AMENDMENT TO AGREEMENT

This Amendment amends the SaaS Subscription Agreement or other written agreement with Flo Recruit for Services (the **"Agreement"**) entered into between Flo Recruit, Inc. or the affiliate thereof that entered into the Agreement ("**Flo Recruit**") and the customer that has entered into the Agreement with Flo Recruit (**"Customer"**) (Flo Recruit and Customer are, together, the **"Parties"**). This Amendment is effective the date signed by the Customer ("**Effective Date**").

The Parties agree to amend the Agreement as follows:

1. **Data Processing Addendum**. Flo Recruit's processing of personal data included in the Customer Data shall be subject to the Data Processing Addendum in **Exhibit A**. For the purpose of this Amendment, **"Customer Data"** have the meaning set forth in the Agreement.

2. **Order of Precedence**. In the event of a conflict between the provisions of this Amendment and those of the Agreement in respect of the processing and protection of Protected Data, the provisions of this Amendment will prevail. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect.

Signed for and on behalf of	Signed for and on behalf of
FLO RECRUIT, INC.	**CUSTOMER:**
_____	_____
by its authorized representative	by its authorized representative
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

EXHIBIT A

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA"**) is incorporated into the Agreement between Flo Recruit and Customer in relation to Flo Recruit's processing of Customer's Protected Data in the Services.

1. DEFINITIONS

1.1. "**CCPA / CPRA**" means the California Consumer Privacy Act of 2018 ("**California Consumer Privacy Act**" or "**CCPA**") California Civil Code § 1798.100 et seq. and the California Privacy Rights Act of 2020 ("**CPRA**") upon its entry into force and any regulations issued pursuant thereto;

1.2. **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data;

1.3. **"Data Subject Request"** means a request made by an individual to exercise their rights under Data Protection Laws;

1.4. "**Data Protection Laws**" means the laws, regulations, and binding administrative rules worldwide regarding the protection of data and privacy of individuals, but not including any industry-specific or sector-specific laws, regulations, rules, or industry-standards, such as those related to healthcare, financial services, payment card, or government and public bodies;

1.5. **"GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and implementing legislation of European Union / EEA member states made pursuant thereto;

1.6. **"Personal Data"** means any information relating to: (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity where such information is protected similar to the personal information of a natural person under Data Protection Laws;

1.7. **"Personal Data Breach"** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Protected Data;

1.8. **"Processor"** means the entity which processes Personal Data on behalf of the Controller;

1.9. **"processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (and related terms such as process have corresponding meanings);

1.10. **"Protected Data"** means Personal Data in Customer Data uploaded to the Services or otherwise provided to Flo Recruit by the Customer pursuant to the Agreement;

1.11. **"Services"** means the cloud services provided by Flo Recruit provided to Customer by Flo Recruit pursuant to the Agreement;

1.12. **"Sub-Processor"** means any processor engaged by Flo Recruit or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

1.13. **"Data Protection Authority"** means any duly authorized government authority responsible for administering Data Protection Laws.

2. APPLICATION OF LAWS

2.1. **Data Protection Laws**

i. If any Data Protection Law (other than GDPR) applies to the processing of Protected Data, then the parties acknowledge and agree that Customer shall be the "organisation", "data controller", "business" (or their equivalent terms) and Flo Recruit shall be the "data processor" or "service provider" (or their equivalent terms) under such Data Protection Law. Each Party is responsible for complying with the Data Protections Laws as they apply to it.

ii. If any Data Protection Laws (other than GDPR) impose on Flo Recruit additional or overriding obligations to those in this Data Processing Addendum with respect to its processing of Protected Data or require Customer and Flo Recruit to enter into any additional agreements or to implement any additional security or organizational security measures to process Protected Data under the Agreement, Flo Recruit and Customer agree to negotiate such additional obligations, agreements, or security measures in good faith.

2.2. **GDPR**. If GDPR applies to Flo Recruit's processing of Protected Data, then the parties acknowledge and agree that, with respect to such processing of Protected Data, Customer shall be the Controller (or Processor on behalf of a third-party) and Flo Recruit shall be the Processor (or Sub-Processor on behalf of Customer) and that the Standard Contractual Clauses attached hereto as **Exhibit 1** shall apply to such processing. The Parties' entering into the Agreement incorporating this DPA constitutes their signature on the Standard Contractual Clauses and Annex I.

2.3. **CCPA / CPRA**. If the CCPA / CPRA apply to Flo Recruit's processing of Protected Data, then the parties acknowledge and agree that, with respect to such processing of Protected Data, Customer shall be a business and Flo Recruit shall be the service provider and that the CCPA / CPRA Additional Terms attached hereto as **Exhibit 2** shall apply to such processing in addition to this DPA.

