DATA PROCESSING AGREEMENT

Last Updated: 6th March 2026

This Recruiterflow Data Processing Agreement ("DPA"), that includes the Standard Contractual Clauses adopted by the European Commission, and where applicable the UK International Data Transfer Addendum, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under Recruiterflow's Terms of Service. This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement. Upon its incorporation into the Agreement, the DPA will form a part of the Agreement.

The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

THIS DPA INCLUDES:

(i) Standard Contractual Clauses (EU) 2021/914, attached hereto as EXHIBIT 1.

(a) Annex I to the Standard Contractual Clauses, which includes details of the parties, the processing, and the competent supervisory authority.

(b) Annex II to the Standard Contractual Clauses, which includes a description of the technical and organisational security measures implemented by the data importer.

(c) Annex III to the Standard Contractual Clauses, which includes the list of sub-processors.

(ii) UK International Data Transfer Addendum to the EU Standard Contractual Clauses, attached hereto as EXHIBIT 2.

(iii) List of Sub-Processors, attached hereto as EXHIBIT 3.

1. DEFINITIONS

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Protection Law" means all applicable legislation relating to data protection and privacy including without limitation (a) the GDPR; (b) the UK GDPR and the UK Data Protection Act 2018; and (c) all local laws and regulations in any Member State of the European Union or the United Kingdom which implement, supplement, amend or replace any of the foregoing, as amended, repealed, consolidated or replaced from time to time. The terms "process", "processes" and "processed" will be construed accordingly.

"Data Subject" means the individual to whom Personal Data relates.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"UK GDPR" means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

"Instruction" means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalising, blocking, deletion, making available).

"Personal Data" means any information relating to an identified or identifiable individual where such information is contained within User Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Processing" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. "Processor"

means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as set out in Exhibit 1.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, as set out in Exhibit 2.

2. DETAILS OF THE PROCESSING

2(a) Categories of Data Subjects

Controller's Contacts and other end users including Controller's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller's end users. In the context of recruitment services, Data Subjects include candidates and applicants.

2(b) Types of Personal Data

Contact Information, the extent of which is determined and controlled by the User in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Subscription Service. In the context of recruitment, this may include CVs/résumés, employment history, education records, and other candidate profile data.

2(c) Special Categories of Data

The parties acknowledge that, in the context of recruitment processing, Controller may upload or process special categories of personal data (as defined in Article 9 of the GDPR and section 10 of the UK Data Protection Act 2018), which may include data revealing racial or ethnic origin, health data, trade union membership, or other sensitive information contained within candidate records. Where Controller uploads such data, the provisions of Section 4(i) of this DPA shall apply.

2(d) Subject-Matter and Nature of the Processing

The subject-matter of Processing of Personal Data by Processor is the provision of the services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order.

2(e) Purpose of the Processing Personal Data will be Processed for purposes of providing the services set out and otherwise agreed to in the Agreement and any applicable Order.

2(f) Duration of the Processing Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. USER RESPONSIBILITY

Within the scope of the Agreement and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA is User's complete and final instruction to Recruiterflow in relation to Personal Data and additional instructions outside the scope of DPA would require prior written agreement between the parties. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

Where Controller uploads or processes special categories of personal data, Controller shall be solely responsible for ensuring that a valid legal basis exists for such processing (including, where required, obtaining explicit consent from the relevant Data Subjects) and for conducting any required data protection impact assessment.

4. OBLIGATIONS OF PROCESSOR

4(a) Compliance with Instructions

The parties acknowledge and agree that User is the Controller of Personal Data and Recruiterflow is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union, United Kingdom or Member State law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

4(b) Security

Processor shall take the appropriate technical and organisational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data, described under Annex II to the Standard Contractual Clauses. Such measures include, but are not limited to:

(i) the prevention of unauthorised persons from gaining access to Personal Data Processing systems (physical access control);

(ii) the prevention of Personal Data Processing systems from being used without authorisation (logical access control);

(iii) ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control);

(iv) ensuring that Personal Data cannot be read, copied, modified or deleted without

authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);

(v) ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control);

(vi) ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions);

(vii) ensuring that Personal Data is protected against accidental destruction or loss (availability control).

Upon Controller's request, Processor shall provide a current Personal Data protection and security program relating to the Processing hereunder. Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR and the equivalent provisions of the UK GDPR), by (i) implementing and maintaining the security measures described under Annex II, (ii) complying with the terms of Section 4(d) (Personal Data Breaches); and (iii) providing the Controller with information in relation to the Processing in accordance with Section 5 (Audits).

4(c) Confidentiality

Processor shall ensure that any personnel whom Processor authorises to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

4(d) Personal Data Breaches

Processor will notify the Controller without undue delay, and in any event within 72 hours, after it becomes aware of any Personal Data Breach affecting any Personal Data. Such notification shall include, to the extent reasonably available:

(i) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned;

(ii) the likely consequences of the Personal Data Breach;

(iii) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

Where it is not possible to provide all such information at the same time, the information may be provided in phases without undue further delay. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

4(e) Data Subject Requests

Processor will provide reasonable assistance, including by appropriate technical and organisational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests. Controller shall reimburse Processor for the costs arising from this assistance.

