

justtrack Data Processing Agreement (DPA)

justtrack GmbH, An der Alster 42, 20099 Hamburg, Germany

Version 1.0 — 28 July, 2026

1. Scope and Incorporation

1.1 This Data Processing Agreement (“DPA”) forms part of the agreement between justtrack GmbH (“justtrack” or the “Processor”) and the customer identified in the associated Account or Order Form (the “Customer” or the “Controller”) governing the use of the justtrack platform (the “Agreement”). It is incorporated into the Agreement by reference and applies automatically upon creation of an Account; no separate signature is required. Where the Parties have separately executed this DPA or an equivalent data processing agreement, the separately executed version prevails.

1.2 This DPA applies to the processing of personal data by justtrack on behalf of the Customer in connection with the provision of the Service (“Customer Personal Data”), in particular End User data collected through the SDK. It does not apply to personal data that justtrack processes as a controller (e.g. account, billing and contact data of the Customer’s personnel), which is described in the justtrack Privacy Notice.

1.3 Capitalized terms not defined in this DPA have the meaning given in the Agreement. “GDPR” means Regulation (EU) 2016/679; the terms “controller”, “processor”, “data subject”, “processing”, “personal data” and “personal data breach” have the meaning given in the GDPR.

2. Roles; Details of Processing

2.1 The Customer is the controller and justtrack is the processor of Customer Personal Data. The Customer is responsible for the lawfulness of the collection of Customer Personal Data and of its transfer to justtrack, including any required notices to and consents of data subjects.

2.2 The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

3. Instructions

3.1 justtrack processes Customer Personal Data only on documented instructions from the Customer, unless required to do otherwise by Union or Member State law to which justtrack is subject; in such a case, justtrack informs the Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

3.2 The Agreement, this DPA and the Customer’s configuration of the Service (including the activation or deactivation of features, integrations and data sharing with advertising networks) constitute the Customer’s

complete instructions at the time of conclusion. Additional instructions require agreement between the Parties; justtrack may charge reasonable compensation for instructions exceeding the agreed scope of the Service.

3.3 justtrack informs the Customer without undue delay if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions; it may suspend the implementation of the instruction until confirmed or amended by the Customer.

4. Confidentiality

4.1 justtrack ensures that persons authorized to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and process the data only as instructed.

5. Security of Processing

5.1 justtrack implements and maintains appropriate technical and organizational measures pursuant to Art. 32 GDPR to ensure a level of security appropriate to the risk. The measures implemented at the date of this DPA are described in Annex 2. justtrack may update the measures provided that the level of security is not reduced.

6. Subprocessors

6.1 The Customer grants justtrack general authorization to engage subprocessors for the processing of Customer Personal Data. The subprocessors engaged at the date of this DPA are listed at <https://justtrack.io/subprocessors/> (the "Subprocessor List").

6.2 justtrack will inform the Customer of any intended addition or replacement of a subprocessor at least thirty (30) days before the new subprocessor starts processing Customer Personal Data, by updating the Subprocessor List and notifying the Customer by email to the Account address and/or via an in-product notice. Customers may additionally subscribe to notifications of changes to the Subprocessor List on the Subprocessor List page.

6.3 If the Customer has a legitimate data protection reason to object to a new subprocessor, it may object in text form within the notice period, stating the reasons. The Parties will then seek a mutually acceptable solution (e.g. a configuration avoiding the subprocessor). If no solution is found within a reasonable period, either Party may terminate the affected Service with effect from the date on which the new subprocessor takes up the processing; prepaid fees for the period after termination are refunded pro rata.

6.4 justtrack imposes on each subprocessor, by way of contract, data protection obligations essentially equivalent to those set out in this DPA, and remains fully liable to the Customer for the performance of the subprocessor's obligations.

7. Assistance; Data Subject Rights

7.1 Taking into account the nature of the processing, justtrack assists the Customer by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests for exercising data subject rights (Arts. 12–22 GDPR). If a data subject contacts justtrack directly, justtrack forwards the request to the Customer without undue delay and does not respond on the merits without the Customer's instruction, unless legally required.

7.2 justtrack assists the Customer, taking into account the nature of the processing and the information available to it, in ensuring compliance with the obligations pursuant to Arts. 32–36 GDPR (security, breach notification, data protection impact assessments, prior consultation).

8. Personal Data Breach

8.1 justtrack notifies the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. The notification contains at least the information pursuant to Art. 33(3) GDPR, to the extent available, and may be provided in stages. justtrack takes reasonable measures to mitigate the effects of the breach and documents the breach in accordance with Art. 33(5) GDPR. Notifications to supervisory authorities and data subjects are the Customer's responsibility.

