Rubiklab
AI powered research

GENERAL DATA PROTECTION REGULATION

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data

Effective: 1st of April 2022

Rubiklab Ltd.
1A Falmer Court, London Road, Uckfield, TN22 1HN

Overview

Rubiklab is committed to complying with privacy and data protection laws and takes privacy seriously. This document provides an overview of Rubiklab's General Data Protection Regulation compliance measures (GDPR).
This policy was last updated in January 2026.

1. Definition

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that governs the processing of personal data from the EU. As defined by the GDPR, personal data includes any information relating to an identified or identifiable living individual, such as names, email addresses, and phone numbers.

2. Our role under GDPR

GDPR differentiates "controllers" and "processors." The distinction between these roles is essential, as each has distinct responsibilities. In simple terms, a "controller" is the entity that decides how and why personal data is processed. In contrast, a "processor" only processes personal data on behalf of a controller; it is a service provider and only uses the data in accordance with its controller's instructions.
To the extent that a party acts as a data processor ("Processor") on behalf of another party acting as a data controller ("Controller") in respect of any personal data comprised in the Controller Data ("Personal Data"), the Processor shall ensure that the following obligations are fulfilled:

(i) Where Rubiklab acts as a data processor on behalf of a controller, it processes Personal Data solely on documented instructions from the controller and strictly in accordance with applicable Data Protection Laws. Rubiklab ensures that all individuals authorised to process Personal Data are subject to appropriate confidentiality obligations and receive suitable training in data protection and information security practices. Rubiklab implements and maintains appropriate technical and organisational measures designed to ensure a level of security appropriate to the risks associated with the processing activities performed.

(ii) persons authorised by the Processor to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii) if Data Protection Laws require it, to process Personal Data other than stated before, it shall notify the Controller of any such requirement before processing the Personal Data (unless applicable law prohibits such information on important grounds of public interest);

(iv) it informs the Controller of any addition, replacement, or other changes of Sub-processors and provides the Controller with the opportunity to reasonably object to such
changes on legitimate grounds. The Controller acknowledges that these Sub-processors are essential to provide the Services and that objecting to the use of a Sub-processor may

prevent the Processor from offering the Services to the Controller.

The Processor will enter into a written agreement with the Sub-processor imposing on the Sub-processor obligations comparable to those imposed on the Processor under this Agreement, including appropriate data security measures. In case the Sub-processor fails to fulfill its data protection obligations under such written agreement with the Processor, that Processor will remain liable to the Controller for the performance of the Sub-processor's obligations under such agreement. By way of this Agreement, the Controller provides general written authorization to the Processor to engage Sub-processors as necessary to perform the Services; including those listed in Rubiklab's privacy policy. "Sub-processor" means another data processor engaged by the Processor for carrying out processing activities in respect of the Personal Data on behalf of the Controller;

(v) taking into account the nature of the processing, it shall assist the Controller by appropriate technical and organizational measures (at the Controller's sole expense), insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR;

(vi) it shall implement and maintain the technical and organizational measures in relation to the processing of Personal Data by the Processor and taking into account the nature of the processing;

(vii) at the choice of the Controller, it deletes or returns all the Personal Data to the Controller after the end of the provision of Services relating to processing, and deletes existing copies unless Data Protection Laws require storage of the Personal Data;

(viii) Rubiklab maintains appropriate documentation and records relating to its processing activities and security controls. Where required under applicable agreements or Data Protection Laws, Rubiklab will make available relevant information necessary to demonstrate compliance with its data protection obligations. Rubiklab will cooperate with reasonable audit or assessment requests from controllers, subject to appropriate confidentiality protections and reasonable notice;

In the event of a Personal Data Breach affecting Personal Data processed on behalf of a controller, Rubiklab will notify the controller without undue delay after becoming aware of the breach. Rubiklab will provide relevant information available at the time regarding the nature of the breach, the categories of data affected, and the steps being taken to address the incident. Where appropriate, Rubiklab will cooperate with the controller to support compliance with breach notification obligations under applicable Data Protection Laws.

3. All transfers of Personal Data to countries outside the United Kingdom or the European Economic Area shall be carried out in accordance with applicable Data Protection Laws and shall rely on appropriate legal safeguards.

   Where required, such transfers will be governed by approved transfer mechanisms including the European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement (IDTA), or other legally recognised mechanisms that ensure an adequate level of protection for personal data. Rubiklab ensures that any third parties or sub-processors involved in such transfers are contractually bound to implement equivalent data protection obligations and appropriate technical and organisational security measures.; and -

   (i) maintain complete and up-to-date records of processing activities carried out on the Controller's behalf as required by the Data Protection Laws.

