Search Guard provides GDPR compliance for Elasticsearch

Jochen Kressin · 2018-02-14

The General Data Protection Regulation (GDPR) is coming. The goal of GDPR is to give individuals (data subjects) better control over their *Personally Identifiable Information (PII)*. GDPR considers any data that can be used to identify an individual as PII. It grants data subjects extensive rights over their data. For example, GDPR mandates affirmative consent for data processing which must be “freely given, specific, informed and unambiguous.”. At any time data subjects can demand information on what data is stored, for what purpose it is used, and who has access to it. Clearly, GDPR requires companies handling EU citizens’ data to undertake major operational reform.

The Search Guard compliance features are specifically designed to help companies meet the requirements of Chapter III – Rights of the data subject (Articles 12-23), and most are also applicable for chapters I, II, IV, and IX.

Data in transit is TLS encrypted. Always.

Documentation: https://docs.search-guard.com/latest/configuring-tls

Search Guard provides TLS encryption for node-to-node traffic, REST traffic, and Transport Client traffic. We support TLS via the Java Cryptography Extension and also OpenSSL, which gives you peak performance and modern and highly secure cipher suites. Your sensitive data is always safe as it travels across the network: TLS makes sure nobody can sniff or tamper with your data, and that only trusted nodes can join your cluster.

How does this help you to be compliant?

You'll meet requirements of Art.6 4.(e), Art.32 1.(a), and if you add encryption to data at rest, meet requirements in Art.34 3.(a).

Article 6 – Lawfulness of processing 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), 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 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 subject3. 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**;_

For general requirements on **encryption** see also Recital (83 – Security of processing):

In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as ***encryption****.*

Role-based access control secures all data on index level.

Documentation: https://docs.search-guard.com/latest/authentication-authorization

Search Guard offers role-based access to your data on index level. You can apply fine-grained permissions to any index, which means you have to full control over what a user can and can't do. We support a wide range of pluggable, industry standard authentication modules to choose from, for example Active Directory, LDAP, Kerberos, JSON web token, HTTP Basic or PKI based authentication. You can combine these modules and with the Enterprise Edition even write your own implementation.

How does this help you to be compliant?

You'll meet requirements of Art.5(f) and Art.32(2).

Article 5 – Principles relating to processing of personal data 1. Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against ***unauthorised*** *or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or* organisational *measures ('integrity and confidentiality').*_Article 32 – Security of processing2. In assessing the appropriate level of security account shall be taken in particular of the risks

that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, **unauthorised** disclosure of, or access to personal data transmitted, stored or otherwise processed._

For general requirements on **unauthorized access** see also:

Article 4, Definitions (12): 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, **unauthorised** *disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

Further references:

- *Recital 39 about Principles of data processing*
- *Recital 49 about Network and information security as overriding legitimate interest*
- *Recital 75 about Risks to the rights and freedoms of natural persons*
- *Recital 83 about Security of processing*
- *Recital 85 about Notification obligation of breaches to the supervisory authority*

Visibility of data is protected all the way down to field level

Documentation: https://docs.search-guard.com/latest/document-level-security

Document- and field-level security provide very fine-grained control over which documents and fields a particular user is allowed to see. Document-level security (DLS) means filtering out records from a search result based on the role of the user. Field-level security (FLS) means including, excluding or masking fields.

How does this help you to be compliant?

You'll meet requirements of Art.14 3.(c), Art.15 1.(c), Art.19, Art.30 1(d) and Art.32(2)

*Article 14 – Information to be provided where personal data have not been obtained from the data subject 3. The controller shall provide the information referred to in paragraphs 1 and 2: (c)if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed._*Article 15 – Right of access by the data subject1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, **access** to the personal data and the following information:(c)the recipients or categories of recipient to whom the personal data have been or will be **disclosed**, in particular recipients in third countries or international *organisations*;_

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing The controller shall communicate any rectification or erasure of personal data or ***restriction*** *of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been* disclosed, *unless this proves impossible or involves* disproportionate *effort. The controller shall inform the data subject about those recipients if the data subject requests it.*

Article 30 – Records of processing activities 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall

contain all of the following information: (d)the categories of recipients to whom the personal data have been or will be ***disclosed*** *including recipients in third countries or international* organisations;_Article 32 – Security of processing2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, *unauthorised* **disclosure** of, or access to personal data transmitted, stored or otherwise processed._

For general requirements on **protected data** see also:

Article 4, Definitions (9): 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Further references:

- *Recital 61 about Time of information*
- *Recital 62 about Exceptions to the obligation to provide information*

Search Guard's audit log module keeps track of all user activity in your cluster.

Documentation: https://docs.search-guard.com/latest/audit-logging-reference

Audit logging enables you to track access to your Elasticsearch cluster, log security and compliance related events, and provide evidence in case of an attack or breach. Search Guard can record events on REST and transport level, and tell you precisely which queries users execute on what indices. For further analysis the audit events can be stored in an Elasticsearch cluster, a SIEM system like SIEMonster or ArcSight, or an off-premise service such as Logsense, so malicious hackers won't be able to cover their tracks.

How does this help you to be compliant?

You'll meet requirements of Art.19

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

For general requirements on **monitoring activities** see also:

- *Recital 85 Notification obligation of breaches to the supervisory authority*
- *Recital 87 Promptness of reporting / notification*
- *Recital 88 Format and procedures of the notification*

Read- and write history audit trails record access and changes to your data

Documentation: https://docs.search-guard.com/latest/compliance-read-history

Search Guard can generate a read history audit trail so you can track what documents and fields have been accessed, when they have been accessed, and by whom. The write history audit trail records when a document has been created, changed or deleted. With this two features you can monitor all read- and write access to PII documents in Elasticsearch.

How does this help you to be compliant?

You'll meet requirements of Art.30 1,2,3,4

*Article 30 – Records of **processing activities** 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information (see a – g). 2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing (see a – d). 3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. 4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.*

*Article 17 – Right to **erasure** ('right to be forgotten')*_1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay [...]_

For general requirements on **recording changes** see also

*Recital (82 – Record of processing activities): In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for **monitoring those processing operations**.*

Where to go next

- Download and install the Search Guard compliance features
- Learn more about the read history audit trail by studying the official docs
- Learn more about the write history audit trail by studying the official docs
- Become a Search Guard Vanguard by answering the compliance survey

Sources:

- https://eur-lex.europa.eu
- https://gdpr-info.eu
- https://www.british-assessment.co.uk/wp-content/uploads/2017/07/GDPR-ISO-27001-Mapping-Table-2.pdf

Photo: shutterstock / SB_photos

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