General Data Protection Regulation (GDPR)

Assessment Package for Nonprofits, Associations, and Foundations

Compliance with new **General Data Protection Regulation (GDPR)** could potentially require material changes to existing systems and policies and processes across multiple functional areas of your organization including legal, compliance, information technology, security, and third-party vendor management. This is especially important in the critical areas related to the gathering and management of personal data covered by these new regulations.

Fíonta's focuses on data stewardship as a key component of your organization. Our approach to organizational compliance with the GDPR combines assessment, gap analysis, planning, education, and change management to help ensure your organization both understands, and adheres, to the new regulations.

Our process starts with a combination of policy reviews, system reviews, data reviews, and interviews with key stakeholders within the organization. These actions are designed to surface all the areas where the management of, and access to, personal information is controlled and executed. Our team analyzes the information to identify gaps between organizational operations and regulation requirements. Where gaps exist, we provide potential solutions and, where applicable, estimates to mitigate issues.

What are the Goals of a GDPR Assessment?

A GDPR Assessment Project targets the following organizational goals:

- Assess existing information system environment and data assets
- Assess current structure and the key personnel roles within the organization
- Assess current policies and processes regarding data management
- Conduct a gap analysis to identify required changes
- Create a plan with best practice frameworks to implement changes

What is Required of My Organization?

Success of this project relies on an organizational commitment to compliance and a prioritization of data stewardship. To ensure success and accuracy, Fíonta requires the following:

- Executive sponsorship with the organization and/or from the Board of Directors
- Key stakeholder participation
- Honest and full disclosure of organizational structure, policies, procedures, and systems
- Access to systems where personal information is stored and/or accessed

How Does Fíonta Approach This Assessment?

1 Data Management

Being a steward of data for your organization requires ongoing maintenance and management to help ensure the proper protection of information and compliance with applicable regulations. Data stewardship, however, also provides immense benefits to your organization. Data is often an organization's most valuable asset and focusing on the integrity of that asset helps organizations generate revenue, measure impact, and further its mission.

Sources
Fíonta will review all the procedures and systems used to collect and store personal information. Our team will catalog these systems, evaluate the data collected, and assign a risk level based on the information being collected and practices being used to collect the information and how each aligns to the GDPR. The effort is proportional to the number of enterprise systems in use. Examples of enterprise systems include email, accounting, fundraising, association management, mass email, and marketing automation. We have "small" compliance projects for organizations with fewer than six
enterprise systems and "medium" compliance projects for organizations with between seven and 12 enterprise systems. Project plans for organizations with greater than 12 enterprise systems are custom.

Accuracy
Fíonta will conduct a data quality analysis of your information using data samples of various record types key within your systems. We focus on the analysis of select elements of data and their alignment with the accuracy rules in the GDPR.

2 Data Governance

Roles
Fíonta will review existing organizational roles and functions relating to data including data compliance and data security and protection. The objective is to document the required functions necessary to ensure current and continued GDPR compliance and that these functions are clearly assigned to named staff and present in documentation of job functions.

In our policy review, Fíonta will align existing policies to these roles appropriately and provide an analysis of gaps within the organization.

Policies
Fíonta will review the existing organizational policies in the following key areas and conduct a gap analysis to determine any required changes:

- General data governance policies
- Retention and backup policies
- Security controls
- Breach notification / incident response reporting
- Auditing / testing of controls

What is the Project Deliverable?

At the end of the assessment, Fíonta will deliver a compliance recommendation plan. This plan identifies issues surfaced during the assessment, assigns risk and urgency to each issue, and provides recommendations for remediation to ensure the organization becomes compliant and maintains GDPR compliance moving forward.

FÍONTA