Data Processing Agreement

(Umowa Powierzenia Przetwarzania Danych)

pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)

Forming an integral part of the Terms of Service of the Quack Runners platform

between:

Processor: Quack Foundry, represented by Michał Żak, conducting unregistered business activity, with registered office at ul. Sienna 9, 70-542 Szczecin, Poland (hereinafter: "Processor").

and

Controller: The entity identified in the Quack Runners account, acting as an event organizer (hereinafter: "Controller").

Date: February 8, 2026 **Contact:** hello@quackfoundry.com

WHEREAS the Controller uses the Quack Runners platform for the management of photos from sporting events, which involves the processing of personal data of event participants; and WHEREAS the Parties wish to ensure compliance with the GDPR and applicable Polish data protection law.

THE PARTIES AGREE AS FOLLOWS:

§ 1. Subject Matter and Scope

1. The Controller entrusts the Processor with the processing of personal data in accordance with Article 28 of the GDPR, solely for the purpose of providing the Service: hosting, organizing, and distributing photos from sporting events,

including bib number recognition via automated image analysis and OCR technology.

2. This Agreement takes effect upon the Controller's first use of the Service. The first login to the platform constitutes acceptance of this Agreement, the Terms of Service, and the Privacy Policy.
3. Categories of data subjects: (a) participants of sporting events organized by the Controller; (b) employees and associates of the Controller using the platform.
4. Types of personal data processed: identification data (name, surname, bib number), contact data (email address), image data (event photos and metadata), technical and session data (IP addresses, authentication tokens, device information), payment data (Stripe customer IDs, payment statuses), and audit logs.
5. The system uses automated image analysis and OCR technology provided by Amazon Web Services to identify bib numbers on participants' shirts. The system does not process biometric data or special categories of personal data within the meaning of Article 9 of the GDPR.

§ 2. Processor Obligations

The Processor undertakes to:

1. Process personal data only on the documented instruction of the Controller. Account configuration, file uploads, and acceptance of the Terms of Service are considered documented instructions. The Processor shall immediately inform the Controller if an instruction infringes the GDPR.
2. Ensure that all persons authorized to process personal data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality.
3. Implement appropriate technical and organizational measures pursuant to Article 32 of the GDPR to ensure a level of security appropriate to the risk, including encryption of data in transit (TLS 1.2+) and at rest (AES-256), passwordless authentication, role-based access control, audit logging, and regular backups. Detailed security documentation is available to the Controller upon written request.
4. Assist the Controller in responding to data subject requests under Articles 15–22 of the GDPR, by providing appropriate tools in the administration panel (data export, deletion, correction, search by email or bib number).

5. Assist the Controller in ensuring compliance with Articles 32–36 of the GDPR (security, breach notification, impact assessments), considering the nature of processing and information available to the Processor.
6. At the Controller's choice, delete or return all personal data upon termination of the Service, and delete existing copies unless applicable law requires retention.
7. Make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR.

§ 3. Sub-processors

1. The Controller grants the Processor general written authorization to engage sub-processors. The Processor shall ensure that each sub-processor is bound by data protection obligations no less protective than those in this Agreement.
2. The following sub-processors are engaged as of the date of this Agreement:

Sub-processor	Purpose	Location	Safeguards
Amazon Web Services EMEA SARL	Cloud infrastructure, storage, email (SES), OCR	EU (Frankfurt, Germany)	AWS DPA, Art. 28 GDPR
Vercel Inc.	Frontend hosting, serverless functions	US + global edge	DPF + SCC
Stripe Technology Europe Ltd.	Payment processing	EU (Ireland) + US	Stripe DPA, PCI DSS L1, SCC
Functional Software Inc. (Sentry)	Error monitoring (production)	USA	Sentry DPA, DPF, SCC
Google Ireland Limited	OAuth authentication	EU (Ireland) + global	Google DPA, DPF, SCC

3. The Processor shall notify the Controller of any intended changes to sub-processors at least 14 calendar days in advance by email. The Controller may object within 14 days; if the objection is not resolved, the Controller may terminate

this Agreement with immediate effect and is entitled to data export pursuant to § 7.

4. The current list of sub-processors is maintained at https://www.quack-runners.com/legal/sub-processors.

§ 4. Audit Rights

1. The Controller has the right to verify the Processor's compliance with this Agreement, including through audits and inspections.
2. The primary form of audit shall be the Processor providing security documentation and compliance information upon the Controller's written request.
3. On-site audits may be conducted with at least 30 calendar days' advance notice and mutual agreement on scope. Audit costs are borne by the Controller, unless the audit reveals a material breach by the Processor.

