Schedule A

Standard Contractual Clauses for International Transfers

Part 1: Definitions and Application

1. **Definitions.** For the purposes of this Schedule A:

"EU SCCs" means the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"GDPR Personal Data" means "personal data" (as defined by Applicable Privacy Law) relating to a European Economic Area ("EEA"), United Kingdom ("UK"), or Switzerland data subject.

"**ID5 Services Agreement**" as used in these SCCs may refer to the ID5 ID Agreement, the ID5 ID Site Agreement, a Master Services Agreement, or other form of contractual agreement executed between the parties related to the use of ID5 services or technologies.

"Restricted Transfer" means: (i) where the GDPR applies, a transfer of GDPR Personal Data by ID5 from the EEA to the Company in a country outside of the EEA that is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of GDPR Personal Data by ID5 from the UK to the Company in any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of GDPR Personal Data by ID5 from Switzerland to the Company in any other country that has not been determined to provide adequate data protection by the competent Swiss authority.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office.

2. **Application of Standard Contractual Clauses.** Where the processing of GDPR Personal Data under the Agreement involves a Restricted Transfer from ID5 to the Company, the parties agree that the Standard Contractual Clauses shall be deemed incorporated by reference and apply as set forth below.
3. **Transfers from the European Economic Area (EEA).** With respect to any Restricted Transfer of GDPR Personal Data from the EEA:
    a. The EU SCCs will apply between **ID5 Technology SAS** (as data exporter) and the **Company** (as data importer).
    b. The EU SCCs will be completed as follows:
        i. Module One (Controller-to-Controller) will apply.
        ii. In Clause 7, the optional docking clause will apply.
        iii. In Clause 11, the optional language will not apply.
        iv. In Clause 17 (Governing Law), Option 1 will apply, and the EU SCCs will be governed by the law of **France.**
        v. In Clause 18(b) (Choice of forum and jurisdiction), disputes will be resolved by the courts of **France**.
        vi. Annex I of the EU SCCs will be deemed completed with the information set forth in Part 2 of this Schedule A.
        vii. Annex II of the EU SCCs will be deemed completed with the information set forth in Part 3 of this Schedule A.

4. **Transfers from the United Kingdom (UK).** With respect to any Restricted Transfer of GDPR Personal Data from the UK:
    a. The EU SCCs, completed as set out in Section 3 above, will also apply to transfers of such GDPR Personal Data, subject to the following.
    b. The UK Addendum will be deemed executed between **ID5 Technology Limited** (as data exporter) and the **Company** (as data importer).
    c. The EU SCCs will be deemed amended as specified by the UK Addendum in respect of the transfer of such GDPR Personal Data.
5. **Transfers from Switzerland.** With respect to any Restricted Transfer of GDPR Personal Data from Switzerland, the EU SCCs as completed in Section 3 above will also apply, provided that:
    a. References to 'Regulation (EU) 2016/679' will be interpreted as references to the Swiss DPA.
    b. References to 'EU', 'Union' and 'Member State' will be deemed replaced with 'Switzerland'.
    c. The 'competent supervisory authority' will be the Swiss Federal Data Protection and Information Commissioner.
    d. In Clause 17, the EU SCCs will be governed by Swiss law.
    e. In Clause 18(b), disputes will be resolved by the courts of Switzerland.
6. **Conflict.** In the event of a conflict between the terms of the Standard Contractual Clauses and any other agreement between the Parties, the terms of the Standard Contractual Clauses will govern.

Part 2: Annex I

A. LIST OF PARTIES

Data exporter(s):

Name: ID5 Technology SAS (for transfers from the EEA and Switzerland); ID5 Technology Limited (for transfers from the UK)

Address:

For ID5 Technology Limited: 8 Devonshire Square, London, EC2M 4YJ, United Kingdom.

For ID5 Technology SAS: 14 Rue Du Vieux Faubourg, Lille, 59800, France

Contact person's name, position and contact details:

ID5's Chief Privacy Officer can be contacted at privacy@id5.com.

