EU General Data Protection Regulation – Are you prepared?

Claudia Kressin · 2017-08-28

This is a general introduction article to the broad range of topics about General Data Protection Regulation (GDPR) affecting almost every company using Elasticsearch. It is the first post of a series with more coming up regularly showing what GDPR is about, how it affects your Elasticsearch cluster and how Search Guard can help you be compliant.

> At the time of writing this article, there are only 277 days and a few hours left for securing data in your company according to EU General Data Protection Regulation.

The EU GDPR has been constituted to homogenize European data protection regulations. It has an impact on **any company worldwide** with revenue-generating processes based on using personal data of EU citizens. This is because GDPR protects data of every EU citizen, no matter where in the world the data is processed and stored. And GDPR protects a broad variety of types of data!

GDPR is officially released since April 2016. After a two-year transition phase, the date of enforcement is May 25 in 2018. Other than most EU regulations GDPR is in effect without undergoing ratification of the EU member states first. In short, it is all about improving protection of data people assume to be private and personal.

The GDPR is not rewriting data protection completely but adds regulations to better protect the fundamental rights and liberties of EU citizens, by giving them back control over their personal data.

© 2026 floragunn GmbH · search-guard.com

The basic rules for handling data are

- Rightfulness & the principle of utmost good faith
- Transparency
- Appropriation
- Minimization & restricted storage
- Accurateness
- Integrity and privacy
- Accountability

Expanding on the rules of previous data protection regulations like 95/46/EG, the area of the application now includes the location of the marketplace. This means personal data processed in the European union is affected, such as data related to offers of goods or services: If a company is collecting individual level customer data, and/or has processes where such data is running through to create revenue, it needs to take extra care of this data.

Sanctions are very high. They can grow up to 20 million Euro or 4 percent of the total worldwide annual turnover of the preceding financial year of the organization, whichever is higher. Large multi national companies are treated as one.

Compliance to EU-GDPR is achieved by:

Consent

Companies need to prove that consent to processing personal data has been given by the user via Opt-In, prior to any processing. Existing consents must be obtained again if they do not comply with the new conditions.

Information rights

Users have the right to get informed about which data is being stored and how it is being processed. Individuals can ask for their data to be changed. And they can request all their data to be provided in a commonly used file format, in order to be transferred to another party.

Limitation to intended purposes

Companies need to make sure that personal data is only stored and processed to the extent where it is necessary to the explicit purpose for which the data was originally collected. Individuals can restrict processing their data to certain purposes.

Withdrawal of consent

Companies have to dele personal data immediately on withdrawal of consent. Third parties must be informed and prompted to remove any copies of that data. Generally, data shall not be stored longer than it is necessary.

© 2026 floragunn GmbH · search-guard.com

Handling of data breaches

What does breach mean? For example, if data gets disclosed (like reaching an incorrect recipient), this is considered a breach. As well is theft of data, failure to access or edit data and failure to delete data properly. GDPR rules that data protection authorities, as well as the affected users, have to be notified promptly and within 72 hours about any such breach.

Any company that has individual level customer data inside an elastic search cluster is affected. Because these new rules apply to transparency and information requirement next to an increased strictness for collecting and holding data.

We strongly recommend familiarizing with the terms of GDPR compliance. As a first step adding security to your Elasticsearch cluster is the least you can do. As stated in the General Data Protection Regulation Encryption is considered sufficient for protection. However, compliance is only achievable if you make sure encrypted data can be searched, indexed and correlated.

Photo: shutterstock / Ink Drop

This article was published on the Search Guard blog: https://search-guard.com/blog/eu-gdpr-elasticsearch/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial