Guide to GDPR Compliance

Introduction to the EU GDPR

The EU General Data Protection Regulation (GDPR) is a law designed to enhance data protection and provide a consolidated framework to guide business usage of personal data across the EU. The GDPR replaces the patchwork of existing regulations and frameworks across the EU and sets the global standard for personal data protection.

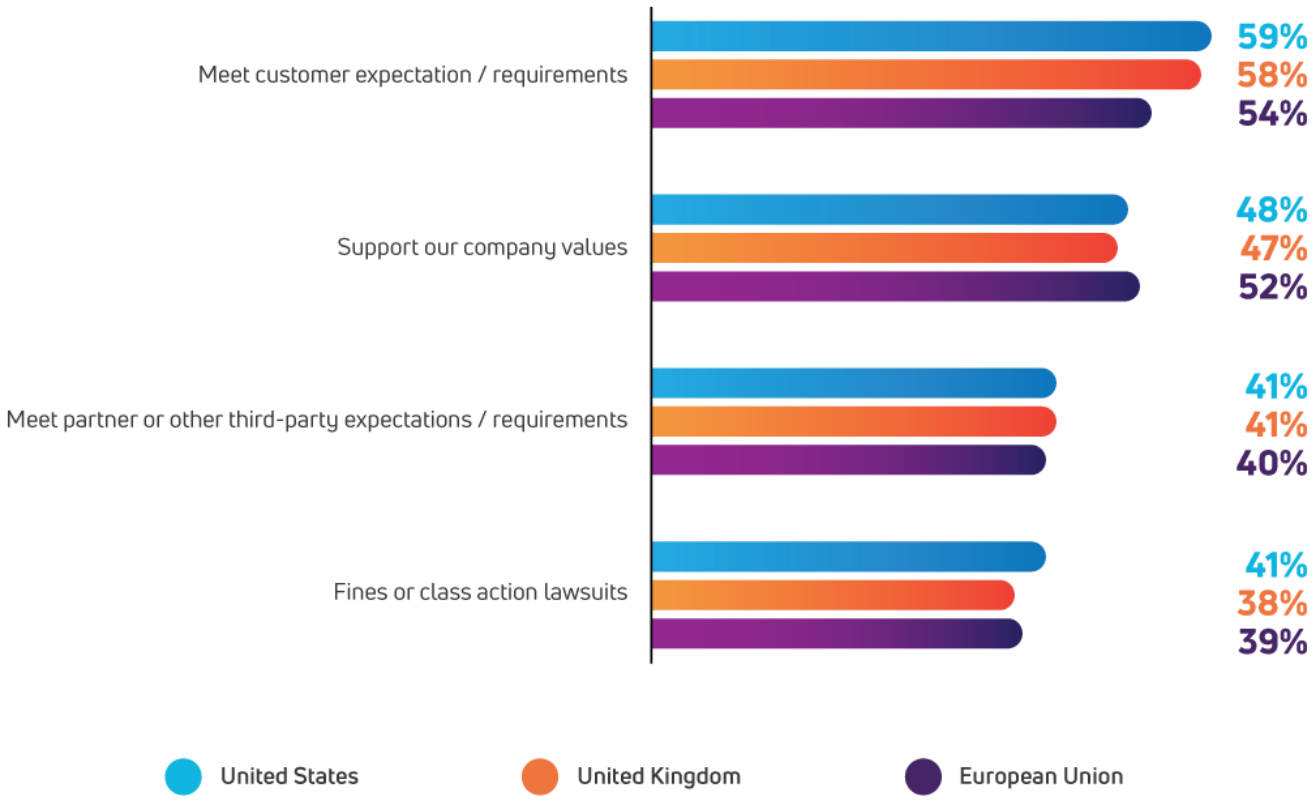
The law has an extraterritorial scope, meaning that it affects companies outside of the EU that target the European market. For example: if you offer goods and services to individuals in the EU, monitor individuals' behavior, or have employees in the EU. Because of the sweeping changes involved, many organizations are implementing new privacy programs with new controls.

Why Comply with the GDPR?

GDPR comes with significant financial penalties for non-compliance - fines up to 20,000,000 EUR or 4% of the total worldwide annual turnover of the preceding year (whichever is higher). However, research conducted by TrustArc shows that fines and lawsuits are not the primary reason companies invest in GDPR compliance. The most significant catalyst is driven by meeting customer expectations.[1] Not meeting customer expectations can lead to a loss of business and customer trust, which can take a long time to recover.

Drivers for investing in GDPR compliance consistent across regions

What are your primary reasons for investing in GDPR compliance?



[1] https://info.trustarc.com/Web-Resource-2018-07-12-GDPR-ResearchReport_LP.html

Requirements and How to Comply With the GDPR

The full text of the GDPR is over 200 pages and encompasses 99 articles. We've taken those requirements and broken them down into the five phases of GDPR compliance your organization should focus on.

