Kolay IK

Data Processing Agreement (UK)

Last updated: 21 November 2026
Version 2.0. Replaces version 1.0 of 17 June 2026.

This Data Processing Agreement ("DPA") forms part of the Master Subscription Agreement, Order Form or other agreement under which Kolay IK Limited, a company registered in England and Wales (company number 16968866) with its registered office at Capital Office, 124-128 City Road, London, EC1V 2NX ("Kolay IK" or "Processor"), provides the Kolay IK platform to the customer named in that agreement ("Customer" or "Controller") (together the "Principal Agreement"). It applies automatically when the Principal Agreement is signed or accepted; no separate signature is needed. A countersigned copy is available on request from privacy@kolayik.co.uk.

1. Definitions

1.1. "Data Protection Laws" means all applicable data protection and privacy legislation in force from time to time in the UK, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 and the Data (Use and Access) Act 2025, each as amended or replaced from time to time.

1.2. "UK GDPR" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.3. The terms "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach" and "Processing" have the meanings given to them in the UK GDPR.

2. Role of the Parties

2.1. For the Processing of Personal Data under the Principal Agreement, the Customer is the Controller and Kolay IK Limited is the Processor.

2.2. The subject matter, nature, purpose and duration of the Processing, the types of Personal Data and the categories of Data Subjects are set out in Annex 1.

3. Obligations of the Processor

3.1. Documented instructions: The Processor shall process Personal Data only on the documented instructions of the Controller, unless required to do so by UK law to which the Processor is subject. In that case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.2. Confidentiality: The Processor shall ensure that all personnel authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3. Security: Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, the Processor shall implement appropriate technical

and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the UK GDPR.

3.4. Data Subject rights: Taking into account the nature of the Processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, to respond to requests to exercise Data Subject rights under Chapter III of the UK GDPR.

3.5. Assistance: The Processor shall assist the Controller in ensuring compliance with Articles 32 to 36 of the UK GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of Processing and the information available to the Processor.

3.6. Unlawful instructions: The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the UK GDPR or other Data Protection Laws, and may suspend the affected Processing until the Controller confirms or changes the instruction.

3.7. Security measures: The technical and organisational measures the Processor maintains are described in Annex 3. The Processor may update them provided that the overall level of security is not reduced.

4. Sub-processing

4.1. General authorisation: The Controller gives a general written authorisation for the Processor to engage the Sub-processors listed in Annex 2.

4.2. Notification of changes: The Processor maintains a current list of Sub-processors at kolayik.co.uk/sub-processors and will notify the Controller by email at least 30 days before adding or replacing a Sub-processor. The Controller may object on reasonable data protection grounds within that period. The Parties will discuss the objection in good faith. If they cannot resolve it, the Controller may terminate the affected part of the service without penalty and receive a pro rata refund of prepaid fees.

4.3. Flow-down obligations: The Processor shall impose on each Sub-processor, by contract or other legal act, data protection obligations materially similar to those in this DPA.

4.4. Liability: The Processor remains fully liable to the Controller for the performance of each Sub-processor's data protection obligations.

5. International data transfers

5.1. The Processor shall not transfer Customer Personal Data to a country outside the UK unless (a) the country is covered by UK adequacy regulations, or (b) the transfer is subject to appropriate safeguards under Article 46 of the UK GDPR, such as the ICO International Data Transfer Agreement (IDTA) or the International Data Transfer Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment.

5.2. Customer Personal Data is hosted in the EEA (AWS, Frankfurt, Germany). Personnel of the Processor's group company Kolay Yazılım A.Ş. in Türkiye access it remotely to provide engineering, maintenance and support. That access is a restricted transfer and is covered by an IDTA between Kolay IK Limited and Kolay Yazılım A.Ş.

5.3. On request, the Processor will provide the Controller with a copy of the transfer safeguards and a summary of the transfer risk assessment, with commercial terms redacted.

