THE GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is a guideline by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU) and to synchronize the present data protection laws of the EU member states. It also addresses the export of personal data outside the EU.

The new GDPR brings substantial changes and compliance challenges for organizations which process the personal data of individuals located within the EU. It governs how these organizations can collect, process, store, and transfer personal data. Companies have two years to comply with the GDPR. Beginning 25 May 2018, penalties may be levied for those who are not in compliance.

By the end of May 2018, companies need to have implemented appropriate technical and organizational measures and stand ready to demonstrate compliance. They are further obligated to review and update measures on an ongoing basis as necessary.

KEY REQUIREMENTS OF THE GDPR

- **Data privacy policies**: Organizations must post clear data privacy policies on their websites to explain to customers their rights and remedies.
- **Free and full consent:** Organizations are required to obtain explicit consent from data subjects prior to collecting data, as communicated by a statement or clear action. Data subjects must be able to withdraw consent at any time.
- **Notification of data breaches**: Organizations must notify authorities of data breaches within 72 hours of discovery and keep records of all breaches. Data subjects must be notified of any breaches affecting their unencrypted personal data.
- **Expanded rights for data subjects**: Organizations must delete customer data upon request ("the right to be forgotten") and allow customers to transfer their personal data to another provider.
- **Data impact assessments**: Organizations that execute "high-risk" data processing will be required to conduct data impact assessments to identify privacy risks to data subjects and determine appropriate safeguards.
- **Data protection officers (DPOs):** Organizations processing Europeans' data "on a large scale," including US companies, are required to appoint a Data Protection Officer.

For more information see: http://ec.europa.eu/justice/data-protection/

CERTIFICATION FOR THE GDPR

A certification mechanism to prove that a certain data protection standard has been met, is planned but still in development. Certification will come as a seal (probably) called the 'European Data Protection Seal' and will be provided by the national authorities.

WHAT YOU CAN DO TO PREPARE NOW

Regardless if you use ZyLAB in an on-premises environment or if you use ZyLAB from one of our partners or ZyLAB SaaS providers, you can already start preparing yourself.

Locate your data and know what is in it

An effective path to GDPR compliance begins with assessing what data you have, where it is located and knowing what is in that data. ZyLAB's software uses the latest techniques from Artificial Intelligence and Data Science to identify and classify information, even in documents that are "non-searchable" like images, ZIP, PST or MSG and other container files. Information then categorized in clear overviews so you have direct insight into what data is obsolete and can defensibly be deleted and what data needs to be secured.

Protect your data

ZyLAB provides the most advanced tools for auto-redaction or anonymization, which allow you to redact personal and sensitive data before disclosure to comply with the GDPR. Using advanced pseudonymization allows you to protect sensitive and confidential information, but keep the flexibility to disclose information later if needed or wanted.

For more information: https://zylab.com/resources/ebooks/critical-technology-era-gdpr

Additional information GDPR and Privacy if you use a ZyLAB cloud deployment

If your ZyLAB ONE eDiscovery runs on Microsoft Azure (US and EMEA), you are able to select a data center and keep your data in your own jurisdiction.

Microsoft designed Azure with industry-leading security measures and privacy policies to safeguard your data in the cloud, including the categories of personal data identified by the GDPR.

Read more about the GDPR requirements and Microsoft Azure: *https://www.microsoft.com/en-us/trustcenter/privacy/gdpr#GDPR-requirements*

If your data is hosted by Interoute B.V. (EMEA), then you can find more on their privacy policy and measures taken for GDPR here: http://www.interoute.nl/privacy-policy

ABOUT ZYLAB

ZyLAB provides SaaS services through the following entities. Please provide your provider should you have more questions on GDPR and ZyLAB's SaaS solutions.

ZyLAB Headquarters United States

Servicing the North America region

ZyLAB DCS USA LLC
7918 Jones Branch Drive
McLean, VA 22102
United States of America

ZyLAB Headquarters EMEA & APAC

Servicing the Europe, Middle East, Africa and Asia Pacific regions

ZyLAB eDiscovery & Compliance Services (DCS)
Laarderhoogtweg 25
1101 EB
Amsterdam, The Netherlands