GDPR Compliance Review and Vendor Assessment

End-to-end encryption based Geens asset review manual

GDPR Compliance Review and Vendor Assessment

Objective

The purpose of this manual is to provide transparency to the latest data protection law and Geens.com solution compliance reviews conducted by the Geens Team, identify key compliance principles, and raise compliance concern. This aims to help reduce risk to your brand.

As a matter of fact, data protection is becoming more and more a major awareness for variety of businesses and services. A new set of law to protect privacy and data is called General Data Protection Regulation (GDPR). The regulation is aiming to severely change the way businesses and services can collect, store and protect data of their clients, customers or even website visitors.

Why does the GDPR matter to your business?

The GDPR regulation that unifies data protection in all EU countries will directly apply from 25 May 2018.

The GDPR has a very broad territorial scope and will apply to any organisation that manages the personal data of individuals who are based in the EU, regardless where the organisation is registered.

Non-compliance leads to severe consequences. The fines may amount to a maximum of EUR 20 million, or 4% of global annual turnover.

According to the new regulation, organisations have to take reasonable measures to protect their consumers and employees' personal data in order to avoid any loss or revelation. It is achievable within the current law as it handles all subjects related to data management and processing, user consent collection, company specific data protection cases, data breaches, etc. In this paper you will learn the necessity for encryption technology for the GDPR goals' achievement.

Document also shows how end-to-end encryption helps your business manage data in the cloud in a GDPR compliant way.

What will my business have to do?

1. Appoint one of your directors to be accountable. This person has to be suitably competent to handle the technicalities involved, and it's worth considering where you want the accountability to remain – with the IT, legal, HR, marketing department or elsewhere.

2. Ensure you have safeguards in place: procedures to ensure data is confidential, accurate, available when necessary, backed up and encrypted.

3. Ensure your suppliers are GDPR-compliant. Any service provider you use to process data has to comply with GDPR standards – and ensuring they do is your responsibility.

4. Ensure your customers, clients or website users have explicitly consented to their data being stored. This is a significant change, and most current measures are not sufficient. Your records need to prove that users have agreed to you storing their data – and failing to disagree is not enough. Crucially, users will also have a statutory right to have their data erased permanently from your records – so you'll need the the capability to perform that activity.

5. Ensure you're explaining to users, in plain language, what data you're holding, how long you're holding it for, and how users can withdraw their consent. Your policy has to be simple and appropriate, as well as containing all the required information.

6. Report breaches. Under GDPR, any breach of data protection must be reported to the relevant supervisory authority within 72 hours. You'll need a robust process for detecting, reporting and responding to databreaches.

7. Be prepared for more access requests. As people become more aware of their data privacy rights, they are likely to query the data you're holding, and you'll need to turn those requests around in good time.

In the short term, we recommend appointing an accountable director, setting aside a budget for new data protection systems, and establishing exactly what personal data your business is storing and how. This will enable you to establish a plan for appropriate compliance in advance of the GDPR rollout in May 2018. Contact us for more detailed GDPR advice over the coming weeks and months.

At the bottom line, GDPR is going to affect almost every business in the EU and the World at large.

How does end-to-end encryption help meet GDPR requirements?

1. Using cloud is less risky with encryption

Using cloud based applications is convenient and efficient in your business, on the other hand, they could create risk or breaches of your data. To comply with GDPR, your organisation as a data collector or forwarder is responsible for protecting any third parties' data during data assessment and management on your cloud based services.

General data protection regulation distinguishes encryption as one of the best ways to ensure data protection within your organisation.

> ***Article 32. Security of processing***
> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 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:*
>
> *(a)the pseudonymisation and encryption of personal data;*

2. Use encryption to keep your data safe and secure from third party access

There is always a possibility of data leakage or breach especially when dealing with third parties.

End-to-end encryption assures that leaked data or data sets will stay unidentified. However, always keep in mind that "a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified" to relevant supervisory authorities (WP29 Opinion 03/2014).