To the extent that Rubiklab processes any Personal Data on Controller's behalf when performing its obligations under this Agreement, Controller shall:

(i) ensure that the Controller is entitled to lawfully transfer the Relevant Personal data to Rubiklab so that Rubiklab may lawfully use, process, and transfer the Personal Data in accordance with this Agreement on the Controller's behalf;

(ii) ensure that the relevant third parties have been informed of, and have given their permissions or consent to, such use, processing, and transfer as required under Data Protection Laws or other applicable law;

(iii) take appropriate technical and organizational measures against unauthorised or unlawful processing of personal data or its accidental loss, destruction, or damage;

(iv) not instruct or request Rubiklab (including in Controller's use of the Services) to undertake any processing which is not in accordance with Data Protection Laws; and

(v) notwithstanding any other indemnity provided by Controller in connection with this Agreement, Controller shall indemnify Rubiklab (and each of their respective officers, employees, and agents) against all losses, costs, expenses, or liabilities incurred by Rubiklab.

In the event that each party acts as an independent controllers, each party agrees that it shall:

(i) at all times during the term of this Agreement, comply with the Data Protection Laws;

(ii) provide reasonable assistance as is necessary to each other to:

a. enable each party to comply with any subject access requests (whether in relation to access to personal data, rectification, restrictions on processing, erasure, or portability) and to respond to any other queries or complaints from their data subjects ("Data Subject Request") in accordance with the Data Protection Laws;
b. facilitate the handling by the other party of any Personal Data Breach for which the other party is responsible as soon as reasonably practicable upon becoming aware which shall include the party responsible for the breach notifying:
c. (i) the Information Commissioner's Office (ICO) or other applicable supervisory authority and data subjects as required under the Data Protection Laws; and (ii) before such notification, each party agrees not to make any other announcement or otherwise make public any notice or information about a Personal Data Breach without the other party's approval, where applicable; and
d. provide reasonable assistance as is necessary to the other party to respond within a reasonable time to any inquiries from the ICO or other applicable supervisory authority.

Controller shall be responsible for maintaining the security of accounts, passwords (including but not limited to administrative and user passwords), and files, and for all uses of Controller

accounts with or without Controller's knowledge or consent. The Controller acknowledges that it is responsible for taking backup copies of any data and appropriate precautions to protect the Controller's computer systems against unauthorised access.

If the Controller does anything to or in relation to the Services that is a criminal offense under any law, including but not limited to the Computer Misuse Act 1990, the Controller's right to use the Services will be withdrawn immediately. Due to the nature of the Internet, the Services are not guaranteed to be delivered free of all viruses and technical defects of any description.

Data Subject Rights Fulfillment

Rubiklab Ltd. recognizes the importance of the rights granted to individuals under GDPR and is committed to ensuring their effective fulfillment. To this end, we have established a clear procedure for handling data subject requests. This includes a designated contact point for data subjects to submit requests related to access, rectification, erasure, data portability, restriction of processing, and objection to processing. Upon receiving a request, we promptly assess its validity and respond within the stipulated time frame of one month, extending this period when necessary due to complexity or number of requests. We ensure that data subjects are informed about their rights through clear, accessible information provided at the point of data collection. Additionally, we maintain a record of all data subject requests and our responses to ensure accountability and compliance. Regular training is provided to staff members who handle personal data to ensure they are equipped to identify and process these requests efficiently and in accordance with GDPR requirements.

Data Protection Impact Assessments (DPIAs)

To proactively manage risks associated with data processing activities, Rubiklab Ltd. incorporates Data Protection Impact Assessments (DPIAs) into its data governance framework. DPIAs are conducted for all new projects, technologies, or processing activities that are likely to result in a high risk to the rights and freedoms of individuals. This assessment includes evaluating the necessity and proportionality of the processing activities, assessing the risks to data subjects, and identifying measures to mitigate these risks. The DPIA process involves consulting with relevant stakeholders, including data subjects where appropriate, and keeping a record of the assessment outcomes. We review and update our DPIAs regularly or when significant changes in data processing occur, to ensure ongoing compliance and risk management. DPIAs are integral to our approach to privacy by design, ensuring that data protection principles are embedded in all new initiatives from the outset.

4. Our commitment to compliance

Rubiklab Ltd. maintains a structured data protection governance framework designed to ensure continued compliance with applicable data protection laws and recognised industry practices. This framework includes periodic internal reviews of data protection processes, security assessments, and ongoing staff awareness and training programmes. These measures are intended to ensure that personal data is handled responsibly, securely, and transparently throughout its lifecycle and that appropriate safeguards remain in place as technologies, regulatory expectations, and operational requirements evolve. Concurrently, as part of our commitment to fostering a culture of data privacy, we engage in ongoing awareness programs through our partnership with the DataExpert group. These programs are designed to keep our team informed and vigilant about data protection principles, emerging risks, and the evolving legal landscape. By intertwining rigorous compliance reviews with continuous employee education, we strive to maintain the highest standards of data protection and privacy, reflecting our deep commitment to safeguarding the personal data entrusted to us.

Please contact us

Please email support@rubiklab.ai with any questions, concerns, or comments regarding this privacy statement or any requests concerning your personal data.