

# Navigating General Data Protection Regulation (GDPR)

Preparing your organization to comply with GDPR guidelines will require you to navigate a complex regulation and supplemental local laws of relevant EU member states. There are hundreds of sources of information on the topic, and it is difficult to sift through all the details to determine what is applicable and relevant to your contact center. Alvaria conducted a year-long review of GDPR as it applies to our own products, services, and practices, and is committed to helping customers process data using Alvaria's products and services in compliance with the requirements of GDPR. To get you started, we've compiled a list of key GDPR principles and the business practices that are required to comply with them.

## Geographic Scope of GDPR

GDPR regulations apply to all organizations established in the European Union that process personal information, regardless of where the data is stored or processed. Any organization not established in the Union that analyzes the behavior of EU citizens (including using online cookies) or offers goods or services in the EU is also obligated to comply with GDPR.

## Personal Data Processed Outside of the European Union

Many institutions process the personal data of EU citizens outside of the Union, and GDPR regulations necessitate that the countries in which these organizations operate require an "adequate level of protection" for the information.

The European Commission is obligated to monitor how countries around the world define what practices and measures constitute an adequate level of data protection on an ongoing basis. Organizations that process the personal data of EU citizens should determine what guidelines apply within the country they operate in. For example, organizations in the United States may seek to certify under the EU-US Privacy Shield, adopt binding corporate rules or adopt the European Commission's Standard Contractual Clauses into its agreements.

## Lawfulness of Processing

Processing personal data is lawful only if permitted based on:

- Consent
- Contractual necessity
- Compliance with legal obligations
- Vital interests of a data subject or another person
- Public interest
- Legitimate interests of a controller except where overridden by interests, fundamental rights, or freedoms of a data subject

One of the most challenging requirements under GDPR is obtaining and tracking customer consent. Per GDPR, before processing personal data, explicit consent is required from customers to give them individual control over their personal data. "Explicit" consent must be freely given, specific, informed, and unambiguous. However, there are a few limited circumstances when personal data can be processed without consent.

## Information Obligations and Rights of Data Subjects

Organizations must take appropriate measures to provide information to affected individuals, access to personal data, and comply with the exercising of all rights that data subjects have under the GDPR. Below you will find some more information on specific data subjects' rights, such as:

### **Right of Access to Data**

Under GDPR, individuals have the right to request confirmation as to whether or not their personal information is being processed by an organization. If the data subject's personal information is being processed, they must be permitted access to the information as well as, among other items, provided with the following explanations:

- Why the data is being processed and what categories of data are being used
- Who will have access to the personal data
- How long the data will be stored

Data subjects also have a right to obtain a copy of the personal information undergoing processing.

### **The Right to be Forgotten**

GDPR requires organizations to erase personal data at the request of data subjects in the following circumstances, among others:

- When the personal data no longer needs to be collected or processed
- Upon the withdrawal of a data subject's consent and there are no legal grounds for processing
- If data subjects object to the processing of their personal data, and there are no overriding, legitimate grounds for processing
- If consent of a minor is given by a parent/guardian, and is later revoked
- When personal data is collected via information society services

EU citizens have the right to ensure their personal information is not utilized for direct marketing, but in many cases, they have limited ability to prevent their data from being used. An example of when they cannot prevent their personal information from being processed is when it is needed by an organization to comply with a legal obligation.

### **Data Protection Impact Assessments**

Data Protection Impact Assessments (DPIAs) are required by GDPR when the processing of personal information is likely to result in a high risk to the rights and freedoms EU citizens. Large scale monitoring or extensive automated decision-making processes are

good examples of when DPIAs should be conducted. If a project or process requires a DPIA, the analysis must:

- Describe the nature, scope, context, and purposes of the data processing
- Assess the proportionality, compliance, and necessity of the data processing
- Assess risk to the rights and freedoms of data subjects
- Identify additional measures to address those risks such as safeguards, security measures, and security mechanisms

### **Data Protection Officers**

GDPR regulations mandate that a data protection officer is required when:

- The organization processing personal information is a government institution
- The core activity of the organization is to systematically monitor individuals on a large scale
- Special data under GDPR Article 9 or criminal convictions and offences are processed on a large scale as part of an organization's core activities

Data Protection Officer responsibilities include:

- Educating and training staff about data privacy requirements and practices under GDPR
- Auditing and monitoring compliance with GDPR
- Serving as a point of contact between an organization and GDPR regulators
- Monitoring data protection efforts and maintaining records on these activities
- Communicating with data subjects

### **Final Note**

After a year-long review of GDPR and our processes/systems, we evaluated how personal information is used within our products and services. We then improved them when necessary to help customers process data using Alvaria's products and services in compliance with GDPR by:

- Adopting more explicit privacy by design principles
- Adopting more explicit privacy by default principles

- Supplementing existing documentation to help customers demonstrate compliance with GDPR principles
- Reasonably assisting customers in conducting Data Protection Impact Assessments as needed

Alvaria will continue to closely monitor GDPR and the litigation that will clarify many of the requirements of this landmark legislation. We are dedicated to helping our customers achieve GDPR compliance pertaining to processing data with our products and services, and are committed to helping customers navigate the regulations and guidelines that contact centers must abide by to process data with our products and services.

**DISCLAIMER:** The information provided herein is for informational purposes only. To ensure that any organization using Alvaria products and services, or any other call center technologies is complying with applicable law, the organization should seek independent legal counsel or other professional advice. These materials are provided “as is” and, as such, Alvaria does not represent that they are complete, up-to-date, error free, or applicable to any particular organization’s situation. In addition, as with any call center system, the products by themselves cannot be “compliant” with all laws. Rather, compliance or non-compliance with the law ultimately is dependent upon how an organization uses the product in question. Therefore, nothing herein should be construed as a warranty of GDPR compliance or assurance that an Alvaria product or service cannot violate the GDPR or any other law.

#### **Corporate and Americas Headquarters**

5 Technology Park Drive, Suite 9  
Westford, MA 01886  
+(1) 978 250 7900 office  
+(1) 978 244 7410 fax

#### **Europe & Africa Headquarters**

The Record Store, 15 Pressing Lane  
Hayes UB3 1EP, United Kingdom  
+(44) 20 8018 8000 office  
+(44) 20 8561 4776 fax

#### **Asia Pacific & Middle East Headquarters**

3 Temasek Avenue, Centennial Tower, #21-00  
Singapore 039190  
+(65) 6590 0391 office  
+(65) 6324 1003 fax

#### **About Alvaria**

Alvaria was founded through the merger of Aspect Software and Noble Systems, technology leaders in Customer Experience (CX) and Workforce Engagement solutions. Our name is derived from Latin for “hives” – nature’s perfect form for millions of years – bringing you solutions that are scalable, resilient and secure, with efficiency, speed and pinpoint accuracy. **ALVARIA™**. Reshaping Customer Experience™.