Data Processing Agreement

under Article 28 of Regulation (EU) 2016/679 (GDPR) for the Flaree service
Version 1.0 - 13 October 2026

Parties

Controller	The customer that has accepted the Flaree Terms of Service, identified by the company and billing details in its Flaree account (the "Controller")
Processor	Mobile Reality sp. z o.o., registered in Warsaw, Poland, operator of Flaree (the "Processor"). Registered address: ul. Grzybowska 62, lokal 02-104, 00-844 Warszawa, Poland. Entered in the National Court Register (KRS) under number 0000608261 (registry court: Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego); NIP 7010559296; REGON 363981117; share capital PLN 50,000.00. Contact for data protection matters: biuro@mobilereality.pl. According to the KRS, any member of the management board may represent the company alone.
Main agreement	The Flaree Terms of Service (flaree.app/terms-of-service), accepted by the Controller's authorised representative at registration, together with the Controller's subscription plan and any order (the "Main Agreement").

1. Subject-matter, duration, nature and purpose of the processing

1. **Subject-matter.** The Processor processes personal data on behalf of the Controller to provide the Flaree service described in the Main Agreement.
2. **Duration.** The processing lasts for as long as the Controller's Flaree account is open under the Main Agreement, and ends as described in section 10. Effective date: the date on which the Controller accepts the Terms of Service.
3. **Nature and purpose.** Hosting, backup, export and deletion of the Controller's company data, and the operations listed in Annex I (emails and push notifications, Slack and Microsoft Teams messages, survey and recognition features, AI-assisted features, fraud and abuse prevention, error monitoring), solely to deliver the service to the Controller.
4. **Roles.** The Controller determines the purposes and means of processing the personal data of its employees and other users in Flaree and acts as controller. The Processor processes that data on the Controller's behalf and acts as processor. The Processor acts as an independent controller only for data it needs for its own purposes, such as account administration, billing, security and service improvement, as described in its Privacy Policy. This DPA does not cover that processing.

Billing, payment and invoicing data relating to the Controller as a customer is processed by the Processor as an independent controller.

2. Types of personal data and categories of data subjects

1. **Data subjects.** Employees and other users of the Controller's company who hold a Flaree account or have been invited, and the Controller's company representatives. A user reaches only their own company's data.
2. **Types of personal data.** Identification and contact: full name, email address, password (stored as a hash), profile image. Account and access: company membership, role and permissions, department, invitation and onboarding status, session tokens, sign-in provider identifiers (Google, Microsoft, LinkedIn), Slack user ID. Dates: birthday and work anniversary, where provided. Activity and content: recognition cards and their comments, points and badges, Flareeboard messages and images, survey answers and check-in conversation transcripts, culture book text, event notes. Device and network: push notification token, and the IP address recorded at registration with a fraud-risk score. Notifications: content and delivery status of emails and push notifications. Integration data: Slack workspace installation data and API keys.
3. **Special categories of data (Article 9) and data on criminal convictions.** The service has no field designed to collect special categories of personal data (Article 9) or data on criminal convictions, and the Processor does not analyse content to infer them. Free-text fields (recognition comments, survey answers, check-in conversations, Flareeboard messages) accept unrestricted text, so users could enter such data. The Controller decides which survey questions it asks and instructs its users not to enter such data.

3. Processing only on documented instructions (Art. 28(3)(a))

1. The Processor processes personal data only on documented instructions from the Controller, including with regard to transfers to a third country, unless Union or Member State law to which the Processor is subject requires otherwise. In that case the Processor informs the Controller of the legal requirement before processing, unless that law prohibits such information.
2. The Controller's documented instructions at acceptance are this DPA, the Main Agreement, and the Controller's configuration and use of the Flaree features. Further instructions are given in writing.
3. The Processor informs the Controller without undue delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection law.

4. Confidentiality (Art. 28(3)(b))

1. The Processor ensures that every person authorised to process the personal data has committed to confidentiality or is under an appropriate statutory obligation of confidentiality.
2. Access to the Controller's personal data is limited to the Processor's management board and its employees in software development roles.

5. Security of processing (Art. 28(3)(c) and Art. 32)

The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The measures published by the Processor on its Security page are listed in Annex II. The Processor may update the measures, provided the overall level of protection is not reduced.

6. Sub-processors (Art. 28(3)(d), Art. 28(2) and 28(4))

1. The Controller gives general written authorisation for the Processor to engage the sub-processors named in Annex III.
2. The current list is published at **flaree.app/sub-processors**. The Processor names every third party that processes data on its behalf, and what each one handles.
3. The Processor informs the Controller of an intended addition or replacement of a sub-processor at least 14 days in advance, by updating the public list and notifying the Controller's administrator by email. The Controller may object on reasonable data protection grounds within that period. The parties then discuss in good faith, and if no solution is found the Controller may terminate the affected service.
4. The Processor imposes on each sub-processor the same data protection obligations as in this DPA, by contract, and remains liable to the Controller for the sub-processor's performance of those obligations.

