Getting ready for the GDPR with end-to-end encryption

Regulation and technology overview of encryption and compliance

Tresorit Whitepaper

Introduction: why the GDPR matters for your business

The GDPR is a comprehensive regulation that unifies data protection in all EU countries. It will directly apply in all EU member states from 25 May 2018; businesses have less than a year to prepare. It's time to act now.

The GDPR has a very broad territorial scope and will apply to any organization that manages the personal data of individuals who are based in the EU, regardless where the organization is registered. Non-compliance leads to severe consequences. Fines may amount to a maximum of EUR 20 million, or 4% of global annual turnover.

The GDPR requires organizations to implement reasonable data protection measures to protect the personal data of consumers and employees against data loss or exposure. To achieve that goal, the law regulates all areas related to data management and processing, from obtaining user consent to setting up company-wide data protection practices and handling data breach incidents. This whitepaper helps you to explore why the GDPR highlights encryption as an important technology measure to safeguard data. It also details how encryption, especially end-to-end encryption, helps your business manage data in the cloud in a GDPR compliant way.

> "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

Why encryption helps GDPR compliance

1. **Encryption makes data processing in the cloud less risky.**

   Cloud-based applications are convenient and useful, but they could create risks for your data. Under the GDPR, your organization as a data controller is responsible for protecting all personal data you manage throughout its lifecycle, from collecting to forwarding, while managing that with cloud-based services.

   The GDPR highlights encryption as one of the appropriate technical 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

2. **Encryption keeps personal data secure from third party access.**

   In case of a data breach or leak, encryption, and especially end-to-end encryption, makes the re-identification of persons from the leaked datasets impossible with reasonable efforts.

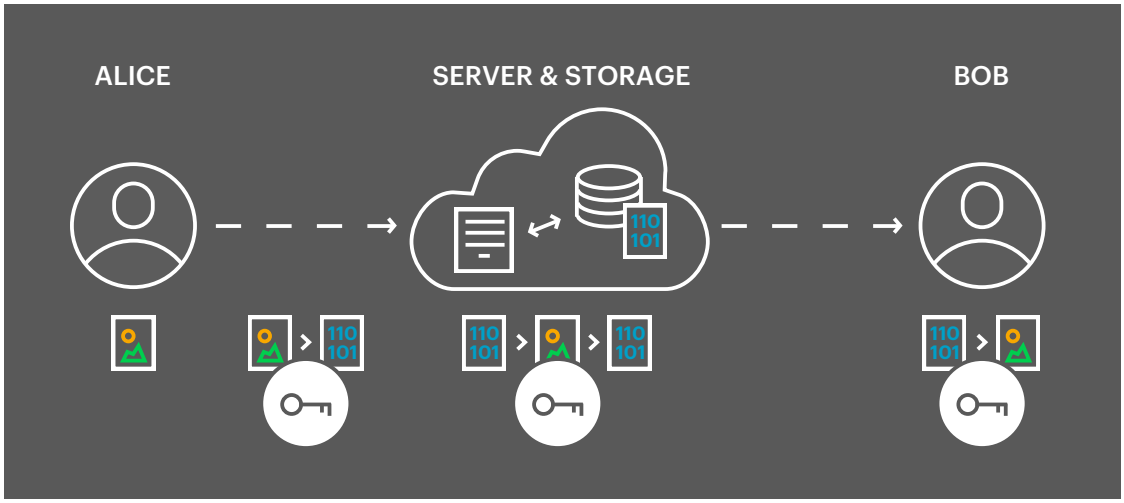
> "Using robust end-to-end encryption to safeguard personal data is both a responsible choice and a key step towards compliance."
>
> Paolo Balboni, Ph.D., Founding Partner of ICT Legal Consulting and President of the European Privacy Association

3. **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.

