DATA PROCESSING AGREEMENT

GDPR-compliant agreement defining how worker personal data is handled

Issued by ASL Seasonal Labor Platform | Date: 04.11.2026

1. Introduction & Legal Basis

This Data Processing Agreement ("DPA") forms part of the Standard Service Agreement between ASL Seasonal Labor Platform ("Controller / Processor") and the Employer ("Controller") and governs the processing of personal data of workers pursuant to Article 28 of the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Processing is lawful under Article 6(1)(b) GDPR (performance of a contract to which the data subject is party) and Article 6(1)(c) GDPR (compliance with a legal obligation -- Norwegian UDI visa and German BA pre-approval requirements).

2. Categories of Personal Data Processed

The following categories of worker personal data are processed: Full legal name (as per passport), date of birth, nationality, passport number, passport issue and expiry dates, photograph, residential address (Thailand), work history, educational qualifications, agricultural skill certifications, and health fitness declarations required by UDI/BA.

Special category data (Article 9 GDPR): health-related data is processed only to the minimum extent required by Norwegian or German visa regulations and is stored encrypted at rest (AES-256).

3. Purposes of Processing

Personal data is processed exclusively for: (a) matching workers to suitable agricultural job requests; (b) generating government-mandated visa application forms (UDI GP-7028, BA Vermittlungsauftrag); (c) compliance with Thai Department of Employment (DOE) certified labor contract requirements; (d) worker welfare monitoring during placement.

Data shall not be used for any purpose other than those stated above without prior written consent from the data subject.

4. Data Retention

Worker personal data is retained for a maximum of 7 years from the end of the last employment contract to satisfy statutory accounting and labor law audit requirements. After expiry of this period, data is securely deleted using NIST 800-88 compliant methods.

Passport scan images and police clearance certificates are retained only for the duration of the visa application process and deleted within 90 days of visa issuance or rejection.

5. Sub-processors

The Agency uses the following approved sub-processors: Microsoft Azure SQL (database hosting, EU region), Stripe, Inc. (payment processing). No worker personal data is transferred to sub-processors outside the EEA or Thailand without adequate safeguards (Standard Contractual Clauses or equivalent).

6. Data Subject Rights

Workers have the right to access, rectify, erase, restrict processing of, and port their personal data. Requests must be submitted through the worker portal or by written request to the Agency's Data Protection Officer. Requests will be responded to within 30 days.

Workers have the right to lodge a complaint with the relevant supervisory authority: Datatilsynet (Norway), Bundesbeauftragter fuer den Datenschutz (Germany), or the Office of the PDPC (Thailand).

7. Security Measures

The Agency implements the following technical and organisational measures: AES-256 encryption at rest for sensitive documents; TLS 1.3 in transit; role-based access control (Admin, Employer, Worker roles); comprehensive audit logging of data access events; annual security review.

8. Breach Notification

In the event of a personal data breach, the Agency will notify affected Employers within 72 hours of becoming aware of the breach, as required by Article 33 GDPR.