Lepide

Mapping the Lepide Data Security Platform to **GDPR Articles**

What is the GDPR?

What is the General Data Protection Regulation?

The European Parliament adopted the regulation on GDPR on 27th April 2016, and it came into effect from 25 May 2018. After becoming effective, it replaced an old data protection regulation (Directive 95/46/EC of 1995). Under the law, businesses are required to protect the personal data and privacy of EU citizens for transactions within EU member states. It also regulates the process for when a company exports the personal data of EU citizens outside Europe.

What Type of Data is Covered?

Personally Identifiable Information (PII), or any personal data. These include, but are not limited to, names, addresses, phone numbers, account numbers, email and IP addresses.

Who is Affected?

Any company that collects the data of EU citizens, regardless of the geo-location of that company.

What are the Penalties?

One of the most talked about elements of GDPR are the fines that apply to businesses that don't comply. The level of fines being imposed has increased to up to 4% of an organization's turnover as the maximum fine and 2% of an organization's turnover for less serious offenses.

Summary of the New Requirements

Privacy by Design - This is a legal requirement of GDPR in which companies will have to consider data privacy during all the design stages of the projects. Everything related to the privacy of personal data should be taken into consideration to control their storage and accessibility.

Data Protection Impact Assessment - Companies will have to first analyse the risks to their privacy when certain high-risk or sensitive data associated with subjects is to be processed.

Right to Erasure and To Be Forgotten –The GDPR extends an already existing right that consumers have to have their data erased to include digital data. Essentially, consumers have the right to stay out of the public view and "to be forgotten".

Extra-Terrestrial Scope – GDPR applies to controllers and processors, both outside and inside the EU, who handle data generated in the European Union. All businesses offering goods and services to those within EU are subject to the regulation. So even if Britain opts out of European Union, the businesses located there may still have to stay compliant with GDPR.

Breach Notification – When a security breach occurs, it the responsibility of the organization to report it to all customers and stakeholders. They will have to notify the concerned authorities within 72 hours of discovering the breach.

Mapping GDPR Articles to the Lepide Data Security Platform

Article	What it Means	Technology Alignment
25 – Data Protection by Design and By Default	Embrace accountability and privacy by design as a business culture.	Analyze user and entity behavior, spot anomalies, track file and folder modifications and spot permission changes to help implement data-protection principles, such as a policy of least privilege.
30 – Records of Processing Activities	Implement technical and organisational measures to properly process personal data.	Discover and classify your sensitive data, determine who has access to it and set up detailed auditing so that you have a record of exactly what is happening to the data. Get alerts on suspicious activity/behavior.
17 – Right to Erasure and "to be forgotten"	Be able to discover and target specific data and automate removal.	Identify, discover and classify sensitive, personal data, so that you can easily adhere to subject access requests and requests for data erasure.
32 – Security of Processing	Ensure least privilege access; implement accountability via data owners; provide reports that policies and processes are in place and successful.	Reduce risk through the identification of users with excessive permissions. Govern access to data and implement a policy of least privilege. Get alerts when permissions change that may create unnecessary risk to data.
33 – Notification of personal data breach to the supervisory authority	Prevent and alert on data breach activity; have an incidence response plan in place.	Use Lepide to detect breaches involving personal data. Generate pre-defined reports and real time alerts that will enable you to react quickly and take the correct information to the supervisory authority.
35 – Data Protection Impact Assessment	Quantify data protection risk profiles.	Take a data risk assessment with Lepide to understand where your areas of data security weakness are and get actionable advice on how to strengthen them. Instantly see where GDPR breaches are likely to originate.

Meet GDPR Compliance with Lepide

Lepide uses data-centric audit and protection functionality to discover GDPR data, see who has access to it, analyze user behavior and ensure the surrounding environment is secure. With hundreds of pre-set reports related to GDPR specific requirements, you'll be able to quickly and easily meet those GDPR audits and avoid potentially crippling fines.

Data Classification for PII

Discover, classify, tag and score data based on whether it is applicable under GDPR compliance.

Access Governance

Ensure that the only users able to access GDPR data are those that require access for their job.

Monitoring User Behavior

User behavior analysis, continuous monitoring and anomaly spotting for interactions with sensitive, covered data.

Start a Free Trial

Get a Demo

Get a GDPR Risk Assessment