7. Assistance with data-subject requests (Art. 28(3)(e))

1. Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the Controller's obligation to respond to requests to exercise data-subject rights under Chapter III of the GDPR.
2. Company administrators export their employee data from the dashboard at any time, and can request a full machine-readable export by email.
3. The Processor forwards a data-subject request it receives directly to the Controller without undue delay and does not answer it on its own initiative unless instructed. The Processor provides assistance within 72 hours of the Controller's request.

8. Assistance with Articles 32 to 36 (Art. 28(3)(f))

Taking into account the nature of the processing and the information available to it, the Processor assists the Controller in ensuring compliance with:

- Article 32, security of processing (section 5 and Annex II);
- Articles 33 and 34, notification and communication of personal data breaches (section 9);
- Article 35, data protection impact assessments, and Article 36, prior consultation. The Processor provides this assistance within 72 hours of the Controller's request.

9. Personal data breach notification (Art. 33(2))

1. The Processor notifies the Controller without undue delay after becoming aware of a personal data breach affecting the Controller's personal data. The Processor notifies the Controller within 72 hours.
2. The notification describes, as far as then known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Notification is sent by email to the Controller's account administrator and to any data protection contact the Controller names in writing.
3. Assistance with the Controller's notification duties under Articles 33 and 34 is as set out in section 8.

10. Deletion or return of data at the end of the services (Art. 28(3)(g))

1. Personal data is kept while the Controller's account is open.
2. On the Controller's choice at the end of the services, the Processor deletes the personal data or returns it. Administrators can export their employee data from the dashboard, and can request a full machine-readable export by email.
3. When the Controller asks the Processor to delete an account, the Processor removes it from the production database. The last backup copy expires 30 days later, as backups are retained for 30 days and then deleted.
4. The Processor deletes existing copies unless Union or Member State law requires storage of the personal data. The Processor completes deletion from the production database within 72 hours of the Controller's request or of the end of the services.

11. Audits and information (Art. 28(3)(h))

1. The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR, and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.
2. Audits take place at most once every 12 months, or after a confirmed personal data breach, on at least 30 days' written notice, during business hours and for no more than two working days. They cover only the processing under this DPA, do not give access to other customers' data, and are subject to confidentiality. The Processor may offer current documentation or an independent audit report as an alternative to an on-site audit. The Controller decides whether that is sufficient and keeps its right to inspect where it considers an inspection necessary. Each party bears its own costs.

12. International transfers

1. The Processor runs Flaree's application servers, production database and its backups on Amazon Web Services in the eu-central-1 region, Frankfurt, Germany.

2. Some sub-processors in Annex III are located outside the European Economic Area or operate there (for example OpenAI, Google and Sentry). Where personal data is transferred to such a sub-processor, the Processor relies on a transfer mechanism under Chapter V of the GDPR: the sub-processor's participation in the EU-U.S. Data Privacy Framework, or Standard Contractual Clauses. The mechanism for each sub-processor is stated in Annex III.

13. Liability and relationship to the Main Agreement

1. Liability under this DPA follows the liability provisions of the Main Agreement and applicable law. This DPA adds no separate liability cap.
2. If this DPA and the Main Agreement conflict on the processing of personal data, this DPA prevails.
3. This DPA is governed by Polish law. The courts competent for the Processor's registered office in Warsaw have jurisdiction.
4. This DPA takes effect on the date on which the Controller accepts the Terms of Service and stays in force while the Processor processes personal data on the Controller's behalf, that is for the term of the Main Agreement. It ends automatically with the Main Agreement. Sections 4, 10 and 13 continue until the deletion under section 10 is complete.

Acceptance

This DPA is incorporated into the Main Agreement by reference. It takes effect, without a separate signature, when the Controller accepts the Terms of Service, and it binds both parties from that date. The Processor's details are those in the Parties section; the Controller's details are those in its Flaree account. A copy signed by both parties is available on request.

Annex I - Description of the processing

Item	Description
Controller	The customer, as identified in its Flaree account
Processor	Mobile Reality sp. z o.o., Warsaw, Poland
Service	The Flaree service, as described in the Main Agreement
Data subjects	Employees and other users of the Controller's company who hold a Flaree account or have been invited; the Controller's company representatives
Types of personal data	Identification and contact: full name, email address, password (stored as a hash), profile image. Account and access: company membership, role and permissions, department, invitation and onboarding status, session tokens, sign-in provider identifiers (Google, Microsoft, LinkedIn), Slack user ID. Dates: birthday and work anniversary, where provided. Activity and content: recognition cards and their comments, points and badges, Flareeboard messages and images, survey answers and check-in conversation transcripts, culture book text, event notes. Device and network: push notification token, and the IP address recorded at registration with a fraud-risk score. Notifications: content and delivery status of emails and push notifications. Integration data: Slack workspace installation data and API keys.
Special categories	None collected by design; free-text fields could contain such data if users enter it (section 2.3)
Operations	Hosting, backup, export and deletion; account, invitation, reminder and notification emails; push notifications; Slack and Microsoft Teams messages and member lookups; the survey check-in assistant and card and brand generation using OpenAI; IP fraud-risk analysis at registration; error monitoring; scheduled jobs (reminders, badges, event points); CSV and Excel import and user export
Duration	While the Controller's account is open; deletion as in section 10
Location of processing	Application, database and backups: Amazon Web Services, eu-central-1, Frankfurt, Germany. Other sub-processors: see Annex III

Annex II - Technical and organisational measures (Art. 32)

As published on the Processor's Security page.

