CODEVISTO

CODING TRUTH THAT POWERS DECISIONS.

Data Processing Agreement (DPA)

Last updated February 17, 2026

1. Definitions

"Customer" means the legal entity that subscribes to and uses the Codevisto Service and determines the purposes and means of the processing of Personal Data.

"Processor" means Teva Software S.L.U, a company established in Spain, which processes Personal Data on behalf of the Customer in connection with the Service.

"Personal Data", "Processing", "Data Subject", "Personal Data Breach" and "Supervisory Authority" have the meanings given in Regulation (EU) 2016/679 (GDPR).

"Service" means the Codevisto software development activity analysis platform, as described in the Codevisto Terms and Conditions.

"Sub-processor" means any processor engaged by the Processor to process Personal Data on behalf of the Customer.

"Data" has the meaning given in the Codevisto Terms and Conditions and includes technical metadata, analysis results and organizational information processed through the Service.

2. Roles and Responsibilities

The parties acknowledge that, in relation to the Processing of Personal Data under this Agreement, the Customer acts as Controller and the Processor acts as Processor.

The Processor shall process Personal Data only on the basis of documented instructions from the Customer, including those set out in this Agreement, in the Terms and Conditions and in the Customer's configuration and use of the Service, unless Union or Member State law to which the Processor is subject requires otherwise. In such a case, the Processor will inform the Customer of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

If the Processor considers that any instruction from the Customer infringes the GDPR or other applicable data protection law, the Processor shall inform the Customer without undue delay.

The Processor shall ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. Details of the Processing (Annex I)

Nature and purpose. The Processing consists of providing the Codevisto Service, including connecting to code repositories to extract technical metadata (commits, pull requests, reviews), generating metrics and insights on engineering activity and performance, and providing dashboards, reports and related analytics.

Categories of Data Subjects. Users authorised by the Customer to access the Service. Software developers and reviewers whose activity in repositories is analysed (e.g. names, email addresses, usernames contained in repository metadata).

Types of Personal Data. User account data: name, business email address, authentication identifiers. Developer metadata: name, email address, repository username and identifiers appearing in commits, pull requests and reviews. Organizational information: company name, teams, associations between Users and teams. Access and activity logs required for security, auditing and troubleshooting.

Duration. Personal Data is processed for the duration of the Service agreement between the Customer and the Processor. Upon

termination, Personal Data will be deleted within thirty (30) days unless the Customer requests its return within that period, as described in Section 10.

Source code. The Processor does not store source code, file contents or complete copies of repositories. The Service operates solely on technical metadata and derived analytical results. Any temporary access to repository contents during analysis is limited and ephemeral, and such data is not retained after processing.

4. Obligations of the Processor

The Processor shall: Process Personal Data only on documented instructions from the Customer and for the purposes set out in this Agreement and the Terms and Conditions.

Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in the Codevisto Security and Data Protection Report available at the URL communicated by the Processor from time to time, and shall not materially decrease the overall level of security of the Service during the term of the Agreement.

Ensure that access to Personal Data is strictly limited to personnel who need such access for the performance of the Service and who are bound by confidentiality obligations.

Assist the Customer, taking into account the nature of the Processing and the information available to the Processor, in fulfilling the Customer's obligations with respect to Data Subject requests, security of processing, Personal Data Breach notifications and data protection impact assessments, to the extent required by applicable law and within the scope of the Service. Such assistance may be subject to reasonable fees where it goes beyond standard functionality or support included in the Service.

5. Sub-processors

The Customer grants the Processor a general authorisation to engage Sub-processors for the provision of the Service. These include, without limitation, infrastructure and hosting providers (such as Heroku in the EU region), managed database and cache services, and email delivery providers, all operating within the EU/EEA or otherwise providing adequate safeguards.

An up-to-date list or description of the categories of Sub-processors is available upon request and, where applicable, through the Processor's security and privacy documentation.

The Processor shall inform the Customer, by email or through the Service or other written means, of any intended changes concerning the addition or replacement of Sub-processors, giving the Customer at least thirty (30) days' prior notice. The Customer may object to such changes on reasonable data protection grounds. If the parties cannot agree on a solution, the Customer may terminate the affected part of the Service upon written notice.

