Manage your data securely in the cloud:

A concise guide to getting ready for the GDPR

tresorit

Tresorit eBook on GDPR compliance

1. Introduction: why the GDPR matters for your business

The General Data Protection Regulation (GDPR) is a comprehensive regulation that unifies data protection laws across all European Union member states. It defines an extended set of rights for European Union citizens and residents regarding their personal information. Consequently, it describes strict requirements for companies and organizations on collecting, storing, processing and managing personal data. Businesses have little time and a lot of challenges to comply with the requirements, as they must review and adapt all their existing processes and services used to collect and handle personally identifiable data of their employees and customers.

This eBook aims to help you comprehend what the General Data Protection Regulation is, what are its requirements for managing personal data, and why the GDPR highlights encryption as an important technology measure to safeguard data.

> "The GDPR will change not only the European data protection laws but nothing less than the world as we know it." Jan Philipp Albrecht, MEP, EU rapporteur on GDPR

Our eBook helps you:

- ✓ **Learn basic concepts** such as personal data, data collector, and data processor of the GDPR regarding data protection
- ✓ **Get familiar with technical measures** recommended by the GDPR to safeguard data
- ✓ **Understand how encryption, especially end-to-end encryption, helps** your business manage personal data in the cloud in a GDPR compliant way
- ✓ **Get actionable tips on what you and your company should do** to prepare your data management processes for the GDPR

1. Which companies does the GDPR affect?

The GDPR has a broad territorial scope. The regulation applies not only to all organizations established in the EU that process personal data, but also to any non-EU established organizations that process personal data of individuals who are in the EU in order to offer them goods and services or monitor their behavior within the EU.

Checklist 1: Is my organization impacted?

- ☐ Do you manage personal data of EU residents, such as customers and employees?
- ☐ Do you process data of EU residents for offering them goods?
- ☐ Do you monitor customer or user behavior in the EU?

If you checked any of these boxes, you need to comply with the GDPR.

2. What's a data controller and a data processor?

The GDPR aims to protect personal data at all stages of data processing. The GDPR identifies two different entities that both have obligations: data controllers and data processors. Under the previous EU Data Protection Directive, only controllers could be held liable. With the GDPR, processors now also face serious data protection requirements and obligations.

A controller is an entity that determines the purposes, conditions, and means of the processing of personal data. For example, educational and research private and public institutions, healthcare services, or any business that manages the personal data of their employees and customers.

A data processor is an entity which processes personal data on behalf of the controller, such as a cloud provider (for example, Software-as-a-Service companies like a CRM software).

It is important, that a company can act both as a controller and a processor, depending on the exact type and usage of data. For example, a cloud-based software company is a data controller regarding the personal data of their own employees, but a processor regarding the personal data that their clients process with their software.

Checklist 2: Am I a data controller or processor?

- Do you keep or process information about living people?

If your answer is yes, you are a controller.

- Do you process personal information, but without the responsibility or control over that data?

If your answer is yes, you are a processor.

3. When will the GDPR be enforced?

The GDPR entered into force on May 24, 2016, and it will directly apply in all EU Member States from May 25, 2018. Organizations have less than a year to prepare for compliance.

The GDPR is immediately binding for and applicable in all European member states starting on 25 May 2018. This presents an important contrast to the previous legislation, known as the EU Data Protection Directive, which was a directive addressed to the EU member states and made it their responsibility to turn it into internal law.

4. What are the fines for non-compliance?

Data controllers and data processors face severe consequences if they do not comply with the European rules. Depending on the infringed provision of the GDPR, fines may amount to a maximum of EUR 20 million, or, 4% of the global annual turnover of the controller, whichever is bigger. Moreover, both controllers and processors are subject to joint liability for damages.

2. Requirements of the GDPR regarding the protection of personal data

The GDPR requires companies to implement reasonable data protection measures to protect consumers' personal data and privacy against data loss or exposure.