Area	Measure
Data residency	Application servers, the production database and its backups are in AWS eu-central-1, Frankfurt, Germany.

Encryption at rest	Data at rest is encrypted with AES-256.
Encryption in transit	Data in transit is encrypted with TLS 1.2 or higher. The load balancer and the CDN both reject earlier versions.
Access control	Each account carries a role, and each role carries an explicit set of permissions. A user reaches only their own company's data, and only the parts their role allows. Company administrators assign and revoke roles from the dashboard.
Backups	The production database is backed up daily, in the same region. Backups are retained for 30 days and then deleted.
Retention and deletion	Data is kept while the account is open. On account deletion it is removed from the production database, and the last backup copy expires 30 days later.
Vulnerability reporting	Vulnerabilities are reported to security@flaree.app; the same contact details are published at /.well-known/security.txt.
Personnel access	Access to customer personal data is limited to the Processor's management board and its employees in software development roles.
Further measures	Regular security training for personnel.

Annex III - Sub-processors

The Processor publishes its sub-processor list at **flaree.app/sub-processors**. At the date of this version, the sub-processors below process personal data of the Controller's users. The location and transfer basis are stated per sub-processor and come from each provider's published terms. Items in red are still to be resolved.

Sub-processor	Processing	Personal data involved	Location
Amazon Web Services	Hosting, database, file storage, CDN, queues, key management, email delivery (Amazon SES)	All categories in Annex I; for email delivery, name, email address and message content	eu-central-1, Frankfurt, including Amazon SES (the CDN is global)

Google (Firebase Cloud Messaging)	Push notifications	Push token, notification content	USA. EU-U.S. Data Privacy Framework certification and the Standard Contractual Clauses in Google's Firebase data processing terms
OpenAI	Survey check-in assistant; card text and artwork generation	Survey answers and conversation text; company description and culture text	Ireland (OpenAI Ireland Ltd, the contracting entity for customers in the EEA) and the USA. Transfers within OpenAI rely on agreements containing Standard Contractual Clauses; OpenAI's sub-processor list is published at platform.openai.com/subprocessors
Brevo	Marketing contact list, once the user's email address is confirmed	Name, email address	EU hosting (France, Germany, Belgium). Standard Contractual Clauses and the EU-U.S. Data Privacy Framework for access from non-EU group companies
Scamalytics	Fraud-risk score of the registration IP address	IP address	UK (Scamalytics Ltd, London). Transfer relies on the EU adequacy decision for the UK, renewed until 27 December 2031
IPinfo	Location lookup of the registration IP address	IP address	USA (IPinfo Inc). Standard Contractual Clauses (Module Two) and UK Addendum in its data processing agreement
Cloudflare (Turnstile)	Bot protection on forms	IP address and browser signals	Global. EU-U.S. Data Privacy Framework certification, with Standard Contractual Clauses as fallback
Sentry	Error monitoring and sampled frontend session replay	Technical data, user identifiers	EU data storage in Frankfurt (de.sentry.io). Functional Software, Inc. (USA) is certified under the EU-U.S. Data Privacy Framework
Tidio	Support chat	Name, email address, company, plan, role	USA and Poland. Tidio LLC as processor under a data processing agreement with Standard Contractual Clauses (Module Two); Tidio Poland Sp. z o.o. as sub-processor
Google (Tag Manager, Analytics, Ads)	Usage analytics and conversion measurement, subject to cookie consent	User identifier, hashed email address	USA. EU-U.S. Data Privacy Framework certification and Standard Contractual Clauses in Google's data processing terms

Meta, Microsoft Clarity, LinkedIn Analytics, Fraud Blocker, HubSpot	Marketing and analytics tags loaded through Google Tag Manager on the Processor's website and application, only after the user has accepted the matching cookie category (consent defaults to denied)	Browser identifiers and page activity; for sign-up conversion events, the email address	USA. Meta Platforms, Inc., Microsoft and HubSpot, Inc. state EU-U.S. Data Privacy Framework certification; LinkedIn Corporation also states its EU-U.S. Data Privacy Framework certification and relies on Standard Contractual Clauses; Fraud Blocker relies on Standard Contractual Clauses

Slack, Microsoft Teams and the sign-in providers (Google, Microsoft, LinkedIn) are platforms the Controller or its users choose to connect. Data moves between Flaree and the Controller's own workspace or account. The configuration of the Google Tag Manager container is outside the source code, so which tag fires on which page is managed by the Processor's marketing team.