AQIRA DATA PROCESSING AGREEMENT (DPA)

1. Parties

This Data Processing Agreement ("Agreement") is entered into and made effective as of **19.05.2026**, by and between:

- **Data Controller:** [Owner of Aqira Platform], (hereinafter referred to as the "Company" or "Data Controller").
- **Data Processor:** [Name of Service Provider / Agency / Partner], (hereinafter referred to as the "Processor").

(The Data Controller and the Processor may individually be referred to as a "Party" and collectively as the "Parties".)

2. Purpose and Scope

This Agreement is supplemental to the **19.05.2026** dated [Main Service Agreement Name] ("Main Agreement") entered into by the Parties. The purpose of this Agreement is to govern the processing, protection, security, and confidentiality of personal data processed by the Processor on behalf of the Data Controller, in accordance with applicable data protection laws (including GDPR and KVKK).

3. Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Processing:** Any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination, or destruction.
- **Data Controller:** The natural or legal person which determines the purposes and means of the processing of personal data (Aqira).
- **Data Processor:** The natural or legal person which processes personal data on behalf of the Data Controller.

4. Processing Obligations and Instructions

The Processor agrees and covenants that it will handle personal data under the following conditions:

- Process personal data only on documented written instructions from the Data Controller and within the scope defined in the Main Agreement.
- Never process personal data for its own purposes, marketing, or for the commercial interests of any third party.

- If the Processor is required by applicable law to act outside the Data Controller's instructions, it shall notify the Data Controller in writing before processing (unless prohibited by law on important grounds of public interest).

5. Data Security and Technical Measures

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of unlawful processing or unauthorized access. At a minimum, these measures include:

- Protecting infrastructure where data is stored against cyber-attacks (firewalls, encryption at rest, strict access logging).
- Limiting access to personal data strictly to personnel who need it to fulfill the Main Agreement, ensuring such personnel are bound by strict confidentiality agreements.
- Utilizing industry-standard end-to-end encryption (e.g., SSL/TLS) during data transmission between systems.

6. Data Breach Notification

In the event that the Processor detects a security incident involving unauthorized access, leakage, or loss of personal data under its custody:

- The Processor must notify the Data Controller in writing without undue delay, and no later than **24 hours** after becoming aware of the breach.
- The notification must include the categories of data affected, the approximate number of data subjects, the likely consequences of the breach, and the remedial measures taken or planned.
- The Processor will fully cooperate with the Data Controller to mitigate the effects of the breach.

7. Sub-processors

The Processor shall not engage another processor (Sub-processor) to handle Aqira’s personal data without the prior specific or general written authorization of the Data Controller. If authorization is granted, the Processor must impose the exact same data protection obligations on the Sub-processor as set out in this Agreement via a formal contract.

8. Data Subjects' Rights and Audits

- **Data Subject Requests:** If a data subject (an Aqira user) contacts the Processor regarding data deletion, correction, or access, the Processor shall forward the request to the Data Controller immediately and provide necessary technical assistance to resolve it.
- **Audit Rights:** The Data Controller, or an independent auditor appointed by them, has the right to audit the Processor’s compliance with this Agreement upon reasonable prior written notice.

9. Term, Termination, and Return of Data

- This Agreement shall remain in effect for the entire duration of the Main Agreement.
- Upon termination of the Main Agreement, the Processor shall, at the choice of the Data Controller, securely delete or return all personal data, including all existing copies and backups, to the Data Controller, unless local legislation requires the retention of certain personal data.

Annex 1: Categories of Data and Data Subjects (Aqira Specific)

- **Categories of Personal Data Processed:** User identity data (name, surname, username), contact details (email, phone number), device information (IP address, Device ID, OS), financial data (purchase history, in-app wallet balance), audio-visual data (live stream recordings, profile photos, voice messages).
- **Categories of Data Subjects:** Aqira mobile application users, live stream hosts (broadcasters), and agency administrators.