6. Personal Data Breach

6.1. The Processor shall notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notice will include, as far as then known, the information listed in Article 33(3) of the UK GDPR, and the Processor will provide further information in phases as it becomes available.

6.2. The Processor shall give the Controller enough information to meet any obligation to report the breach to the Information Commissioner's Office (ICO) or to notify Data Subjects.

7. Audit and inspection

7.1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the UK GDPR.

7.2. The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, on reasonable prior written notice, during normal business hours and subject to appropriate confidentiality undertakings. The Controller bears the cost of an audit unless it reveals a material breach by the Processor.

8. Return or deletion of data

8.1. On termination or expiry of the Principal Agreement, the Processor shall, at the Controller's choice, delete or return all Personal Data to the Controller and delete existing copies, unless UK law requires storage of the Personal Data. Details are in Annex 3, section 14.

9. Contact details

Privacy and data protection enquiries, notices and breach reports: privacy@kolayik.co.uk

10. Governing law and jurisdiction

This DPA is governed by the laws of England and Wales. Each Party irrevocably submits to the exclusive jurisdiction of the courts of England and Wales.

11. Electronic execution

This DPA and any amendments may be executed electronically (including through Google Workspace eSignature), and electronic signatures have the same legal effect as wet-ink signatures.

Annex 1: Details of processing

A. Subject matter and duration: The provision of the Kolay IK cloud-based HR platform to the Controller, for the duration of the Principal Agreement.

B. Nature and purpose: Providing human resources management software services, including employee record keeping, payroll data preparation, absence tracking and related HR administration.

C. Categories of Data Subjects: The Controller's current, past and prospective employees, independent contractors and workers, and their nominated emergency contacts.

D. Types of Personal Data: Standard HR and employment data: first and last name, residential address, gender, job title or role, start date, basic salary information, bank account number, phone number, email address, emergency contact details, education history, marital or family status, career history, company-related financial transactions and advances, working pattern, absence and leave records (including sickness absence dates and reasons where the Controller records them), performance review content, time and attendance records, and recruitment data (CVs and application details).

E. Special categories of data (Article 9 UK GDPR): The platform allows the Controller to record sickness absence and, at the Controller's discretion, related health information such as fit notes. This is data concerning health. The Controller is responsible for having an Article 9 condition (normally Article 9(2)(b) with Schedule 1, Part 1, paragraph 1 of the Data Protection Act 2018) and an appropriate policy document. The Processor applies the measures in Annex 3 to this data. The Controller shall not upload other special category data or criminal offence data without the Parties' prior written agreement.

Annex 2: Approved Sub-processors

The Controller authorises the following Sub-processors. The current list is maintained at kolayik.co.uk/sub-processors.

Sub-processor	Service	Data location	Transfer mechanism
Kolay Yazılım A.Ş. (group company)	Platform engineering, maintenance, customer support	Türkiye (remote access)	IDTA and transfer risk assessment
Amazon Web Services EMEA SARL	Cloud infrastructure and primary database	Frankfurt, Germany	UK adequacy (EEA)
Google Cloud EMEA Ltd (Workspace)	Email and document storage used in support	EU and other Google locations	UK adequacy / UK-US data bridge
Sendinblue SAS (Brevo)	Transactional email (for example password resets and alerts)	EU (France)	UK adequacy (EEA)
Crisp IM SAS	Support chat and tickets	EU (France)	UK adequacy (EEA)
Functional Software, Inc. (Sentry)	Error tracking and diagnostics	EU (Frankfurt, Germany)	UK adequacy (EEA)

Internal business tools used by Kolay IK that do not process the Controller's employee data, such as CRM and accounting software, are not listed here. These tools may contain business contact details of the Controller's own staff who deal with us, which we process as a controller under our Privacy Policy.

Annex 3: Technical and organisational measures

This Annex describes the technical and organisational security measures implemented by the Processor under Article 32 of the UK GDPR and clause 3.3. They are reviewed at least annually. If this Annex conflicts with the body of the DPA, the DPA prevails.

