Aprio

Passionate for what's next℠

Aprio GDPR Compliance Services

PREPARING YOUR ORGANIZATION FOR THE BIGGEST DATA PROTECTION SHAKE UP IN 20 YEARS

In April of 2016, the General Data Protection Regulation (GDPR) was voted into law by the European Union. GDPR's impact has been seismic as global businesses scramble to create compliance strategies to meet the May 25, 2018, enforcement deadline.

GDPR represents monumental challenges to global business operations, because, unlike its predecessor Directive 95/46 EC, GDPR is a regulation (not a directive) and comes with steep penalties for non-compliance of up to 4 percent of annual revenue or €20 million, whichever is greater. But the greatest challenge is posed by GDPR's sweeping reach. The regulation applies to virtually every business in and outside the E.U. that processes personal data to sell goods and services to citizens of E.U. member states. To dispel any confusion entities who are currently Privacy Shield Certified must also comply with GDPR.

At Aprio, we view GDPR as an opportunity for organizations to greatly improve their risk management operations. The key challenge that most organizations will face is prioritizing their compliance initiatives within a tight timeline. Our team of Certified GDPR Practitioners have deep security and privacy experience in fintech and digital marketing and provide step-by-step guidance through the compliance readiness process.

Protecting the rights of data subjects

GDPR's six guiding principles were intended to strengthen data protection practices, align regulators under one authority and provide greater citizen control over personal data. The regulation's focus on data subject rights and consent will pose sizeable obstacles for digital marketing organizations. Those who currently capture data through Google IDs and are unclear as to the source, will face additional challenges.

GDPR's Six Guiding Principles

LAWFULNESS & FAIRNESS OF PROCESSING

Data subjects must give consent and be informed of how their data will be processed, and processing activities must align with how they are described.

PURPOSE & INTENT OF PROCESSING

Personal data can only be obtained for "specified, explicit and legitimate processing purposes" the subject has been made aware of and no other, without further consent.

DATA MINIMIZATION

Data collected on a subject should be limited to what is necessary in relation to the purposes for which it is processed.

ACCURACY & UP TO DATE

It is now the obligation of the data controller to ensure (to the best of their abilities) that the information collected is correct and current.

RETENTION LIMITATIONS

All personal information must now have an expiration date applied appropriate to its collected purpose, after which it must cease to be available.

SECURITY

Processors must handle data to ensure appropriate security, including protection against unlawful processing, accidental loss, destruction or damage.

GDPR is a regulation (not a directive) and comes with steep penalties for non-compliance of up to 4 percent of annual revenue or €20 million, whichever is greater.

Aprio

Passionate for what's next℠

Our approach

At Aprio, we believe that information risk management is a team sport. So, we partner with your internal resources to provide step-by-step guidance through our GDPR compliance process.

1. **Business understanding:**
   - GDPR applicability
   - Automated system mapping and data flow diagrams
   - Role establishment: Are you a Processor or Controller?
   - Data Protection Impact Assessment

2. **Gap assessment against GDPR requirements**
   - Conduct due diligence on the current state of the company with respect to GDPR requirements
   - Prepare GDPR applicability matrix
   - Study, analysis and assessment of PII lifecycle through web contents, business processes, technical infrastructure and people aspect
   - Discuss feasibility options and guidance for effective remediation with management
   - Provide Gap Assessment report with management summary recommendations
   - Provide guidance on "Privacy by Design Program"

3. **Remediation of gaps**
   - Remediation of identified gaps to be executed by the client organization
   - Aprio team of experts to provide the required guidance

4. **Review of GDPR remediation**
   - Collection and review of supporting evidence to establish demonstrable compliance

GDPR compliance with fewer hassels

GDPR's focus on protecting personal information and the rights of data subjects represents a bold leap forward in data security and privacy. At Aprio, we are committed to working with clients to make effective, sustainable risk management easier to achieve. Let us apply our proven process and compliance roadmap to help your organization become GDPR compliant.

About Aprio

Since 1952, clients throughout the U.S. and across more than 40 countries have trusted Aprio for guidance on how to achieve what's next. As a premier, CPA-led professional services firm, Aprio delivers advisory, assurance, tax and private client services to build value, drive growth, manage risk and protect wealth. With proven expertise and genuine care, Aprio serves individuals and businesses, from promising startups to market leaders alike.

Aprio.com

Morison KSi
Independent member

Let Aprio help you develop and implement your GDPR compliance strategy. Contact:

Dan Schroeder
Partner-in-Charge,
Information Assurance Services
dan.schroeder@aprio.com
770.353.8379

Sonali Vaidya
Senior Manager,
Information Assurance Services
sonali.vaidya@aprio.com
770.353.8391