding, and revoke access.
Breach notification exception	Generally, controllers must report data breaches to authorities within 72 hours, and to data subjects "without undue delay." However, organizations do not have to report breaches to data subjects if the data were made "unintelligible to any person who is not authorized to access it" through measures "such as encryption." *Art. 34(3).*	Virtru's strong AES 256-bit encryption is military grade. Unless both the encrypted content and the keys are compromised, the information remains unintelligible to unauthorized persons.
Privacy by design and by default	Controllers must consider privacy and data protection in the design of their systems, and this includes technical measures to ensure "by default" that only necessary personal data are processed. "This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility." *Art. 25(2)*	Virtru allows administrators to set rules for data sharing, limit or prevent forwarding of emails or files, set expiration dates for data, and includes data loss prevention features to warn users, add encryption, notifying administrators, and more.

Topic	GDPR Requirements	Relevant Virtru Features
Access control	Controllers "shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons." *Art. 25(2)*. In other words, controllers must show that they can control to whom personal data is provided.	Users and administrators decide who can access content, and for how long. Access can be revoked at any time—even after emails and files have been shared or opened.
Technological neutrality	The regulation requires that the "protection of natural persons should be technologically neutral." *Preamble ¶ 14, p. 9* In other words, the requirement to protect personal data should not depend on the technology the organization is using (e.g., storing data on site versus "in the cloud.")	Emails and files are protected from the time they are created throughout their lifetime—no matter where they are shared. Virtru does not depend on which device or platform is used.
Audit and compliance	Personal data may be processed only on certain lawful grounds (contract, vital interests, public interest, among others) or with valid consent of the subject. Consent must be given in clear and plain language. Lengthy, legalistic terms of service agreements will not work. Organizations are required to keep records that demonstrate compliance with these and other rules.	Administrators can audit access to protected content in real time. They can see when emails and files have been forwarded or shared, and who has access to them. Emails and files can be classified based on their contents to support data protection actions.

Topic	GDPR Requirements	Relevant Virtru Features
Withdrawal of consent	The regulations specifies that it must be as easy to withdraw consent as it is to give consent, and that the organization must be able to make effective a data subject's decision to withdraw consent.	Virtru permits an administrator to search protected files by keyword (such as name or identification number), and allows revocation of access at any time, even where data has been opened or forwarded.
Erasure	Data subjects have the right to have data deleted when it is no longer relevant (commonly known as the "right to be forgotten").	Rules can be set that revoke access to data after a specific period of time.
Retention and expiration	Organizations must specify policies providing for limits on retention of personal data, and ensure that such data will be erased or rendered unusable after a certain time (expiry).	Rules can be set that revoke access to data after a specific period of time.

About the Author

Timothy H. Edgar is a former national security and intelligence official, cybersecurity expert, privacy lawyer and civil liberties activist. Edgar joined the American Civil Liberties Union shortly before the terrorist attacks of September 11, 2001, and spent five years fighting in Congress against abuses in the "war on terror." He left the ACLU to try to make a difference by going inside America's growing surveillance state—a story he tells in *Beyond Snowden: Privacy, Mass Surveillance and the Struggle to Reform the NSA*.

In 2006, Edgar became the intelligence community's first deputy for civil liberties, advising the director of national intelligence during the George W. Bush administration. In 2009, after President Barack Obama announced the creation of a new National Security Council position "specifically dedicated to safeguarding the privacy and civil liberties of the American people," Edgar moved to the White House, where he advised Obama on privacy issues in cybersecurity policy.

In 2013, Edgar left government for Brown University to help launch its professional cybersecurity degree program and he is now a senior fellow at Brown's Watson Institute for International and Public Affairs. Edgar also works to help companies navigate cybersecurity problems, and is on the advisory board of Virtru, which offers simple encryption software for businesses and individuals.

Edgar has been profiled by CNN's Christiane Amanpour and his work has appeared in the *Wall Street Journal*, the *Los Angeles Times*, the *Guardian*, *Foreign Affairs*, and *Wired*, and he is a contributing editor to "*Lawfare: Hard National Security Choices*." Edgar was a law clerk to Judge Sandra Lynch, United States Court of Appeals for the First Circuit, and is a graduate of Harvard Law School and Dartmouth College.

To learn more about leveraging Virtru for GDPR compliant email and file protection, get in touch with us today. virtru.com/contact-us