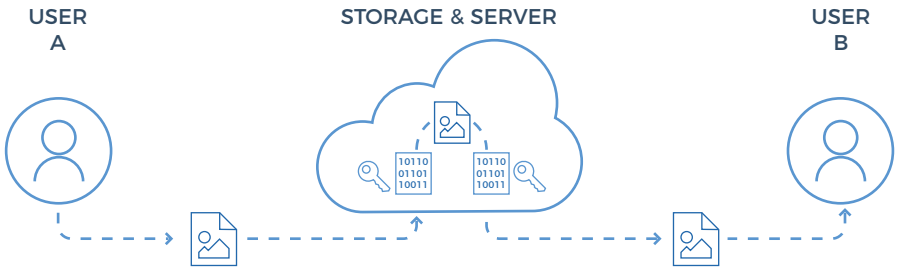
> *"In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design."*
>
> ***Marju Lauristin, Member of the European Parliament***

3. End-to-end encryption is the way to go

The GDPR will not specify or suggest what type of applications and their algorithms will thoroughly comply. Therefore, to ensure identification of a person or leaked data sets reidentification, encryptions keys' management is crucial. By using end-to-end encryption with the client side key management, will hold a significantly stronger protection of private data.

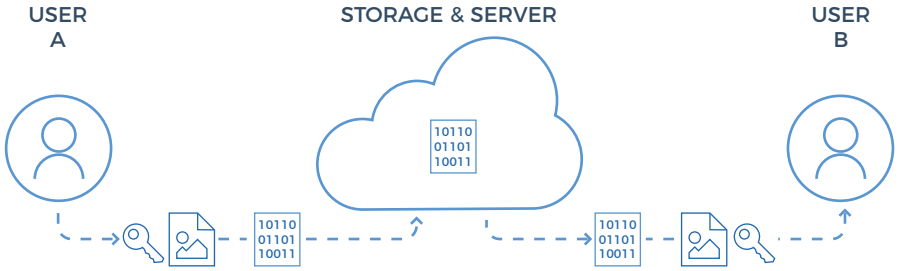
Pitfalls of server-side encryption

By using channel & at-rest encryption cloud providers or administrators, will have access to the encryption keys because they are stored on servers in an unencrypted format. In this case, if data sets are leaked or data breach occurs, it is technical possible to decrypt or identify persons and their sensitive data.



Advantages of End-to-end encryption

By using end-to-end encryption, neither cloud providers nor system administrators can access encryption keys. The keys and user data are encrypted on a client side and only encrypted data are stored on a server side. Thereby, end-to-end encrypted cloud storage providers, such as Geens, can never access or decrypt users data. If data breach happens on a server side, to identify encrypted users data is impossible to realize. Only encrypted data sets can be leaked. The content itself - as the most vulnerable data part - stays encrypted so no one can read it. Thus, your company's personal data and your clients data will remain safe and still private.



GDPR compliance and end-to-end encryption advantages

Easier GDPR compliance. Your data details stay protected inside the company and its controlled environment, even in cases of data leakage.

Saving cost of data leakage notifications or huge penalties. There is no need to inform your clients or employees if confronted with a security incident resulting in a breach of confidentiality, availability or integrity. It does not pose a high risk to those individuals affected. Your data are unidentified all the time.

Currently, end-to-end encryption is the strongest data protection technology to increase trust for your services, keep your company's, clients or users data confidential and secure, and comply with the GDPR regulations.

Risk reduction in case of a data leakage or breach. GDPR recommends to apply encryption and this approach can reduce your company's liability.

What is personal data?

The GDPR only applies to personal data. Personal data is any information related to an identified or identifiable living individual ("data subject"). Examples: a name and surname, home address, email such as name.surname@company.com, identification card number, location data (such as the location data function on a mobile phone), IP address, a cookie ID*, advertising identifier of your phone, data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

Examples of data not considered personal data: a company registration number, email address such as info@company.com, anonymised data.

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 longer than necessary.

**In some cases, there is a specific legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).*

How does end-to-end encryption protect personal data?

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

About Geens.com NPO

Geens.com - operating from Belgium - is a nonprofit membership organisation that provides information technology services to individuals, governments and businesses, governed by a legal and ethical data protection control. The platform lets the users save their private digital information securely and share the information to anybody else only on their own will and benefit. Geens refers to 'genes', given the fact that our genome data contain even more of our private data then we could ever imagine. As such, the platform focuses on personal records that should be owned and kept by our members, encrypted offline and online. Empowering patients, consumers or providers becomes a reality.

Geens is an NPO organisation that provides white-labelled secure and private login in combination with data services. Geens solutions can be integrated in a variety of e-products. Data benefits and income from personal information return to the members. Geens.com makes the core from private and secure e-experience.