4(f) Sub-Processors

Processor shall be entitled to engage sub-Processors to fulfil Processor's obligations defined in the Agreement only with Controller's written consent. For these purposes, Controller consents to the engagement as sub-Processors of Processor's affiliated companies and the third parties listed in Exhibit 3. For the avoidance of doubt, the above authorisation constitutes Controller's prior written consent to the sub-Processing by Processor for purposes of the Standard Contractual Clauses.

If the Processor intends to instruct sub-Processors other than the companies listed in Exhibit 3, the Processor will notify the Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 14 days after being

notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the sub-Processor). If the Processor and Controller are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

Where Processor engages sub-Processors, Processor will enter into a contract with the

sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations.

Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this DPA and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.

The provisions of this Section 4(f) shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") or the United Kingdom not recognised by the European Commission or the UK Secretary of State (as applicable) as providing an adequate level of protection for personal data. If, in the performance of this DPA, Recruiterflow transfers any Personal Data to a sub-Processor located outside of the EEA or the United Kingdom, Recruiterflow shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

4(g) Data Transfers

Controller acknowledges and agrees that, in connection with the performance of the services under the Agreement, Personal Data will be transferred to Recruiterflow, Inc. Recruiterflow will store Personal Data using infrastructure managed by Amazon Web Services (AWS) in the EU (Frankfurt) region by default. Certain Recruiterflow personnel located in the United States and India may access Personal Data for the purposes of providing support, maintenance and platform operations.

The Standard Contractual Clauses at Exhibit 1 will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognised

by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Law). The UK Addendum at Exhibit 2 will apply with respect to Personal Data that is transferred outside the United Kingdom to any country not recognised by the UK Secretary of State as providing an adequate level of protection for personal data.

4(h) Deletion or Retrieval of Personal Data

Other than to the extent required to comply with Data Protection Law, following termination or expiry of the Agreement, Processor will delete all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller.

4(i) Special Categories of Personal Data

Where Controller uploads or causes to be processed special categories of personal data through the Subscription Service, Processor shall:

(i) process such data solely in accordance with Controller's Instructions and the terms of this DPA;

(ii) apply the same technical and organisational security measures described in Annex II to such data, including encryption at rest and in transit;

(iii) ensure that access to special categories of personal data is restricted on a need-to-know basis;

(iv) not use special categories of personal data for any purpose other than the performance of the services under the Agreement.

Processor does not require the input of special categories of personal data to provide the Subscription Service and recommends that Controller minimise the upload of such data wherever possible.

5. AUDITS

The Controller may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organisational measures taken by Processor.

For such purpose, Controller may, e.g.,

(a) obtain information from the Processor;

(b) request Processor to submit to Controller an existing attestation or certificate by an independent professional expert; or

(c) upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor's business operations, conduct an on-site inspection of Processor's business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor.

Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

6. GENERAL PROVISIONS

With respect to updates and changes to this DPA, the terms that apply in the "Amendment; No Waiver" in the Agreement shall apply. In case of any conflict, this DPA shall take precedence over the regulations of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

Upon the incorporation of this DPA into the Agreement, the parties indicated in Section 7 below (Parties to this DPA) are agreeing to the Standard Contractual Clauses and the UK Addendum (where and as applicable) and all annexes and appendixes attached thereto. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Exhibit 1 or the UK Addendum in Exhibit 2, the Standard Contractual Clauses or UK Addendum (as applicable) shall prevail.

Recruiterflow will process Personal Data in accordance with GDPR and UK GDPR requirements

contained herein which are directly applicable to Recruiterflow's provision of the Subscription Services.

7. PARTIES TO THIS DPA

This DPA is an amendment to and forms part of the Agreement. Upon the incorporation of this DPA into the Agreement (i) Controller and the Recruiterflow entity that are each a party to the Agreement are also each a party to this DPA, and (ii) to the extent that Recruiterflow Inc. is not the party to the Agreement, Recruiterflow, Inc. is a party to this DPA, but only with respect to agreement to the Standard Contractual Clauses, the UK Addendum, this Section 7 of the DPA, and to the Standard Contractual Clauses and UK Addendum themselves.

If Recruiterflow, Inc. is not a party to the Agreement, the section of the Agreement entitled 'Limitation of Liability' shall apply as between Controller and Recruiterflow, Inc., and in such respect any references to 'Recruiterflow', 'we', 'us' or 'our' shall include both Recruiterflow, Inc. and the Recruiterflow entity that is a party to the Agreement.

The legal entity agreeing to this DPA as Controller represents that it is authorised to agree to and enter into this DPA for, and is agreeing to this DPA solely on behalf of, the Controller.

EXHIBIT 1 — STANDARD CONTRACTUAL CLAUSES (EU) 2021/914

For the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, the parties incorporate by reference the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (Module Two: Controller to Processor).