ID5's DPO can be contacted at Richard.Merrygold@istormsolutions.co.uk.

Activities relevant to the data transferred under these Clauses: The provision of the ID5 ID Services and related services to the data importer pursuant to the Agreement.

Role (controller/processor): Controller.

Data importer(s):

Name: The "Company" who has agreed to the ID5 Services Agreement.

Address: As set forth for "Company" in the applicable ID5 Services Agreement or as otherwise identified to ID5.

Contact person's name, position and contact details: The Privacy Contact for "Company" set forth at the beginning of the ID5 Services Agreement.

Activities relevant to the data transferred under these Clauses: The receipt and use of Personal Data in connection with the ID5 ID Services pursuant to the Agreement.

Role (controller/processor): Controller.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: Visitors to the Digital Properties* who are EEA, UK, and/or Switzerland data subjects.

*Digital Properties in these SCCs may also refer to Company Sites, Controlled Company Sites, Client Sites, or other digital properties as defined in the applicable

Categories of personal data transferred: encrypted ID5 IDs. For paid services, this may also include additional deliverables and personal data types/categories.

Sensitive data transferred (if applicable): Not applicable. The data importer is prohibited by the Agreement from providing any Sensitive Data to the data exporter.

The frequency of the transfer: Continuous throughout the duration of the Agreement.

Nature of the processing: Transfer of unique identifiers to enable identity resolution and related digital advertising services as described in the Agreement.

Purpose(s) of the data transfer and further processing: To enable the data importer to utilize ID5's identity resolution services in connection with its digital properties and advertising activities, as further described by the Permitted Purpose in the Agreement.

The period for which the personal data will be retained: Personal data will be retained by the data importer in accordance with its own data retention policies and obligations under Applicable Privacy Law.

C. COMPETENT SUPERVISORY AUTHORITY

For transfers from the EEA: The competent supervisory authority will be determined in accordance with Clause 13 of the EU SCCs.

For transfers from the UK: The competent supervisory authority is the Information Commissioner's Office (ICO).

For transfers from Switzerland: The competent supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC).

Part 3: Annex II - Technical and Organisational Measures

The data exporter has implemented and will maintain the technical and organisational measures described in this Annex. The data exporter may update or modify these measures from time to time at its discretion, provided that such updates and modifications do not result in a material degradation of the overall security of the personal data.

Measures of pseudonymisation and encryption: Wireless networks are secured using strong encryption (e.g., WPA2/WPA3). All remote access to organizational networks requires encryption.

Measures for ensuring ongoing confidentiality, integrity, and availability: A Zero Trust security model is used for securing network access. Access controls are based on the principle of least privilege. The Network Security Policy aims to ensure the confidentiality, integrity, and availability of assets.

Measures for restoring availability and access in a timely manner: An Incident Management Procedure is maintained to respond to and recover from security incidents. ID5 leverages third-party data center providers.

Processes for regularly testing and evaluating effectiveness: Regular risk assessments of threats and vulnerabilities are performed. Periodic audits of security measures are conducted. The Network Security Policy is reviewed at least every 6 months.

Measures for user identification and authorisation: Multi-factor authentication is mandatory for remote access connections. User accounts are promptly deactivated upon termination of employment or service agreements.

Measures for the protection of data during transmission and storage: Firewalls with configurations based on industry best practices are implemented to control network traffic. Critical systems and sensitive data are held in segmented networks.

Measures for ensuring physical security: ID5 leverages third-party providers for data centers, who are responsible for physical security.

Measures for ensuring events logging: Access logs are maintained and regularly reviewed. Servers are monitored for intrusion detection.

Measures for internal IT and IT security governance: The Chief Technology Officer is responsible for overseeing and enforcing the Network Security Policy. A comprehensive, mandatory cybersecurity training program is in place for all employees.