Is Geens already compliant?

Geens operate under the "zero knowledge" principle which does not allow our admins to see our users data or recover encryption keys or passwords and because of this we can guarantee a higher level of privacy and security than traditional cloud service providers. Geens as NPO organisations will be compliant with GDPR from 25 May 2018 together with ISO27001 certificate.

Testimonials

"Protecting our private data is in the fast expanding digital world of key importance. As trust is a cornerstone for progress, I am honored to support the initiative for an independent privacy platform and ecosystem in the geens.com NPO."

Herman Van Rompuy
First President of the European Council and former Prime Minister of Belgium

---

"I am impressed with the ambition of the geens.com initiative. I have been fortunate to follow the progress of this new ecosystem. It had been built from the bottom up. It will give privacy back to the internet users. As a Chairman of KU Leuven, according to Reuters Europe's most innovative university, I want to express my strongest support and look forward to the first privacy guaranteed applications."

Herman Daems
Belgian Economist and Professor Emeritus KU Leuven (Belgium) / Groningen (The Netherlands). President of KU Leuven University and the Bank BNP Paribas Fortis

Relevant GDPR articles and Geens end-to-end encryption technology compatibility

Article 6. Lawfulness of processing
4. 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:

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

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, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Article 32. Security of processing
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, 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:

(a)the pseudonymisation and encryption of personal data;

Article 34. Communication of a personal data breach to the data subject
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) 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;

GDPR articles state that end-to-end encryption is a reasonable choice to protect sensitive data. Data collectors are obliged to process data by protecting it in a compatible way like encryption.

Since end-to-end encryption of the data is done on the client side and only then uploaded to the Geens cloud or server, the encryption keys always stay at the user side. Meaning that the user remains responsible for his own actions, whereas your organisation will be considered as making its best efforts to ensure protection of the data.

Geens is using industry standard cryptographic algorithms: symmetric encryption AES and asymmetric RSA.

None of the third parties could access end-to-end encrypted data, therefore, data controller will comply with the Article 32.

Under accident of data leakage when using end-to-end encryption where identification of personal data is impossible, companies don't have to notify users.

Geens can help any company or organisation to set up data protection processes with end-to-end encryption core.

- Data management features: file permission control, DRM, file termination control, file and user availability control
- Blockchain timestamping for documents and proof of existence
- Geens API - Integrations capabilities into third party services;
- Deploy Geens on your own servers for a maximum control.

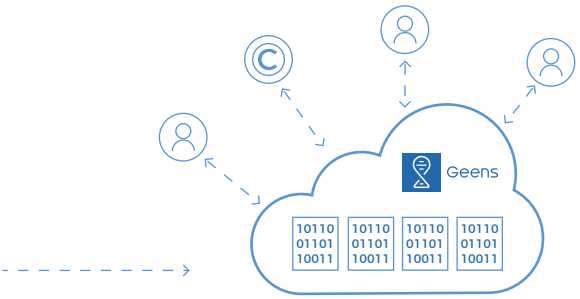
Geens end-to-end encryption technology assessment in your business

Geens.com

Web based end-to-end encryption using geens Geens Cloud.

Use as it is https://geens.com/app

Reach out for custom approach
info@geens.com

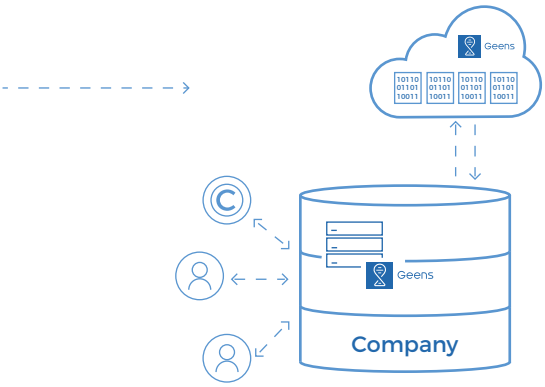


Geens on-premises

Deploy Geens Admin panel on your preferred servers.
Control data access and manage users of your company.

Support and monitoring of Geens platform

Reach out for custom approach
info@geens.com



The information contained in this document is not legal advice and is for informational and educational purposes only. We hope that you will find the information informative and useful, and we would be delighted to speak with you to answer any questions you may have about our organisation and solutions.

Learn more about Geens NPO at: www.geens.com