SCHEDULE EEA DATA PROCESSING DETAILS

SUBJECT MATTER AND DURATION OF THE PROCESSING:
The subject matter of the Processing for EEA-covered Personal Data ("EEA PII") is described in the Services Agreement. S2Verify shall Process EEA PII solely for the purpose of providing the Services and only on behalf of and in accordance with the documented instructions of Customer in its capacity as Data Controller. The Processing shall continue for the duration of the Services Agreement, or for so long as S2Verify is authorized in writing by Customer to Process EEA PII, and shall cease upon the termination or expiration of such authorization in accordance with this Agreement.

NATURE AND PURPOSE OF THE PROCESSING:
S2Verify provides professional pre-employment background screening services and related support functions on behalf of Customer. Processing is limited to activities necessary to (i) conduct pre-employment and workforce screening, (ii) provide related compliance and reporting services, and (iii) fulfill Customer's lawful instructions.

TYPES OF EEA PII PROCESSED:
EEA PII may include the following categories of data associated with pre-employment and Human Resources-related screening activities:

☐ Title and Name
☐ Contact information (telephone number, physical address, email address)
☐ Employment history and application information (position, title, duties, personnel ID)
☐ Compensation and tax-related information
☐ Banking or financial account information (where legally required and instructed by Customer)
☐ Photographs or identity images (where provided or legally required)
☐ Government-issued identifiers
☐ Gender
☐ Date of birth

Special Categories of EEA PII (Only if Authorized and Lawful):
☐ EEA PII revealing racial or ethnic origin
☐ Trade-union membership information
☐ Health or medical-related information
☐ EEA PII relating to criminal convictions and offenses
Processing of Special Categories or criminal offence data shall occur only when instructed in writing by Customer, when necessary for Customer's obligations under applicable employment laws, and when a valid legal basis under Articles 9 or 10 of the GDPR applies.

CATEGORIES OF DATA SUBJECTS:
☐ Current, former, and prospective employees, job applicants, contractors, directors, and staff members
☐ Dependents or beneficiaries, where legally required or provided by Customer
☐ Client or client-authorized personnel, where applicable to background screening services
☐ Vendors or suppliers whose background screening is authorized by Customer

SCHEDULE EEA DATA PROCESSING DETAILS

OBLIGATIONS AND RIGHTS OF THE CUSTOMER:
The obligations and rights of the Customer as Data Controller are set forth in this Agreement. Customer represents that it has provided all required notices, obtained all required authorizations, instructions, and legal bases necessary for S2Verify to Process EEA PII on Customer's behalf.

RETURN AND DELETION OF DATA:
Upon termination or expiration of the Services Agreement, or upon written instruction from Customer, S2Verify shall securely return or delete EEA PII in accordance with Customer's documented instructions, subject to legal retention requirements.

Schedule: Technical & Organizational Security Measures (GDPR Art. 32)

Schedule X — Technical and Organizational Measures (TOMs)
S2Verify shall implement and maintain the following safeguards to protect EEA Personal Data ("EEA PII"), proportional to risk and compliant with Articles 28 and 32 of GDPR.

A. Access Control

- Role-based access controls ("RBAC") ensuring access only to authorized personnel.
- Multi-factor authentication (MFA) for administrative access and privileged accounts.
- Password management controls consistent with NIST/ISO/industry standards.
- Access logs for authentication, administrative actions, and data exports.

B. Physical & Environmental Controls

- Secure, access-controlled facilities and data center locations.
- Visitor controls, badges, logging, and restricted areas for servers.
- Redundant power, fire suppression, disaster safeguards.

C. Encryption & Data Protection

- Encryption in transit using TLS 1.2+ (or successor protocols).
- Encryption at rest using AES-256 or equivalent.
- Secure hashing and tokenization where appropriate.