§ 5. Personal Data Breach Notification

1. The Processor shall notify the Controller of any personal data breach without undue delay, and no later than 48 hours after becoming aware of the breach.
2. The notification shall include, to the extent available: (a) description of the nature of the breach and categories/number of data subjects affected; (b) likely consequences; (c) measures taken or proposed to address the breach; (d) contact details for further information.
3. The Processor shall cooperate with the Controller in assessing notification obligations under Articles 33–34 of the GDPR, notifying data subjects where required, and documenting the breach.

§ 6. Duration and Data Retention

1. This Agreement remains in force for the duration of the Controller's active account and terminates automatically upon termination of the Principal Agreement (Terms of Service).
2. The Controller controls the retention of most data and may delete individual data sets at any time via the administration panel.
3. Specific retention periods:

Data Category	Retention Period
Session tokens	7 days (automatic TTL)
OTP codes	5 minutes (max 3 attempts)
OAuth state tokens	10 minutes
Organization invitations	7 days (automatic TTL)
Photo access links (presigned URLs)	1 hour
Audit logs — high severity	7 years
Audit logs — compliance/financial	5 years
Audit logs — standard	90 days
Event and participant data	Until deleted by Controller
Photos	Until deleted by Controller
Invoices / payment data	Min. 5 years (Art. 86 § 1 Tax Ordinance)

4. Upon termination: (a) the Processor shall make a full data export available within 14 calendar days (30 days for data sets over 10 GB); (b) the export download link shall remain active for 30 days; (c) after the export period, the Processor shall delete all entrusted data within 60 days, except data required by law; (d) written confirmation of deletion is available upon request.

§ 7. Data Export

1. Upon termination or at the Controller's request, the Processor shall provide a full export of entrusted personal data, including: participant data (CSV/JSON), event metadata (JSON), photo file lists with assignments, audit logs (to the extent permitted by retention policy), and billing data not subject to mandatory retention.
2. Photos shall be provided as a ZIP archive or as time-limited download links. The Controller is responsible for downloading and securely storing the export within the provided timeframe.

§ 8. Obligations of the Controller

1. The Controller represents and warrants that: (a) it has a legal basis for processing participant data under Article 6 GDPR; (b) it has obtained all necessary consents

or established another lawful basis before transmitting data to the platform; (c) it has provided participants with all information required under Articles 13–14 GDPR; (d) the submitted data is accurate and current.

2. The Controller shall not transmit special categories of personal data (Article 9 GDPR) to the platform without the express prior consent of the Processor.

3. The Controller is solely responsible for: handling data subject requests, reporting breaches to supervisory authorities and data subjects where required, conducting DPIAs where applicable, and compliance with all applicable data protection laws.

4. The Processor does not verify whether the Controller has obtained appropriate consents. By using the Service, the Controller confirms compliance with GDPR requirements as a Data Controller.

§ 9. Liability

1. The Processor shall be liable for damages caused by processing only insofar as it has failed to comply with obligations under the GDPR specifically directed at processors, or has acted outside or contrary to the Controller's lawful instructions.

2. The total aggregate liability of the Processor shall not exceed the greater of: (a) the total fees paid by the Controller in the 12 months preceding the claim; or (b) the total fees paid for the specific event to which the claim relates.

3. The Processor shall not be liable for lost profits (lucrum cessans).

4. The limitations in this section shall not apply to damages caused intentionally or through gross negligence.

5. Each Party's liability under Articles 82–83 of the GDPR remains unaffected.

§ 10. International Data Transfers

1. Personal data may be transferred outside the EEA in connection with sub-processors listed in § 3. Transfers to the United States are safeguarded by the EU-U.S. Data Privacy Framework (DPF) and Standard Contractual Clauses (SCC, Commission Implementing Decision 2021/914).

2. Data processed by AWS is stored by default in the eu-central-1 region (Frankfurt, Germany) and is not transferred outside the EEA without the Controller's agreement.

3. The Processor shall provide copies of applicable transfer mechanisms and Transfer Impact Assessments upon the Controller's written request.

4. In the event of a material change to transfer mechanisms, the Processor shall promptly notify the Controller and, if acceptable alternatives cannot be provided, permit termination of this Agreement.

§ 11. Final Provisions

1. This Agreement shall be governed by Polish law. In matters not regulated herein, the GDPR and applicable Polish data protection legislation shall apply.
2. Disputes shall be resolved by the court having jurisdiction over the Processor's registered office (Szczecin, Poland).
3. Amendments require written form (including electronic) under pain of nullity.
4. If any provision is found invalid or unenforceable, the remaining provisions shall remain in full force. The invalid provision shall be replaced by a valid provision most closely reflecting its economic purpose.
5. In the event of company registration (Quack Foundry sp. z o.o. or Quack Foundry UG), the Processor shall notify the Controller at least 14 days in advance. This Agreement shall transfer to the successor entity unless the Controller objects within 7 days.
6. Detailed technical and organizational security documentation (Article 32 GDPR) is available to the Controller upon written request to hello@quackfoundry.com.