1. Certifications and independent assurance

The Processor maintains ISO/IEC 27001 (information security management), ISO/IEC 27701 (privacy information management) and ISO 9001:2015 (quality management), audited annually by accredited third parties. Summary certificates and, under a mutual NDA, the Statement of Applicability are available on reasonable request.

2. Infrastructure and hosting

2.1. Customer Personal Data is hosted on Amazon Web Services in the Frankfurt, Germany (eu-central-1) region. AWS is responsible for physical security, environmental controls and hypervisor isolation under its shared responsibility model.

2.2. Production, staging and development environments are logically and network separated. Production databases sit in private subnets with no direct public ingress.

2.3. Inbound traffic is restricted on a least-privilege basis through security groups and network ACLs. Web-facing services are protected by a web application firewall and rate limiting.

3. Encryption

3.1. Data in transit is encrypted with TLS 1.2 or higher, with HSTS enforced. Internal service traffic is encrypted within the AWS network.

3.2. Customer Personal Data at rest, including databases, object storage, backups and snapshots, is encrypted with AES-256.

3.3. Keys are managed in AWS Key Management Service with rotation policies. No Kolay IK personnel have plaintext access to customer database encryption keys.

4. Access control

4.1. Platform users: unique named accounts, salted password hashing, minimum password complexity, multi-factor authentication available to all users and required for administrative roles, role-based access control, and session timeouts.

4.2. Kolay IK personnel, including Kolay Yazılım A.Ş. staff: access to production systems and Customer Personal Data on a least-privilege, need-to-know basis with documented approval; multi-factor authentication through a managed identity provider; privileged actions logged and reviewed; access rights reviewed at least quarterly and revoked within 24 hours of a role change or departure.

5. Logging and monitoring

Application, infrastructure and access logs are collected centrally and kept for at least 12 months. Error telemetry is processed through Sentry with automatic scrubbing of known sensitive fields.

Automated alerts cover anomalous authentication, privilege escalation and infrastructure integrity events.

6. Vulnerability management and secure development

Critical security patches are applied within 7 days of release where feasible. Dependency scanning and static analysis run in the build pipeline, and dynamic testing runs on staging before major releases. An independent penetration test of the platform is carried out at least annually; an executive summary is available under NDA. Code changes require peer review, and engineers receive annual secure coding training.

7. Backup and business continuity

Encrypted database backups are taken daily and kept for 30 days in the same EEA region. Recovery time objective: 8 hours. Recovery point objective: 24 hours. Restores are tested at least annually, and a business continuity and disaster recovery plan is reviewed annually.

8. Personal Data Breach response

A documented incident response plan covers triage, containment, eradication, recovery and post-incident review. Breaches are notified to the Controller as set out in clause 6.

9. Personnel security

Personnel with potential access to Customer Personal Data are bound by written confidentiality obligations that survive their employment, are background checked where the law allows, and complete security and data protection training at onboarding and at least annually.

10. Physical security

Production data is hosted only in AWS data centres. Kolay IK offices use controlled entry, visitor logging and clear-desk and clear-screen rules. No Customer Personal Data is stored on office infrastructure.

11. Endpoint security

Workstations are centrally managed with full-disk encryption, endpoint detection and response, automatic screen lock and enforced updates. Removable media may not be used for Customer Personal Data.

12. Sub-processor oversight

Sub-processors are engaged only after security and data protection due diligence and are bound by obligations materially equivalent to this DPA, including this Annex.

13. Data segregation

The platform is multi-tenant. Tenant isolation is enforced at the application layer on every data access, with automated tests against cross-tenant access.

14. Return and secure deletion

On termination, Customer Personal Data is deleted from live systems within 30 days and from backups when the backup retention cycle ends (up to 30 further days), unless UK law requires retention. Deletion uses cryptographic erasure or overwrite methods consistent with NIST SP 800-88.

15. Governance and review

These measures are owned by the Processor's information security function and reviewed at least annually as part of the ISO 27001 management review.