The following selections and annexes apply:

Clause	Selection
Clause 7 — Docking clause	The optional docking clause IS included.
Clause 9 — Use of sub-processors	Option 2 (General written authorisation) is selected. The Controller shall be informed of any intended changes to the list of sub-processors within 14 days.
Clause 11 — Redress	The optional language IS NOT included.
Clause 13 — Supervision	The supervisory authority of the Member State in which the data exporter is established shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, the Irish Data Protection Commission shall act as competent supervisory authority.
Clause 17 — Governing law	Option 1 is selected. The SCCs shall be governed by the law of Ireland.

Clause 18 — Choice of forum and jurisdiction	Disputes shall be resolved before the courts of Ireland.

ANNEX I —

DETAILS OF THE PARTIES AND THE TRANSFER

A. List of Parties

Data Exporter:

Field	Detail
Name	The User, as defined in the Recruiterflow Terms of Service ("Agreement")
Role	Controller

Data Importer:

Field	Detail
Name	Recruiterflow, Inc.
Address	2035 Sunset Lake Road, B-2, Newark, Delaware 19702, USA
Role	Processor

B. Description of Transfer

Element	Detail

Categories of data subjects	Controller's Contacts and other end users including Controller's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller's end users. In the context of recruitment services, Data Subjects include candidates and applicants.

Categories of personal data	Contact Information, the extent of which is determined and controlled by the User in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, CVs/résumés, employment history, education records, candidate profile data, and other electronic data submitted, stored, sent, or received by end users via the Subscription Service.
Sensitive data transferred	The parties acknowledge that, in the context of recruitment processing, special categories of personal data as defined in Article 9 of the GDPR may be transferred, including data revealing racial or ethnic origin, health data, or trade union membership contained within candidate records. The restrictions and safeguards set out in Section 4(i) of the DPA apply to such data.
Frequency of the transfer	Continuous, for the duration of the Agreement.
Nature of the	The provision of the Subscription Service to the Controller, as

processing	described in the Agreement.
Purpose of the transfer	Personal Data will be processed for purposes of providing the services set out in the Agreement and any applicable Order.
Retention period	For the duration of the Agreement, subject to Section 4(h) of the DPA.

C. Competent Supervisory Authority

The supervisory authority of the Member State in which the data exporter is established. Where the data exporter is not established in an EU Member State, the Irish Data Protection Commission shall act as competent supervisory authority.

ANNEX II — TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Recruiterflow currently observes the security practices described in this Annex II. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, Recruiterflow may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalised terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

i) Preventing Unauthorised Product Access

Outsourced processing: Recruiterflow hosts its Service with outsourced cloud infrastructure providers. Additionally, Recruiterflow maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Recruiterflow relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Authentication: Users can use their LinkedIn API, Google API, Office365 API or a secure sign-in option in order to log in to Recruiterflow.

Authorisation: User data is stored in multi-tenant storage systems accessible to Users via only application user interfaces and application programming interfaces. Users are not allowed direct access to the underlying application infrastructure. The authorisation model in Recruiterflow's product is designed to ensure that only the appropriately assigned individuals can access relevant features and customisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

ii) Preventing Unauthorised Product Use

Recruiterflow implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

iii) Limitations of Privilege & Authorisation Requirements

Product access: A subset of Recruiterflow's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All Recruiterflow employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines,

non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: Recruiterflow makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Recruiterflow's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Recruiterflow stores user passwords following policies that follow industry standard practices for security. Recruiterflow has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: Recruiterflow designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Recruiterflow personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: Recruiterflow maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Recruiterflow will take appropriate steps to minimise product and User damage or unauthorised

disclosure.

Communication: If Recruiterflow becomes aware of unlawful access to User data stored within its products, Recruiterflow will: 1) notify the affected Users of the incident; 2) provide a description of the steps Recruiterflow is taking to resolve the incident; and 3) provide status updates to the User contact, as Recruiterflow deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the User's contacts in a form Recruiterflow selects, which may include via email or telephone.

ANNEX III — LIST OF SUB-PROCESSORS

See Exhibit 3.

EXHIBIT 2 — UK INTERNATIONAL DATA TRANSFER ADDENDUM

The parties incorporate by reference the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, as issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 (version B1.0, in force 21 March 2022), ("UK Addendum").

The following selections apply to the UK Addendum:

Table 1: Parties

	Data Exporter	Data Importer
Party	The User, as defined in the Agreement	Recruiterflow, Inc.
Address	As set out in the Agreement	2035 Sunset Lake Road, B-2, Newark, Delaware 19702, USA
Contact	As set out in the Agreement	privacy@recruiterflow.com

Table 2: Selected SCCs

The Approved EU SCCs referenced are those set out in Exhibit 1 (Module Two: Controller to Processor).

Table 3: Appendix Information

Annex I, Annex II, and Annex III as set out in Exhibit 1 apply.

Table 4: Ending the Addendum

Either party may end the UK Addendum as set out in Section 19 of the UK Addendum.

EXHIBIT 3 — LIST OF SUB-PROCESSORS

The current list of sub-processors is available upon request. To obtain the most up-to-date list, please contact devops@recruiterflow.com.