D. Network & System Security

- Hardened network perimeter (firewalls, intrusion prevention).
- Continuous vulnerability management and patching program.
- Threat detection and logging (SIEM or equivalent monitoring).
- Endpoint protection and anti-malware safeguards.

E. Data Management & Minimization

SCHEDULE EEA DATA PROCESSING DETAILS

- Data retention and deletion strictly per Controller instructions.
- Data minimization and pseudonymization where feasible.
- Logical separation of Customer data.

F. Incident Response

- Documented incident response plan with defined roles/escalation.
- Breach notification to Controller without undue delay and within a maximum of **72 hours** after confirmation where PII is impacted.
- Post-incident remediation documentation.

G. Business Continuity & Disaster Recovery

- Tested backup/restore capabilities.
- Redundant systems and geographically distributed resources.
- BCP/DR plans tested at least annually.

H. Personnel Security

- Background checks where permitted by law.
- Mandatory confidentiality obligations.
- Data protection and security training at least annually.

DPA Attachment (GDPR Article 28(3) Processor Clauses)

Schedule Y — Article 28(3) Mandatory Terms

When Processing EEA PII on behalf of Customer as Data Controller, S2Verify ("Processor") agrees:

1. Instructions

Processor shall Process EEA PII only:

- on documented, lawful instructions of Customer; and
- for purposes set out in the Services Agreement.

2. Confidentiality

Processor shall:

- ensure personnel authorized to Process EEA PII are bound by confidentiality.

3. Security Measures

SCHEDULE EEA DATA PROCESSING DETAILS

Processor shall:

- implement the Technical and Organizational Measures in **Schedule X** and shall notify Customer before materially modifying such measures.

4. Subprocessing

Processor shall:

- obtain prior written authorization before engaging subprocessors;
- flow down obligations equivalent to this Schedule to all subprocessors; and
- remain liable for subprocessors' performance.

5. Data Subject Requests

Processor shall:

- assist Customer, where feasible, with data subject access, rectification, erasure, objection, and portability requests.

6. Data Breach Notification

Processor shall notify Customer without undue delay, and no later than **72 hours**, after becoming aware of a breach impacting EEA PII.

7. Data Transfer Outside EEA/UK

Processor shall:

- only transfer EEA PII outside the EEA/UK under an approved transfer mechanism (e.g., SCCs or adequacy decision).

8. Return and Deletion

Upon termination, Processor shall:

- securely delete or return EEA PII, at Customer instruction, unless retention is legally required.

9. Documentation and Audit Assistance

Processor shall:

- maintain records of Processing (ROPA) and allow audit or provide certification/report(s) to demonstrate compliance (e.g., SOC 2, ISO reports).

SCHEDULE EEA DATA PROCESSING DETAILS

Standard Contractual Clauses (SCC) Data Transfer Addendum (U.S.)

Schedule Z — International Transfer Addendum (EEA/UK → United States)

This Addendum incorporates the applicable **EU Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914, Modules 2 and 3 as applicable). Where Customer exports EEA PII to S2Verify in the United States:

A. Scope

- Clause applies to data transfers where the Customer is **Data Controller** and S2Verify is **Processor or Sub-Processor**.

B. Incorporation of SCCs

The Parties agree that:

- Module 2 (Controller→Processor) and/or Module 3 (Processor→Subprocessor) of the SCCs shall apply.
- SCC Annexes are incorporated by reference.
- S2Verify shall not engage a subprocessor in a third country without the same safeguards.

C. Supplemental Measures

To address U.S. government access concerns, S2Verify will:

- challenge unlawful government access requests;
- notify Customer where legally permitted; and
- disclose only where strictly compelled by valid, binding legal process.

D. Annex II (Technical Measures)

- The TOMs in **Schedule X** satisfy Annex II of the SCCs.

E. Conflicts

Where terms conflict:

- SCCs → supersede national law and the Services Agreement;
- This Addendum → supersedes the Services Agreement where it enhances GDPR protections.