1. Main principles

Article 5. of the GDPR summarizes the most important principles regarding the management of personal data:

- **Lawfulness, fairness, and transparency**: personal data should be processed lawfully, fairly, and in a transparent manner
- **Limited purpose**: personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- **Data minimisation**: personal data should be adequate, relevant, and limited to which it is necessary in relation to the purposes for which they are collected
- **Accuracy**: personal data stored and managed should be accurate and, where necessary, kept up to date
- **Storage limitation**: personal data should be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- **Confidentiality and integrity**: personal data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

2. Main areas of obligations

The GDPR lists the rights of persons (called "data subjects") and the obligations of data processors and controllers in a detailed way. A significant change brought by the GDPR is that organizations will be held more accountable for how they manage people's personal information.

- **Natural persons have a right to their personal data**, this means among other things, their right for asking their data to be deleted (right to be forgotten), that companies must respect.

- **Organizational measures**: the GDPR details the organizational measures needed to take to comply, such as appointing a Data Protection Officer, having data protection policies in place, and more.
- **Security measures**: the GDPR explains several technology measures to protect personal data and describes the way how organizations should act in case of a data exposure and breaches. The GDPR enables data protection authorities to impose severe fines on organizations in case of non-compliance.

3. What is personal data?

The GDPR requirements only apply for personal data. Organizations should take measures to minimize the amount of personally identifiable information they store, and ensure that they do not store any information for longer than necessary.

In the GDPR, personal data is defined as any information related to an identified or identifiable natural person. For example, if a medical dataset contains the patients' name, hometown, and medical diagnosis, then a record (or „row") within a dataset is personal data if the patient who this record is about can be re-identified, that is, anybody who has access to this dataset is able to associate the record with the patient.

However, there are other factors to consider. Datasets are regarded personal when any record owner is re-identifiable during an attack, depending on whether a re-identification attack is (1) likely to happen and (2) also likely to succeed. Specifically, the attack must have reasonable (1) plausibility and (2) success probability.

The GDPR's definition of personal data is very general and includes many kinds of information which may seem non-personal at first sight. These are not necessarily "structured" or relational datasets.

1. Is sensitive data also personal data?

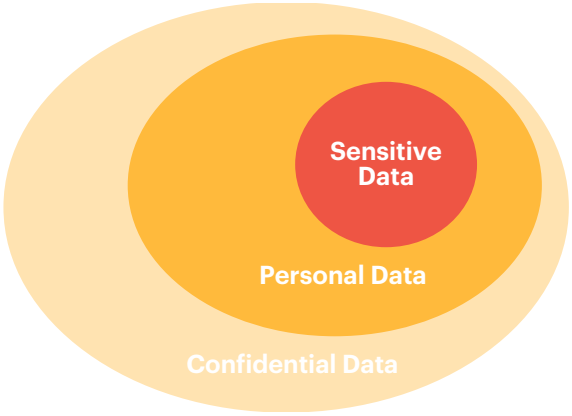
Sensitive data is a special sub-category of personal data which enjoys extra consideration and protection in GDPR as they may give rise to strong stigmatization or discrimination in a society. Sensitive data are personal data that reveal any racial or ethnic origin, financial status, political opinion, philosophical belief, religion, trade-union membership, sexual orientation, or concerns health and sex life, genetic data, or biometric data.

Many people (falsely) think that GDPR addresses only sensitive data. For GDPR, personal data is any information that is attributable to a specific individual independently of the nature of the information.

Nevertheless, the distinction between sensitive and insensitive data can be at least as blurred as between personal and non-personal data. An extreme example: is a video about a person sensitive? It can be, as one can compute the pulse rate from the variation of skin color using sophisticated image processing techniques, and abnormal pulse rate can be a precursor of many diseases. It is to be seen how this legal definition will be interpreted in practice.