The GDPR Articles to Focus On

Reviewing all 99 GDPR Articles can be overwhelming. These are the core regulatory Articles that are worth focusing on as you begin complying with the regulation. Each Article aligns to one of the five phases of GDPR compliance above.

Article 6: Lawfulness of processing

Conduct Data Inventory & Data Flow Analysis

Article 6 in the GDPR provides several different basis for the lawful processing of personal data. Think of these as the standard reasons why your business uses personal data. For example, whether the data subject has given consent or whether the processing is necessary to protect the data subject's vital interests or another natural person.

To comply with this requirement, companies need to assess the basis for which they conduct the processing while documenting this analysis for accountability-on-demand purposes. Documentation should happen in a centralized and transparent place, one that is connected to the business activity. Conducting a data inventory that captures your lawfulness of processing will streamline future compliance steps.

One prominent example of a lawful basis is the basis of consent. If companies wish to use consent as a lawful basis of processing, they need the technology tools that ensure the consent was given by a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication that the data subject agrees to process personal data relating to him or her.

Article 30: Records of processing activities

Conduct Data Inventory & Data Flow Analysis

This Article requires data controllers (the company determining the means and processing purposes) and processors (the company undertaking these actions) to keep records of data processing activities and prescribes the information that the records shall contain.

To comply with this requirement, companies need to have a process to record these activities. The process should make it easy to update records, find data if a data subject requests it, and produce reports on demand. These reports often take the form of a data inventory and data flow maps along with Article 30 reports.

Article 35: Data protection impact assessment

Conduct DPIAs/PIAs

Article 35 requires that if the processing is likely to result in a high risk to the rights and freedoms of natural persons[2], then data controllers must assess how the processing will impact the protection of personal data. Luckily, this Article provides examples of processing that may impose this high risk and prescribes what the assessment shall contain.

Some examples of high-risk activities include:

- Genomic testing
- Credit checks or;
- Cloud computing services for personal or household activities such as e-readers or private webmail

To comply with this requirement, companies should have a sustainable process that uses a comprehensive risk assessment (e.g., DPIA or PIA) to address the provisions and produce Article 35 compliance reports. These reports should include details of the processing and any controls to mitigate the high risks.

Articles 15-23: Data subject rights

Individual Data Protection Rights

These Articles provide data subjects with several rights that apply to their data, such as:

- Right of access
- Right to rectification or erasure
- Right to restrict or object processing
- Right to data portability

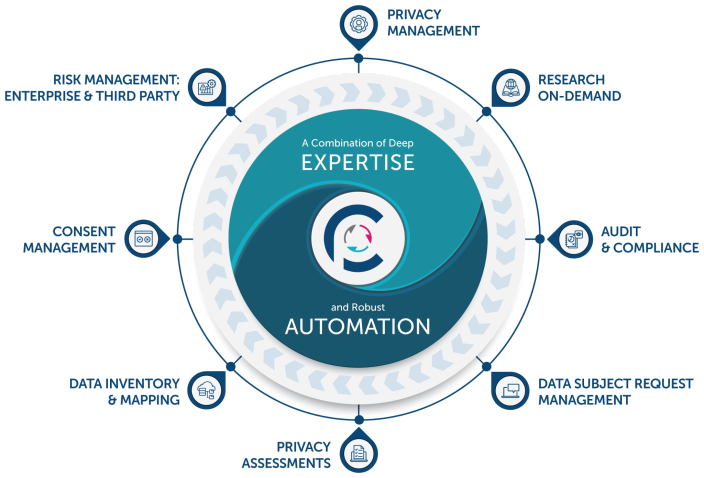
To provide these rights, companies need a process to field the requests, keep audit logs, verify the requestor's identity, fulfill the request, and produce supporting compliance reports.

[2] Processing this personal data could negatively affect data subjects' data privacy, freedoms of speech, or rights to liberty

Leverage a Command Center for Privacy

Whether you're using GDPR as the gold standard for your privacy program or looking to add it to your arsenal of privacy requirements, you are likely trying to figure out how to demonstrate progress.

TrustArc's PrivacyCentral provides a single, intelligent view of where you stand concerning privacy compliance, what actions should be taken, and by whom.



See what PrivacyCentral is all about!

Watch a PrivacyCentral **overview** and

REQUEST A DEMO

About TrustArc

As the leader in data privacy, TrustArc automates and simplifies the creation of end-to-end privacy management programs for global organizations. TrustArc is the only company to deliver the depth of privacy intelligence, coupled with the complete platform automation essential for the growing number of privacy regulations in an ever-changing digital world. Headquartered in San Francisco and backed by a global team across the Americas, Europe, and Asia, TrustArc helps customers worldwide demonstrate compliance, minimize risk, and build trust. For additional information, visit www.trustarc.com.