At-rest, server-side encryption

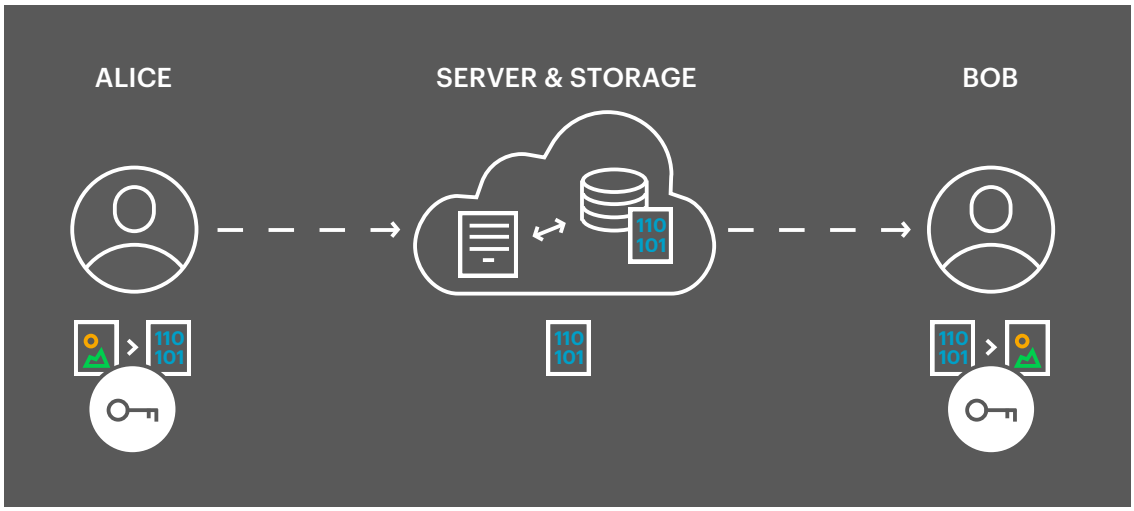
With channel & at-rest encryption, the cloud provider has access to the encryption keys and the server stores the data in an unencrypted format as well. Thus, in case of a breach, re-identification of the persons from the leaked dataset is technically possible.



End-to-end encryption

With end-to-end encryption, the cloud provider doesn't have access to 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.



The advantages of using encryption in ensuring GDPR compliance

- ✓ **Protect the personal data of employees, customers, partners, and users.** Increase trust for your service and organization by complying with the law and using the strongest data protection technology.
- ✓ **Simplify compliance.** When using end-to-end encryption in the cloud, your personal data stays within company walls, even when using the cloud. Even in case of a data breach, encrypted data is not in danger.
- ✓ **Reduce liability in case of a breach.** If you apply end-to-end encryption, you are using an appropriate safeguard that is recommended by the GDPR. This can reduce your liability.
- ✓ **Save costs of data breach notifications and potentially fines.** When using encryption, your organization is not obliged to notify your customers or users on dat breaches.

Relevant GDPR articles and how end-to-end encryption technology helps to comply with them

GDPR Article	Why end-to-end encryption helps?	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 by protecting 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 4092 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 result 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

What is personal data?

The GDPR only applies to personal data. Personal data is any information relating to an identified or identifiable natural person ("data subject"). Examples: a name, an identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Under the GDPR, all businesses 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.

How does end-to-end encryption protect personal data?
The data controller's end-to-end encrypted documents, such as a spreadsheet with employee details stored with Tresorit, may contain personal data. As the data controller has the encryption key to decrypt the files, they can re-identify the person the data belongs to. However, from the perspective of the end-to-end encrypted data processors like Tresorit, this spreadsheet does not contain any personal data because Tresorit, as service provider, does not have the decryption keys to the files. Thus, Tresorit is unable to re-identify the persons.

Is Tresorit already compliant?

Tresorit handles all user data with utmost care, and due to our end-to-end encryption, we are technically unable to access the contents of user files. We are currently working on finalising our ISO27001 compliance process which complements our GDPR efforts. Tresorit as a company itself will be compliant with GDPR by the time it is applied.

Learn more at:
tresorit.com/gdpr
tresorit.com/business