2. What is confidential data?

It's worth noting the difference between confidential and sensitive data. Confidential data is a broad categorization of any information of commercial value in which disclosure, alteration, or loss could cause substantial harm to the competitive position of the data holder. Hence, confidential data includes much more than personal data.



4. The GDPR and encryption

1. The 4 advantages of using encryption to achieve GDPR compliance

Besides pseudonymisation, the GDPR highlights encryption as one of the appropriate organizational and technical measures to ensure data protection.

§

"The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data"

GDPR Article 32. Security of Processing

The GDPR underlines this technology because in case of a server-side data breach or leak, strongly encrypted datasets are unintelligible to unauthorized people. Encryption makes the re-identification of persons from the leaked datasets impossible with reasonable efforts. Therefore, the persons are protected from harmful effects of data exposure.

This chapter will detail why encryption helps your company or organization ensure compliance while enjoying the convenience of cloud-based services.

1. **Protect the personal data of employees, customers, partners, and users.** Increase trust for your service and organization by complying with the regulation and using the strongest data protection technology recommended in the text of the law.
2. **Keep your personal data within company walls.** When using encryption, especially end-to-end encryption for managing data in the cloud, your organization's personal data stays within company walls. Your encrypted cloud-based processor does not technically process personal data, they only manage the encrypted, unintelligible datasets. Even in case of a data breach, encrypted data is not in danger. This can simplify your compliance processes and save you time for working on other GDPR-related requirements. For example, if you're audited for compliance, your encrypted cloud service might fall out of your audit's specific scope.
3. **Reduce your liability in case of a data breach**. If you use encryption, especially end-to-end encryption, you are relying on an appropriate safeguard highlighted by the GDPR. This can reduce your liability in the event of data exposure.
4. **Save costs of data breach notifications and potentially fines**. When using encryption, your organization is not obliged to notify your customers or users on data breaches.

2. Different types of encryption: why end-to-end encryption wins?

The GDPR does not specify technologies such as algorithms and their applications. However, the way encryption keys are managed is important to decide whether the re-identification of persons from the leaked dataset is possible or not. End-to-end encryption with client-side key management represents a significantly stronger protection for personal data.

> "Using robust end-to-end encryption to safeguard personal data is both a responsible choice and a key step towards compliance." Paolo Balboni, Ph.D., Founding Partner of ICT Legal

Checklist 3: Am I using strong enough encryption?

- ■ Does your provider have access to your encryption keys?

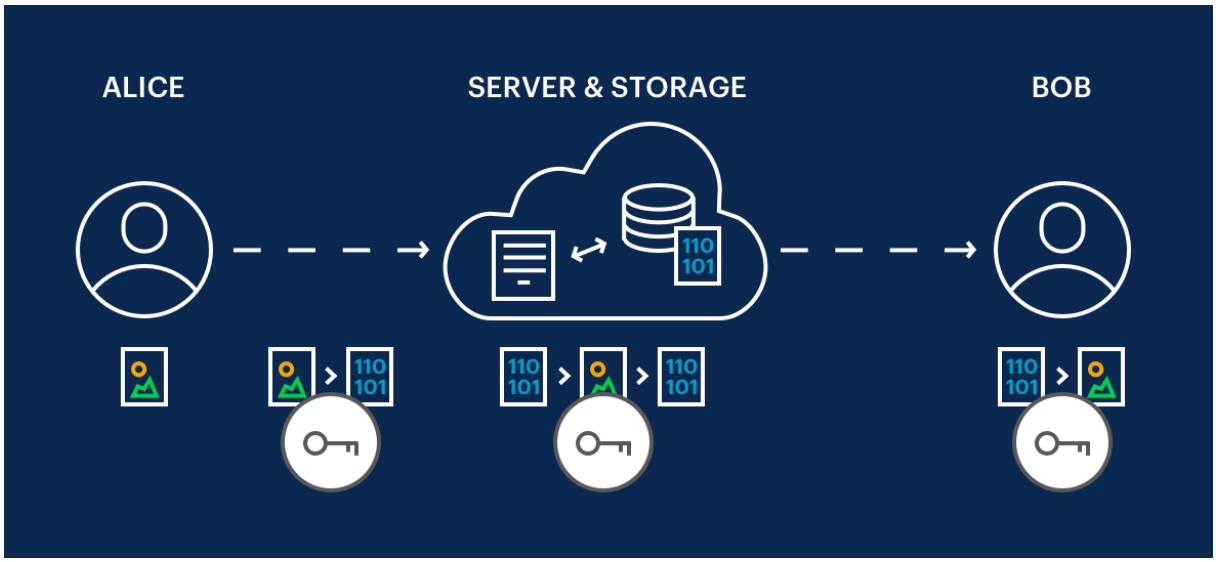
If your answer is don't know or yes, you most likely are using a service with at-rest, server-side encryption.

