Understanding the EU General Data Protection Regulation: An Exhaustive Guide

GDPR or the General Data Protection Regulation comes across as one comprehensive overhaul that replaces the obsolete European Data Protection Legislation, functional since 1995. With varied data security implementations being done away with— first time ever in the last 20 years— this harmonized regulatory framework is expected to be a significant addition to most IT-specific organizations since the corporate-specific Sarbanes-Oxely Act of 2002.

What is GDPR?

GDPR is a cohesive, industry-specific implementation that aims at strengthening, protecting and unifying the confidentiality of the citizens. Synonymous to the European Union, the GDPR will streamline the safety regulations implemented by the companies via a single regulatory measure. Put simply, this approach will get rid of the fragmented data protection guidelines by opting for a more unified approach towards the privacy rights. GDPR will be actively implemented from 25th of May, 2018.

Proposed Highlights and Reforms

1. GDPR expects the concerned companies to inform the National Supervisory Authority about the breaches and hacks. Any kind of risk to user confidentiality needs to be communicated with urgency.
2. Companies falling under the EU GDPR hierarchy must comply with the general guidelines without fail.
3. A Pan-European policy regarding data protection will be holistically implemented. GDPR is expected to knit the entire European contingent with one cohesive law.
4. A 24-72 hour deadline for notifying the authorities seems to be a plausible consideration, especially when the compliant organizations are considered.
5. GDPR considers compliance from companies that actively or passively handle the confidential details of the EU citizens while impacting the EU market in any possible manner.
6. GDPR brings forth data protection by default and data protection by design— each drafted for safeguarding the existing services and products via a host of privacy-friendly norms and settings. This way companies will surely have to depend on third-party services for implementing the changes— right from the initial stages.

GDPR, in the truest possible sense, strengthens the data protection laws by making it compulsory for businesses to abide by the guidelines and offer solutions for adequately protecting personal data of the subjects. When it comes to the types of records evaluated under the GDPR guidelines, organizations must cover everything that directly or indirectly defines confidentiality. Anything related to the company records, staff details, customer history and client database must be taken within the scope of GDPR. Moreover, GDPR also highlights the modus operandi of data security and protection— spanning across the European Union, followed by a host of compliance guidelines— mandatory for the concerned enterprises.

GDPR Compliance: The Expectations

Based on the Article 32, the data processor and controller must take the responsibility of implementing technical and even organizational measures for ensuring adequate levels of safety measures. This puts multiple companies under the compliance radar with authorities expecting them to abide by certain guidelines, synonymous to the GDPR implementations.

1. The first measure or rather expectation happens to be the encryption of customer data as postulated within Article 32, GDPR.
2. Concerned organizations must ensure confidentiality, availability and integrity of services, pertaining to the data subjects.
3. In addition to that, the basics of compliance require the enterprises to restore data access and availability to the consumers— in case of a technical or physical incident.
4. Organizations must also comply with the disaster recovery basics which include password recovery and the likes of key management strategies.
5. Companies, falling under the EU GDPR radar must conduct regular tests and assessments; thereby keeping a close eye on the organizational and technical measures which are being implemented.
6. Based on the Article 333 of the GDPR act, the supervisory authority must know about a breach within 72 hours and any reason for delay must be justified by the concerned organization with valid evidences.

Risks and Penalties for Nonconformity

Article 83, General Data Protection Regulation discourages offenders or rather the noncompliant organizations.

1. Basic acts of noncompliance attract a penalty of 10000000 EUR or 2 percent of annual global turnover— depending upon whichever comes out to be higher.
2. Major breaches are subject to 20000000 EUR as administrative fines or 4 percent of the annual turnover— as calculated above.

In addition to these penalties, authorities are also chalking out other options which are expected to show up in a year or two. Nonconformity is a serious issue and has to be nipped in the bud. Moreover, enterprises which aren't willing to accept the compliance rules must be handled differently. It needs to be understood that every regulation synonymous to the GDPR aims at safeguarding and securing the customer data. The likes of cyber-attacks and ransomware threats have had a major impact on the psyche of the consumers and therefore it is only appropriate to address the issues beforehand. Companies facing cyber threats have the physical and financial reservoirs to bounce back but it is the data subjects which are often compromised, in the long run. GDPR or General Data Protection Regulation aims at amplifying the privacy measures and data protection guidelines pertaining to the European Union and we are only a few months away from witnessing a path breaking implementation.

Bottom-Line

Based on the Article 5 of GDPR, appropriate security standards for identifiable and personal data are of massive importance. Moreover, Article 32 states that encryption is one way of achieving the same. Although these clauses and sections are biased towards the data subjects, it is exceedingly important for the organizations to stay vigilant with their security standards. Any act of negligence or procrastination can attract heavy penalties, as stated within the GDPR rules and regulations.

Make your enterprise GDPR ready with Seqrite

Objective	How Seqrite helps to achieve these objectives?
Data Security and Protection	1. Seqrite Encryption helps to keep the data secure by encrypting entire contents of the disk. It can encrypt entire contents of Hard Disk and Removable Devices.
Data Loss Protection	1. Seqrite Endpoint Security (EPS) enables organizations to enforce control over the user of various devices which are getting used within the organization. Organizations can block access to various types of devices such as USB, Wi-Fi, bluetooth, printers, and mobile phones. 2. DLP helps to establish control over the Data in use and Data at Rest. It enables to define certain policies to classify and protect confidential and critical information, so that end users cannot accidentally or maliciously share data which may put the organization at risk. 3. Seqrite DLP monitors data which is getting transferred through removable devices, Network Share, Clipboard, Printer and various other applications. It monitors certain file types such as document files, confidential data such as credit card information, SSN(Social Security Numbers), Passport, etc. and also enables organizations to create their own dictionary of confidential data.
Data Protection from Ransomware	Ransomware encrypts the data on endpoints. Seqrite Anti Ransomware feature offers protection from ransomware attacks and also keeps a backup of user data on each endpoint.
Data Protection When Device is Stolen	Seqrite Endpoint Encryption has a capability to encrypt entire contents of your Hard Disk and Removable Disk. In case your device is lost/stolen, data on the device is still not accessible to anyone.
Alerts, Notifications, Reports	Real time Email and SMS alerts are sent to defined groups if an attempt to violate policies is detected. Detail reporting helps to track data leakage and further improve DLP policies.

Quick Heal Technologies Limited
Corporate office: Marvel Edge, Office No. 7010 C & D, 7th Floor,
Viman Nagar, Pune - 411014, India.
Support Number: 1800-212-7377 | info@seqrite.com | www.seqrite.com