cority

cority ONE™

FAQ

Cority & GDPR

cority

The European Union General Data Protection Regulations (GDPR)

The European Union General Data Protection Regulations (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. The GDPR came into force on May 25, 2018.

As your Data Processor, Cority is required to implement appropriate security measures, including, but not limited to:

- The pseudonymization and encryption of personal data;
- Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems;
- Restoring the availability and access to personal data in a timely manner; and
- Processes for regular testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring data security protocols.

How Cority Stays GDPR Compliant

Frequently Asked Questions

How does Cority pseudonymize data?

Pseudonymization is a data management and de-identification procedure which involves replacing personally identifiable information fields with artificial identifiers (or pseudonyms). The pseudonym for each replaced field makes the data record less identifiable while remaining suitable for data analysis and data processing. Cority performs pseudonymization through a Personally Identifiable Information (PII) script; our team enacts the script on client databases when required – often dozens of times every day.

How does Cority protect data from unauthorized access?

All Cority users see data based on access rights. Through the user interface (UI), designated administrative users can define roles and their corresponding permissions. Users can then be assigned to these roles which in turn grants them said permissions. Additionally, access control can be determined by location and/or other extended demographic information based on a customer-defined hierarchy. Even more is the ability to set access granularity by module, at the field level, and reporting.

Given the wide level of flexibility of the solution, role and permission recommendations will be made based upon a business process review during the initial implementation. It is also possible to use a System for Cross-domain Identity Management (SCIM) to manage users in the system and then use an Application Programming Interface (API) mechanism to assign/modify said users to existing roles.

How does Cority facilitate the archiving, storage, and periodic deletion of PHI/PII in accordance with the 'right to be forgotten'?

Cority has pre-built rules that can help to facilitate archiving, storage, and deletion of personal health information (PHI) and/or PII. Business Rules can be configured to archive or delete data after a set amount of time. For example, if an employee left the company on 1st January 2020, a Business Rule can be configured to remove all data associated with their name at a specified time after termination.

Additionally, Cority provides pre-built reports that can make accessing and archiving data easier and safer for users. Cority's Medical Records Report was built with GDPR's medical history requirements in mind and allows users to find data based on name, user type, location, and more. These reports make archiving, storage, and deletion easier to manage.

What supplementary technical measures have been implemented by Cority to protect personal information?

Cority protects personal information in several ways. Customer data is encrypted both when in transit and at rest. When data is 'encrypted in transit', it means your data is protected if communications are intercepted while data moves between two services. This protection is achieved by encrypting the data before transmission; authenticating the endpoints; and, on arrival, decrypting and verifying that the data was not modified. Data 'encrypted at rest' protects your data from a system compromise or data exfiltration by encrypting data while stored.

Pseudonymization, a data management and de-identification procedure which replaces personally identifiable information fields with artificial identifiers (or pseudonyms) is another way Cority ensures the confidentiality of private information. The pseudonym for each replaced field makes the data record less identifiable while remaining suitable for data analysis and data processing.

Finally, Cority administers encryption key management to all cryptographic keys, including generating, using, storing, archiving, and deleting of keys, which limits access to the keys through user/role access.

What supplementary administrative measures have been implemented by Cority to protect personal information?

Cority maintains multiple administrative measures to protect personal information. The first of these is the principle of least privilege (PoLP), an information security concept under which users only have access to the specific data required to complete associated tasks. This principle is proven to significantly reduce attack surface and spread of malware.

Cority provides PII training and audits, which helps users and employees to understand why it is important to protect PII, the policies and procedures related to the use and disclosure of PII, and both the organization's and individual's responsibilities for safeguarding PII.

Finally, in conjunction with the PoLP, Cority maintains role-based access controls (RBAC) across the solution, which restricts system access to only authorized users. These rules help ensure that sensitive data is only seen by users that require the information based on configurable authorization set by administrators.

What supplementary contractual measures have been implemented by Cority to protect Personal Information?

Where required by law, Cority has implemented standard contractual measures and inter-group data processing agreements.