- ■ Do you manage your own encryption keys?

If your answer is yes, you are most likely using a service with client-side key management, like end-to-end encrypted services.

1. At-rest, server-side encryption

With channel & at-rest encryption, the cloud provider has access to the encryption keys and the server stores the data in an unencrypted format as well. Thus, in case of a breach, re-identification of the persons from the leaked dataset is technically possible.



2. End-to-end encryption

With end-to-end encryption, the cloud provider doesn't have access to the encryption keys. The server stores the encryption keys and user contents only in an encrypted format. This way, end-to-end encrypted cloud service providers like Tresorit can never access the contents of user files. The re-identification of persons from the end-to-end encrypted data is infeasible, even in case of a server-side data breach. When a breach happens, only the encrypted data leaks and no one can read the contents. The personal data of your staff and clients is not threatened.

5. How Tresorit's end-to-end encryption technology helps to comply with the GDPR

GDPR Article	Why does end-to-end encryption help?	Tresorit technology
Article 6. Lawful basis of processing "The controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: appropriate safeguards, which may include encryption or pseudonymisation."	End-to-end encryption is highlighted as an appropriate safeguard for protecting data. Data controllers must further process data with third-party processors and protect data in a compatible way with the original legal basis and applying safeguards like encryption.	✓ End-to-end encryption is done on the client side: no user file is ever sent to the cloud unencrypted, encryption keys stay at the user's side and never reach Tresorit servers ✓ Using industry-standard cryptography algorithms: AES-256, RSA with 4096 bit long keys ✓ Patented key management technology for sharing end-to-end encrypted content.
Article 32. Security of Processing "The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: the pseudonymisation and encryption of personal data."	End-to-end encryption protects personal data in the cloud from third-party access. By using end-to-end encryption, the data controller will be in compliance with Article 32 GDPR.	✓ See above.
Article 34. Communication of a personal data breach to the data subject "The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;"	If encrypted, especially end-to-end encrypted, data leaks, the re-identification of persons from this dataset is infeasible. Therefore, companies don't have to notify users.	✓ See above. Learn more about our security: https://tresorit.com/security
Article 25. Data protection by design and by default "The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures."	Organizations must develop internal data protection processes and products with data privacy in mind from the ground up.	✓ Data governance features: file permission control, DRM, user group management ✓ Admin Center to set company-wide security policies (IP restrictions, disabling local sync, etc.) ✓ Tresorit ZeroKit – our SDK allows developers to integrate our end-to-end encryption into their own services. Learn more about our data control: https://tresorit.com/business

6. 5 first steps towards managing data in a GDPR-compliant way

Data security in your company or organization stands and falls with your co-workers, service providers, and clients. Here are some best practices to help you establish safer data management in your daily work routine.

1. Establish best practices

• Principle of Least Privilege

The GDPR requires you to minimize the personally identifiable data managed by your teams. Intended to decrease the damage produced by a security breach, the Principle of Least Privilege limits the access of information only to users that need it for a legitimate purpose or role. The idea behind it is that data protection can be improved if data is shared only to a limited number of people who require it for their work and who are professionally trained to manage it. For example, an accounting team does not handle interviews; they do not need database access to incoming job applications.

