GDPR COMPLIANCE ASSESSMENT

HITACHI
Inspire the Next

What is GDPR compliance?

The **General Data Protection Regulation (GDPR)** is a comprehensive data protection and privacy regulation that comes into effect on May 25, 2018. The member states of the European Union (EU) have long maintained strict legal provisions to safeguard the personally identifiable information (PII) collected online by businesses and organizations; and GDPR is a new legal means to unify and clarify these requirements.

The legislation applies to any company that collects the data of EU residents, regardless of its location. As a result, GDPR will have an impact on data protection requirements globally, especially as many countries will attempt to reach the adequacy status required to facilitate cross border data transfers.

Why is GDPR compliance readiness important?

Studies find that up to 20% of businesses still haven't taken steps to prepare for GDPR compliance. GDPR has created an urgent requirement for businesses operating within the EU, offering goods and services or marketing to EU residents to take privacy seriously. Organizations must take action in order to implement the required privacy principles and avoid the fines and penalties threatened by GDPR for non-compliance. In addition, non-compliance with GDPR requirements can result in reputational damages, risk of lawsuits, regulatory interventions, financial losses and operational damages.

RECOGNIZED AS KEY INNOVATOR IN DATA PRIVACY

Our unique approach to helping organizations achieve GDPR compliance was recognized by the research institution MarketsandMarkets, featuring Hitachi Systems Security as major player and key innovator in the data privacy field in the 2018 study "GDPR Services Market by Solution, Service, Organization Size, and Region – Global Forecast to 2023".

How does a GDPR Compliance Assessment help?

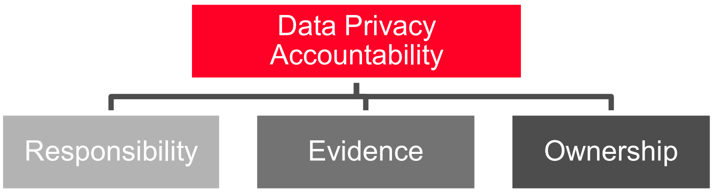
A GDPR Compliance Assessment is a personalized path towards compliance that provides you with a risk model and an ongoing privacy management framework. It can help organizations understand their privacy posture, the gap between their posture and the GDPR, the efforts that have already been implemented and can be reused, the available people, processes and technologies to conduct such an assessment as well as the risk appetite of the organization based on their level of data processing and data flows.

Benefits

- Understand the scope of the applicable GDPR requirements for your organization
- Identify gaps between GDPR requirements and your current privacy posture
- Get a tailored plan towards GDPR compliance with context-based risks considerations
- Reduce potential liabilities during remediation by identifying high risks to be prioritized
- Leverage efficient reporting to prepare for audits and certifications

A Structured Approach to Privacy Management

As part of our Professional Services offering, Hitachi Systems Security has developed a *Structured Approach to Privacy Management* that aims at implementing the desired technical and organizational measures to develop an ongoing capacity to comply with the GDPR. Based on the Enterprise Risk Assessment (ERA) Methodology, our approach is fitted for identifying areas of non-compliance and remediation measures given the risks associated for each and within the specific business context of our customers. The *Structured Approach to Privacy Management* is based on responsibility, evidence and ownership.



Data Privacy Accountability

Responsibility

Evidence

Ownership

Figure 1: The Elements of Data Privacy Accountability

Elements of a GDPR Compliance Assessment

Unless otherwise customized by the customer, a standard GDPR Compliance Assessment consists of four (4) distinct phases:

✓ Phase 1: Statement of Applicability

The Statement of Applicability is critical to review the specific regulatory context of your organization, establish your privacy obligations when it comes to GDPR compliance and identify a proper scope for phase 2, including resource requirements and realistic project timelines.

✓ Phase 2: Gap Analysis

The Gap Assessment aims at determining the baseline GDPR and privacy compliance, including resources that are already available internally, such as processes, technology, and tools. By identifying which technical or organizational measures are already *implemented* or *in progress*, organizations can evaluate the existing resources that can be re-used towards GDPR compliance,

✓ Phase 3: Risk Assessment

During the Risk Assessment, different departments of the customer organization are audited to find out what processes are the most risk-prone and must be addressed first for compliance with the GDPR and to avoid hefty fines in case of data protection breaches.

✓ Phase 4: Privacy Management and Accountability Handbook

The customized Privacy Management and Accountability Handbook serves as a map towards on-going compliance. We identify the areas which must be addressed in priority, outline the recommended controls and list the required accountability mechanisms to demonstrate compliance.

WANT TO LEARN MORE?

Check out our blog article “GDPR: Frequently Asked Questions”.