In the event Cority receives an order from any third party for compelled disclosure of any customer personal data, Cority:

- Uses every reasonable and lawful effort to redirect the third party to request data directly from the customer;
- Immediately notifies the customer, unless prohibited by law; and
- Uses all reasonable efforts to assist the customer with a challenge of the order for disclosure.

If, after the steps described above, Cority or any of its affiliates remain compelled to disclose customer data, Cority will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

For the sake of clarity, lawful efforts do not include measures that would result in civil or criminal sanctions such as contempt of court against Cority.

Does Cority have a comprehensive privacy program?

Cority is ISO 27018 certified. ISO 27018 certification is an industry standard code of practice for the protection of PII in public clouds acting as PII processors. The standards set out in ISO27018 help to ensure users that all personal data is processed securely and sets standards for responsibility and safeguarding of information.

Does Cority have a process for notifying customers if it receives an inquiry from an individual, regulator, or public authority that relates to Cority's processing of personal information?

In the event Cority receives an inquiry, Cority will advise the individual, regulator, or public authority to contact the associated data controller. Additionally, Cority will notify the customers point-of-contact (POC) on the personal data requirements set out by the request.

Will Cority collect personal information directly from individuals on customers' behalf (as a vendor) or through a facility provided by customers (as a controller)? If so, what is Cority's process for providing notice and obtaining consent (where required)?

Cority will not collect personal information directly from any individuals.

Does Cority regularly train employees on privacy and data security? If so, how and how often?

Internal privacy and data security training is conducted on an annual basis for all employees. The training material and training records are captured in Cority's security training platform.

What processes or methods does Cority have for assisting customers in complying with their obligations for handling data subject requests regarding the processing of their personal information? This includes the right to be forgotten, and the rights to access, rectification, objection, restriction of processing, portability, objection to automated decision-making, including profiling, of data.

Cority provides the capabilities to handle personal data requests through the hosted application. Optionally, Cority can assist customers to comply with personal data requests through separate service requests. The requests must be submitted by authorized personnel and it is subject to additional service charges.

Has Cority been the subject of any data protection authority audits? If yes, when was the audit and did it relate to the processing of customer personal information?

Cority has not been the subject of any data protection authority audits, as of August 2023.

Does Cority have a written Incident Response Plan that covers personal information that Cority processes?

Yes – Cority has a documented Incident Response Plan (Cyber Security Incident Response Plan) that addresses various incident types/scenarios including PII related incidents.

Has Cority had a data security breach (involving the unauthorized acquisition of personal information) in the past?

Cority has not been the subject of any data security breaches, as of August 2023.

Does Cority have a process for assisting customers in carrying out a data protection impact assessment or consulting with the data protection authority, when required?

Cority will assist customers to conduct data protection impact assessment (DPIA) upon request. However, these assessments are limited to once per calendar year, and they must be completed in accordance with industry standards.

Has Cority appointed a data protection officer?

Cority's current Data Protection Officer is Atish Ghosh, CTO.

Which external reports assessing Cority's compliance with data privacy laws and privacy policies are available?

Cority provides access to multiple external reports and compliance documents, including our privacy policy, ISO27001/27017/27018 documents, and SOC 2 assessment reports. Applicable documentation can be provided upon request.

What is Cority's process for screening and supervising subcontractors?

Cority conducts background checks for all Cority employees, which includes contractors, before commencing employment. Additionally, Cority conducts third-party risk assessment for security evaluation before onboarding the third-party service providers.

What is the impact of the Cloud Act on customer solutions? What would Cority do in case of a US court order filed to gain access to a customer's database?

To date, Cority has not received any access requests pursuant to the Cloud Act. In the event that a court order is issued concerning a customer's database, Cority will direct the requesting authority to contact the customer, notify the customer to the extent permitted by law, and provide any assistance as required to afford such customer the opportunity to contest any such measures. Cority's sub-processors have made similar contractual commitments to Cority in their Data Processing Addendums to ensure that these commitments flow down, as needed, to protect Cority customers.