Prepare Now for EU General Data Protection Regulation (GDPR)

Senior executives across the EU and around the globe need to be asking: Is our organization ready to meet the new GDPR data privacy mandates?

GDPR Explained

The GDPR gives EU citizens and residents control over their personal data. It broadly defines personal data as any information that can be used on its own or with other data to identify an individual. With permission, an organization can use the data, but each person owns their personal data and can withdraw the right of an organization to use that data. An EU resident can monitor the use of their data, decide who can access it, and can demand its return to them.

Organizations need to begin to put in place policies, procedures and technologies now to ensure they can protect the personally identifiable information (PII) of EU citizens and residents ahead of the GDPR May 25th, 2018 deadline. That is not a lot of time given the complexity of GDPR requirements and the size of fines for GDPR compliance violations: 4% of global revenue or €20 million whichever is greater. In addition to large potential fines, other significant provisions of the GDPR include:

- Companies or public entities with more than 250 employees must have a Data Protection Officer who is personally liable for PII data breaches.
- If a material data breach occurs, companies have 72 hours to notify authorities of that breach.
- Any organization located anywhere in the world doing business with EU residents must comply with GDPR rules.
- GDPR rules apply not just to companies collecting PII, but to any affiliated companies, such as subcontractors, vendors, or distributors, who have access to that PII.
- Consent needs to be obtained from EU citizens on the use of their personal data.

Teleran's Data Protection and Compliance Software Enables You to Be GDPR-Ready

Monitoring, auditing and controlling access and use of PII is critical to comply with GDPR and other personal data protection regulations around the world. Huge amounts of PII is stored and processed in hundreds or thousands of relational databases and applications in organizations today. To establish where GDPR gaps exist, organizations need to start assessing their PII: where does it reside, who is using it, how is it used, and is it appropriate use according to GDPR mandates.

Teleran's best-in-class Data Protection and Compliance solution can help with critical GDPR gap assessments and with addressing five essential GDPR data protection requirements described below. Teleran's software discovers and classifies PII and continuously monitors access and use of PII. It delivers a "fact-based" process that identifies exactly where a company's GDPR compliance risks and liabilities exist and what actions are required to bring their PII processing into compliance. Teleran's real-time alerting, access controls, and detailed audit reporting meet mandatory GDPR impact assessment, security, audit, incident response, and breach notification requirements.

Addressing Key EU GDPR Challenges

What follows are descriptions of five of the most challenging GDPR requirements and how Teleran enables your organization to prepare for and meet these challenges.

Data Protection Impact Assessment – Article 35

The GDPR stipulates that organizations must initially and regularly assess the privacy risks to individuals when processing their personal data. The purpose of the assessment is to identify PII and audit the use of PII to determine if it is in compliance with GDPR requirements. If the use is not in compliance, remedies must be applied to document and attest to compliance prior to the May 2018 GDPR deadline.

Teleran addresses by:

- Identifying PII and auditing who is accessing PII to document GDPR compliance and identify any compliance violations that need to be remediated.
- Applying appropriate data access control policies to protect PII and ensure GDPR compliance.

Purpose Limitation – Article 5-1 (b)

One of the essential principles of the EU data protection law is "purpose limitation" of the use of PII. It has two main elements: The use of personal data must have an explicit purpose and the data must be used only for that stated purpose and no other.

Teleran addresses by:

- Monitoring and analyzing the access and use of PII to ensure it is limited to the stated purpose only and that no other unauthorized or non-compliant accesses are occurring.
- Establishing PII access policies to enforce purpose limitation. These policies can include only allowing specific applications and users to access and process the data and preventing all others from accessing the data.

Security – Article 5-1 (f)

According to this critical security GDPR article, PII must be processed in a manner that ensures its security and integrity, including protecting against unlawful use, manipulation, destruction or loss of the

data. Regular evaluation of data security measures through documented audits is another requirement of this article.

Teleran addresses by:

- Monitoring and controlling the access and use of PII to ensure it remains confidential and protected.
- Establishing PII protection policies to prevent: illegal use of the data, the manipulation or changing of the data, and the destruction or loss of the data.
- Delivering comprehensive data usage audit documentation.

Accountability and Documentation – Article 5-2

Article 5-2 defines a company's accountability in complying with GDPR. In addition, this article requires that the companies must "be able to demonstrate and document" their processes are in compliance.

Teleran addresses by:

- Providing demonstrable and fully documented PII access monitoring audit reports.
- Delivering PII access policy and testing processes to prove that the security measures are effective and GDPR-compliant.

Breach Notification – Articles 33/34

Article 33 requires that the appropriate GDPR government authority be notified within 72 hours of a company becoming aware of a breach of PII data that is likely to result in risks to the rights and freedoms of EU citizens. Article 34 pertains to notifying the EU citizen or resident of the data breach. In this case "owners" of the data need to be notified without delay, but the 72 hour notification period does not apply.

Teleran addresses by:

- Identifying and alerting staff to suspected or actual data breaches, in which case further investigation of the suspected breach can occur using Teleran's forensic audit reports.
- Documenting the breach activity for purposes of notification and preventing further breach activity or future non-compliant activity.
- Applying additional real-time access control policies to prevent future breaches of this nature.

Schedule Your GDPR PII Readiness Assessment with Teleran Now

Under the GDPR it is essential to demonstrate that your PII data is protected. Begin preparing now for GDPR compliance with a Teleran GDPR Readiness Assessment. The assessment identifies where sensitive structured data resides, who is using it, how is it used, and is it appropriate use according to GDPR mandates. In addition, to further minimize your risks as well as lower your data handling costs, the assessment can assist in updating your data archiving and retention policies, identifying unused or "dormant" data and archiving it to reduce your compliance liability and lower your organization's data processing and storage costs.

For more information on Teleran's Data Protection and Compliance Solution visit www.teleran.com or call +1.973.439.1820.