NAVIGATE
Better Experience. Better Outcome.

GDPR COMPLIANCE CHECKLIST

IS YOUR ORGANIZATION GDPR COMPLIANT?

If your business collects or processes any personal data of citizens of the European Union (EU), the General Data Protection Regulation (GDPR) applies to you. Use this checklist to see what your organization should consider in the short and long term to be compliant with this new regulation.

SHORT-TERM COMPLIANCE ACTION ITEMS

☐ An Adequately Funded GDPR Compliance Program

Given the complexity of GDPR, taking a strategic and holistic approach to compliance is key, with defined roles, responsibilities, and a governance structure. Without proper funding and planning, your resources may be spread too thin and compliance may be delayed or not effectively maintained over time.

☐ Training & Awareness Programs

Providing your employees with adequate GDPR training is crucial to drive understanding of the regulation and their obligations when handling personal data. Remember, accountability is one of the core GDPR data protection principles.

☐ Documented Records of Processing Activities

Understanding what data you are collecting and how it is being processed is critical. If a data subject or data protection authority requests information, Records of Processing Activities will be a key resource to leverage.

☐ A Sustainable Complaint Management Process

Beginning May 25, you may experience an influx of data subject requests. Having a sustainable process in place will ensure that inquiries are efficiently triaged, tracked, and responded to.

☐ A Clear Understanding and Enablement of Data Subject Rights

Citizens of the EU will have greatly expanded rights and will be able to request specific actions related to their personal information. You need to understand these rights and your obligation to accommodate them.

☐ A New Approach to Breach Management

GDPR compliance requires new data breach policies and processes to be put in place, including reporting data breaches within 72 hours.

☐ Notices

Notices serve as a vehicle to provide transparency and further promote customer trust. Your notices should help inform all pertinent data subjects (i.e., employees, customers, applicants, vendors, etc.) how their data is being used and shared.

Wayne | Philadelphia | 484.383.0606 | RiskCompliance@navigatecorp.com

LONGER-TERM COMPLIANCE ACTION ITEMS

☐ A Consent Management Protocol

GDPR defines consent to collect and/or process data as being freely given, specific, informed and unambiguous, and a clear affirmative action. You will need to guarantee that your opt-in and opt-out activities meet the definition of consent, and that this consent is tracked and monitored.

☐ Data Protection Impact Assessments (DPIAs)

If you are processing "high risk data," GDPR mandates that you conduct Data Protection Impact Assessments. Higher risk data includes, but is not limited to, race and ethnicity, political opinions, religious beliefs, and health data.

☐ Embedded Privacy by Design

GDPR requires explicit recognition of the concepts of "Privacy by Design," meaning that data protection and security should be embedded into daily business processes across your enterprise.

Navigate teams with its clients to prepare them for GDPR and its wide-ranging impacts. We can help you assess your current GDPR readiness and develop an individualized strategy to manage and sustain compliance. Contact us to learn more.

CONTACT US TODAY TO GET STARTED

Ian Waxman | Principal, Risk & Compliance
484.383.0606 | iwaxman@navigatecorp.com

LOOKING FOR MORE INFORMATION ON GDPR?

Visit our Resource Center.

Disclaimer: This checklist is not exhaustive and should not be considered legal advice or a direct recommendation for your organization.