cority™

Cority, Your Partner in Complying with the GDPR

Your Partner in Complying with the GDPR

General Data Protection Regulations (GDPR)

The European Union GDPR is a law designed to enhance data protection for EU residents and provide a consolidated framework to guide business usage of personal data across the EU, replacing the patchwork of existing regulations and frameworks. The 200-plus page GDPR replaces the 20-year-old Directive (95/46/EC). GDPR will come into force on **May 25, 2018**.

Affected Parties

Data Controllers: The Data Controller is a Cority customer, and is defined in the regulations as, "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data".

Data Processors: The Data Processor is defined as, "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". The Data Processor in this context, where the customer is Cority-hosted, would be Cority.

General Key Elements

1. Most of the responsibility is on the Data Controller. Data Controllers have the primary burden for protection of personal data you collect. However, GDPR also places direct obligations on the Data Processor.

2. Companies must select a Data Processor that has sufficient protection and procedures for personal data.

3. Companies must enter into a Data Processing Contract with the Data Processor.

4. The Data Processor (Cority) must only act under the instruction of the Data Controller.

Cority's Responsibility as a Data Processor

Security

As your Data Processor, Cority is required to implement appropriate security measures, including:

- The pseudonymizing and encryption of personal data.
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems.
- The ability to restore the availability and access to personal data in a timely manner.
- Process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring security of processing.

How Cority supports GDPR security compliance

- Cority is certified as ISO27001 compliant.
- We take Security seriously and have all the security processes and procedures in place as required under GDPR.
- We undergo rigorous external audit verification on an annual basis.
- We encrypt data.
- Our solution allows for archiving and purging of records in accordance with your criteria.
- Our backup and disaster recovery programs are in compliance with the GDPR requirements.
- The Cority application can be configured to secure information on a "need to know" basis, and has every conceivable option to do so.

Data Breach Notification

Key responsabilities on this area:

- Report breaches to our customers.
- Notify individuals of breach of personal information within 72 hours.

How Cority supports data breach notification compliance

- Cority's standard procedures already require notification to affected parties within 48 hours.

Subcontractors

In the event Cority would use any subcontractor:

- Cority as Data Processor is required to seek consent from Controller for use of a sub-Processor to carry out any part of the agreement

How Cority supports GDPR compliance for subcontractors

- Cority is required to reflect the same contractual obligations it has with the Controller in a contract with any sub-processors
- Cority remains liable to the Controller for the actions or inactions of any sub-processor

Contract between Cority and Customers – Data Processing Contract

Cority's activities, as Data Processor, must be governed by a binding contract with our customers, the Data Controller.

How Cority will support Data Processing Contracts

- The Data Processing contract includes the rights and obligations of the Data Processor and Controller, and must include, among other things, the subject matter of processing, the nature and purpose of processing, duration, the type of personal data to be processed, and the categories of data subjects.
- The contract must also include terms that cover:
  - Confidentiality obligations of all persons authorized to process personal data of Controller;
  - Processor's obligation to take all appropriate technical and organizational measures to protect personal data;
  - The deletion or return of all personal data to the controller, at the controller's choosing, upon completion of the processing services and the return any existing copies of the data, unless EU or Member State law requires that the personal data be stored;
  - Processor's obligation to make available to the controller all information necessary to demonstrate compliance with its obligations and allow and cooperate fully with audits, including inspections, conducted by the controller or another person authorized to this end by the controller.

Rights of Data Subjects – Data Portability

Cority recognizes the various rights of Data Subjects under GDPR, including the right for Data Subjects to access, rectify and erase their personal data, and the right for data portability, among other rights.

GDPR allows Data Subjects the right to receive their personal data in a commonly used and machine-readable format so that it can be transmitted for use to another Data Controller.

How will Cority Support Data Portability

- Cority is developing an Employee Data Extraction tool that is fully configurable, so that an employer (Data Controller) can easily choose which data (i.e. from which suites and modules) should be provided back to the employee in order to comply with Data Portability rights of Data Subjects.

Cority must Demonstrate compliance with GDPR

- Cority has the obligation to maintain a record of all categories of processing activities and the categories of processing being carried out by Cority including details of any transfers to third countries or international organizations and a general description of technical and organizational security measures.
- Be able to provide these records to the supervisory authority on request.

We Have You Covered

In addition to the Data Processing contract between Cority and its Customers, Cority's platform associated with our ISO27001 certification provides us with the ability to demonstrate our compliance with GDPR.

If you have any questions about Cority's ability to meet the GDPR requirements, please contact info@cority.com.

This document is intended to provide general guidance to Cority customers on the GDPR and is not meant to provide any legal or professional advice of any kind. Customers of Cority are recommended to seek independent legal advice where needed. No warranties, promises and/or representations of any kind, expressed or implied, are given as to the nature, standard, accuracy or otherwise of the information provided herein.