PARABLU

Regulation: GDPR Readiness: 3-step guide to GDPR compliance

Beckoning the new era of data privacy, General Data Protection Regulation, the first major reform in data protection regulations in 20 years, will now dictate radical changes to the way digital businesses treat the private information of their subjects.

In first, the new rules, as directed by the EU commission, not only exert strict restriction on the kind of data that can be collected and processed, GDPR grants unprecedented authority to the citizens of the Union on how their data is organized, right down to the explicit choice of being 'forgotten', should such a need arise. Read more: GDPR Key changes. And businesses everywhere are required, by law, going forward, but to comply with such demands and fast.

GDPR Readiness

While the rules and mandates are clear, clarity around what must businesses actually do to be deemed 'GDPR-compliant' is still poor. Tech giants like Google and Amazon can already be seen taking GDPR-required steps to compliance – asking user's explicit consent on what data they'd want to share with their products, such as Gmail, and improving encryption on their cloud storage service. However, many are still scrambling to figure the next best steps.

The difficulty is partly because GDPR has enterprise-wide bearings. Every function, from IT to supply chain to human resources comes under the ambit of the regulation's scrutiny.

And with 99 constitutional articles to follow and abide by, instituting relevant action plans to help identify, assess and upend the old ways of data management – from consent forms to data management applications -can feel like a slog.

The goal of this post, therefore, is to help you understand how to build security-first business practices and how to go about it.

3 steps to GDPR Compliance

On the face of it, in the event of a data rift, GDPR will require you to prove compliance and that you are in a position to prevent a breach, ensure backup and restore data upon request in the event of a data disaster.

To this effect,

1. Start with a Privacy Impact Assessment

This is a standard way for most IT-enabled organizations to identify and reduce privacy risks of a process, end to end. While PIA is typically conducted (and now mandated under GDPR) for new projects or processes, privacy risks can be assessed for existing systems as well, as long as there is a realistic chance of implementing changes that may arise as an outcome of the PIA.

It is at this stage that you must ask,

- What is the nature of the data you collect and if it falls under some 'special category' as identified under GDPR?
- How is the data being collected and processed, and the applications involved?
- Is the data stored and accessed at a level of security apposite to the risks associated?

2. Create a well-documented GDPR Compliance Roadmap

Following an assessment of risks, document the findings and investigate any areas that may have been missed. Subsequently, review organizational policies and protocols around data privacy and protection. Identify gaps in data privacy and security controls to reduce the chances of being reprimanded for improper compliance.

- Verify vendor contracts to establish responsibilities and respective rights.
- Create and update data governance and data audit policies in keeping with the new rules
- Identify new vendors and technology to support the new data regulation policies
- Configure capabilities to regularly test and audit data governance policies and controls

3. Set up a Disaster Recovery Plan

Among other GDPR requirements, a disaster recovery plan is mandatory, bearing down on organizations to set in place controls and procedures that ensure safe backup and timely recovery of critical data in the event of a physical disaster. Article 32(1) of the new GDPR regulation states:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of the 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 organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.

(a) the pseudonymization and encryption of personal data, (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."

These warrants organizations to

- Identify and assess the present nature of data security and backup against GDPR mandates
- Pay special attention to recovery times objectives (RTO) and recovery point objectives (RPO)
- Procure secure cloud data encryption solutions for GDPR-compliant backup and restore.
- Configure capabilities to regularly monitor, test, and audit data protection controls for data being collected, data is backed up and data in other repositories.

For new-age organizations, GDPR, is in fact, an opportunity to refine business processes and build capabilities that strengthen the organization's overall defense against data rifts. In fact, embracing GDPR is in the best interest of everyone today, for EU-affiliated companies as well as those that may not yet be serving the EU subjects, since it sets the strong benchmark for data privacy as well as user rights.