• Need-to-Know Principle:

The Need-to-Know policy is usually enforced by organizations dealing with classified military or governmental information. Similar to the Principle of Least Privilege, it implies that even if a person has ample clearance for a certain degree of confidentiality, information will only be shared or discussed if it is required to perform a specific task. If applied to your office, it means that you do not grant access rights or discuss project details only based on hierarchy levels or trust, but by specific role and involvement in an assignment.

• Privacy by Design

The GDPR includes Privacy by Design as part of its data protection framework. This principle aims to take privacy into account throughout the whole engineering process from the very beginning to protect the users' privacy and give them control over their data. It stands by the idea that the future of privacy cannot be assured solely by compliance with external regulations, but it must ideally become an organization's default mode of operation.

2. Use encryption extensively

• Switch to end-to-end encrypted services

With end-to-end encryption, encryption and decryption are done directly on the device before they are uploaded to the cloud. No one can access stored data, except for the owner and users authorized by the proprietor.

Currently, the number of services offering end-to-end encryption for various communications channels is, fortunately, growing every day.

• Use HTTPS

Everything starts with the security and privacy of the internet connection of your organization. HTTPS encrypts the communication channel between your device and the online service you are visiting. Make sure your colleagues submit information only through encrypted sites using the https protocol. This can be achieved by holding regular security trainings for your staff.

• Use local encryption

Encryption in the cloud doesn't mean physical protection. End-to-end encryption protects data in the cloud. However, it means that you are responsible for protecting the device where the information and files are stored. For that, disk encryption, malware protection and the use of pin codes are essential.

3. Set up internal data governance policies

• Manage permission levels for accessing data

Many services, especially cloud storage providers, enable you to manage access permissions for shared projects or folders. Invited users can be granted different roles such as viewer (can read the content), editor (can make edits) or manager (able to make more significant changes such as renaming, deleting or inviting more users). The owner can also revoke access anytime.
With this control feature, you can introduce best practices such as the Least-Privilege Principle and the Need-to-Know Principle in your office and make sure nobody has more access to confidential documents than the ones necessary.

• Set up account security measures

In addition to your password, 2-step verification provides a second, randomly generated, password. As your password is the key to your files including personal data, it is highly recommended to secure it with an extra lock. Adding 2-step verification using voice call, text message, a dedicated authentication app, or email provides an additional layer of security that makes it way harder for hackers. Nowadays, many services make it possible for the system administrator to make it mandatory for everyone in their company.

4. Create data governance policies for external data sharing

• Share files containing personal data carefully

If you are sharing documents with people outside your team or organization, it is not always possible to apply sophisticated permission settings. Revocable download links can help you to avoid the insecure upload of email attachments and, if necessary, block a link after sending the email. Additional safeguards such as password protection are recommended

• Use services that are cross-platform

In the times of remote work, business trips and flexible working hours, it becomes increasingly unrealistic to limit data access to the desktop computers in the company headquarters. If secure IT solutions aren't flexible enough, it is tempting for employees to find insecure workarounds. Even CEOs and state leaders may give in to the temptation if they cannot access important information in a convenient way. Use services that can be accessed from all platforms.

5. Have a fall-back plan

• Protect your devices

If you leave your work mobile phone or laptop unattended on the beach or in a café, your device and data can easily get into the wrong hands. But there are several useful measures next to disk encryption that - if activated - help you to protect confidential business data even if the device itself is stolen and cannot be recovered. Some examples include remote wipe and device unlink.

tresorit

Learn more about GDPR, end-to-end encryption and Tresorit:
Watch our webinars with experts: https://tresorit.com/webinar#gdpr-webinars
Explore Tresorit Business features: https://www.tresorit.com/business