9. Audit

9.1 justtrack makes available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR. justtrack primarily provides such demonstration through current audit reports, certifications or equivalent documentation.

9.2 Where such documentation is not sufficient in the individual case, the Customer or an auditor mandated by it (not a competitor of justtrack) may conduct an audit, including an inspection, of the processing operations concerned, during regular business hours, upon reasonable prior notice of at least thirty (30) days, no more than once per calendar year (except following a personal data breach or where required by a supervisory authority), subject to appropriate confidentiality undertakings. Each Party bears its own costs of the audit.

10. International Transfers

10.1 justtrack processes Customer Personal Data in data centers located in the European Union. Where Customer Personal Data is transferred to a third country without an adequacy decision – including remote access by a subprocessor from such a country – justtrack ensures an appropriate safeguard pursuant to Chapter V GDPR, in particular the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914, Module Three: processor to processor, or Module Two where applicable), which are incorporated into the contracts with the relevant subprocessors, supplemented where required by additional measures.

11. Deletion and Return of Data

11.1 During the term of the Agreement, raw Customer Personal Data is retained on a rolling basis for the operational retention period specified in the Documentation, after which it is deleted or aggregated.

11.2 Upon termination of the Agreement, the Customer may export Customer Personal Data via the export functions of the Service for thirty (30) days. After expiry of this period, justtrack deletes all Customer Personal Data, unless Union or Member State law requires storage. Data in backup systems is deleted or overwritten in the course of routine backup cycles, at the latest [90] days after the deletion from production systems; until then, backup data is not restored to production except where necessary for disaster recovery, in which case the deletion obligation re-applies.

11.3 Upon the Customer's request, justtrack confirms the deletion in text form.

12. AI-Supported Features

12.1 justtrack may use AI-supported services to provide and optimize the Service. Where AI-supported features process Customer Personal Data, such processing takes place exclusively within the infrastructure of the subprocessors named in the Subprocessor List, in accordance with this DPA and the Customer's instructions. Customer Personal Data is not used to train foundation models of justtrack or of third parties.

13. Liability; Miscellaneous

13.1 The liability provisions of the Agreement apply to this DPA. Art. 82 GDPR remains unaffected in the relationship towards data subjects.

13.2 In the event of a conflict between this DPA and the Agreement with respect to the processing of Customer Personal Data, this DPA prevails. Amendments to this DPA follow the amendment mechanism of the Agreement; justtrack may additionally amend this DPA where required by data protection law or supervisory guidance, notifying the Customer in accordance with the Agreement.

13.3 This DPA is governed by the law applicable to the Agreement. It terminates automatically with the Agreement, without prejudice to obligations that by their nature survive (in particular Clause 11).

Annex 1 – Details of Processing

Subject matter: Provision of the justtrack platform for mobile/web app attribution, analytics and campaign performance measurement.

Duration: Term of the Agreement, plus the export and deletion periods under Clause 11.

Nature and purpose: Collection of event data via the SDK and server-to-server interfaces; attribution of installs and in-app events to marketing campaigns; aggregation, analysis and reporting; forwarding of postbacks to advertising networks as configured by the Customer; provision of exports and APIs; where activated, AI-supported analysis and campaign optimization.

Categories of data subjects: End Users of the Customer's Apps.

Types of personal data: device identifiers (e.g. IDFA, IDFV, GAID, Android ID, App Set ID); IP address; app interaction data (e.g. installs, sessions, clicks, views, in-app events); technical information (e.g. device type, OS version, network); coarse location (e.g. city level, derived from IP address). No special categories of personal data are intended to be processed; the Customer shall not submit such data.

Annex 2 – Technical and Organizational Measures (TOMs)

Placeholder – to be completed with input from engineering. Structure: (1) physical access control (AWS data centers, certifications); (2) system access control (SSO, MFA, role-based access, least privilege); (3) data access control (logging, segregation per customer/tenant); (4) transmission control (TLS in transit, encryption at rest); (5) input control (audit logs); (6) availability control (backups, multi-AZ, disaster recovery); (7) separation control (logical tenant separation in the Kubernetes infrastructure); (8) organizational measures (confidentiality undertakings, training, DPO: KINAST Rechtsanwaltsgesellschaft mbH, incident response process); (9) review cadence.

Annex 3 – Subprocessors

The current list of subprocessors, including the processing purpose, location and transfer mechanism per subprocessor, is published and maintained at <https://justtrack.io/subprocessors/> and forms part of this DPA. Changes to the list are governed by Clause 6.