The Processor shall impose on each Sub-processor data protection obligations that are no less protective than those set out in this Agreement, by way of a written contract or other legal act. The Processor remains fully liable to the Customer for the performance of its Sub-processors' obligations with respect to Personal Data.

6. Data Subject Rights

Taking into account the nature of the Processing, the Processor shall assist the Customer, by appropriate technical and organisational measures and as far as possible, in fulfilling the Customer's obligation to respond to requests for exercising Data Subjects' rights under the GDPR.

If the Processor receives a request directly from a Data Subject relating to Personal Data processed on behalf of the Customer, the Processor will promptly forward the request to the Customer without undue delay and will not respond to the Data Subject except on documented instructions from the Customer or where required by applicable law.

The Processor shall provide reasonable assistance so that the Customer can respond to such requests within the deadlines set by applicable law, and in any case within thirty (30) days from the Customer's request for assistance, unless a different legal deadline applies.

7. Personal Data Breach

The Processor shall notify the Customer without undue delay and, where feasible, not later than seventy-two (72) hours after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Customer.

Such notification shall at least: Describe the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and personal data records concerned, where known. Describe the likely consequences of the Personal Data Breach. Describe the measures taken or proposed to be taken by the Processor to address the Personal Data Breach and mitigate its possible adverse effects.

The Processor shall cooperate with the Customer and provide further information as it becomes available, to enable the Customer to comply with any obligations to notify the Supervisory Authority and, where applicable, the affected Data Subjects.

8. Audits and Inspections

The Processor shall make available to the Customer all information necessary to demonstrate compliance with this Agreement and with Article 28 GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, as described below.

In the first instance, the Processor may provide existing security documentation, third-party audit reports, certifications (such as SOC 2 or ISO 27001, where available) or similar evidence that is sufficient to demonstrate compliance, in lieu of an on-site audit.

If, after reviewing such documentation, the Customer reasonably demonstrates that it is insufficient, the Processor will permit an audit or inspection by the Customer or its independent auditor, subject to: At least thirty (30) days' prior written notice. Audits being carried out during normal business hours, in a manner that minimises disruption to the Processor's operations. No more than one audit per calendar year, unless required by a Supervisory Authority or mandatory law. Appropriate safeguards to protect the confidentiality, security and trade secrets of the Processor and its other customers.

The Customer shall bear all costs associated with any audit or inspection, unless applicable law explicitly requires the Processor to bear such costs.

9. International Transfers

All Processing of Personal Data under this Agreement is intended to take place within the European Union / European Economic Area. The Processor's core infrastructure (including Heroku's EU region) and primary Sub-processors operate within the EU/EEA.

If the Processor needs to transfer Personal Data to a third country or to an international organisation, it will do so only on documented instructions from the Customer and in compliance with Chapter V GDPR, implementing appropriate safeguards such as the European Commission's Standard Contractual Clauses or other mechanisms approved by the European Commission.

10. Return and Deletion of Data

Upon termination of the Service or upon the Customer's request, the Processor shall, at the choice of the Customer, delete or return all Personal Data to the Customer and delete existing copies, unless Union or Member State law requires storage of the Personal Data.

Unless the Customer requests the return of Personal Data within thirty (30) days following the effective termination date of the Service, the Processor will delete all Personal Data processed on behalf of the Customer within thirty (30) days after such date. Upon request, the Processor will confirm deletion in writing.

During the term of the Service, the Customer may use the platform's data cleanup tools to delete activity data by repository and period; such deletions will cascade to related derived information (analyses, metrics, exclusions) and update cache entries accordingly.

11. Term and Termination

This Agreement enters into force when the Customer accepts the Codevisto Terms and Conditions or starts using the Service, whichever occurs first, and remains in effect for as long as the Processor processes Personal Data on behalf of the Customer in connection with the Service.

Provisions that by their nature are intended to survive termination, including but not limited to Sections 7, 8, 10 and 12, shall continue to apply after termination of this Agreement.

12. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of Spain. Any dispute arising out of or in connection with this Agreement shall be subject to the jurisdiction of the courts of Spain, unless otherwise required by mandatory applicable law.

13. Contact

For any questions regarding this Data Processing Agreement, please contact:

Teva Software S.L.U
Spain
Email: info@codevisto.com