3. DATA PROCESSING RESPONSIBILITIES

3.1. Flo Recruit Responsibilities. Flo Recruit shall process the Protected Data for the following purposes:

(a) Providing the Services requested by Customer solely in accordance with the Agreement and this DPA; and

(b) Complying with other documented reasonable instructions provided by Customer (e.g., via a support request or email) from time to time where such instructions are consistent with the terms of the Agreement and this DPA.

3.2. **Customer Responsibilities**. Customer is solely responsible for its and its Authorized Users' processing of Protected Data using the Services.

4. SECURITY

Flo Recruit shall implement, maintain, and follow, at its cost and expense:

(a) an information security management system designed to protect the Protected Data from accidental or unlawful destruction, loss, alteration, and unauthorized disclosure, access, or use meeting or exceeding SOC-2 compliance standards;

(b) the security measures and Services features set forth in **Exhibit 3** hereto; and

(c) reasonable technical and organizational security measures to assist Customer to respond to Data Subject Requests.

5. SUB-PROCESSORS

5.1. Flo Recruit has appointed its affiliates and the Sub-Processors listed on its website (https://start.florecruit.com/sub-processor-list) to perform processing activities in respect of the Protected Data on behalf of Flo Recruit. Processing by Sub-Processors is done under a written contract containing materially equivalent obligations to those in this DPA. Flo Recruit shall remain fully responsible for its affiliates and the Sub-Processors' performance of their obligations under their contracts with Flo Recruit.

5.2. Flo Recruit may not add or change a Sub-Processor without first notifying the Customer (including by providing public notice of an update on its website) and giving the Customer ten days (from date of receipt of the notice) to object to the change in Sub-Processor on reasonable and objectively justifiable grounds. Customer may subscribe to e-mail notifications of new Sub-processors by contacting privacy@florecruit.com. If Customer objects to the change in Sub-Processor, then the parties will work together in good faith to resolve the objection, which may include avoiding the functionality provided by the new Sub-Processor or recommending a commercially reasonable workaround to avoid processing of the Protected Data by the new Sub-Processor.

6. PERSONNEL

Flo Recruit shall ensure that only authorized personnel have access to Protected Data and that any persons whom it authorizes to have access to Protected Data on its behalf are subject to a binding contractual or statutory obligations to protect the Protected Data and keep it confidential no less than Flo Recruit is required to do under the Agreement and this DPA. Flo Recruit shall ensure that its authorized personnel are appropriately trained regarding their data protection and confidentiality obligations.

7. DATA SUBJECT REQUESTS AND AUDITS

7.1. Flo Recruit shall promptly notify Customer in writing of any Data Subject Requests or other communications received by it from Data Subjects or Data Protection Authorities relating to the Protected Data and shall not respond to such communications unless it has been expressly authorized to do so by Customer except as required under applicable law. Flo Recruit shall provide to Customer reasonable assistance with respect to answering Data Subject Requests.

7.2. Flo Recruit shall make available to Customer information reasonably necessary to demonstrate its compliance with this DPA and Data Protection Laws, and shall cooperate with reasonable audit, inspection, or privacy impact assessment requests by Customer (or another auditor mandated by Customer). Unless required in connection with the investigation of a Personal Data Breach or to respond to a legally required inquiry, such audit, inspection, or assessment shall take place no more than once per year, upon prior notice of at least 15 days, during regular business hours, and the scope of which shall be mutually agreed to by the Parties.

7.3. Customer shall ensure that all information obtained or generated by Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (except for disclosure to a Data Protection Authority or as otherwise required by law). Customer shall provide to Flo Recruit a copy of such information and audit reports.

8. BREACH NOTIFICATION

In respect of any Personal Data Breach involving Protected Data, Flo Recruit shall notify Customer without undue delay within 72 hours of becoming aware of the Personal Data Breach. So far as possible without prejudicing the continued security of the Protected Data or any investigation into the Personal Data Breach, Flo Recruit shall provide Customer with timely detailed information about the Personal Data Breach.

9. DELETION OR RETURN OF DATA

Flo Recruit shall delete or, if requested, return Protected Data to Customer in accordance with the provisions of the Agreement (including by providing retrieval functionality), unless storage of any data is

required by applicable law and, if so, Flo Recruit shall inform Customer of any such requirement and the period during which it is required to be stored. Any such retained Protected Data shall remain subject to this DPA.

10. ORDER OF PRECEDENCE

In the event of a conflict between the provisions of this DPA and those of the Agreement in respect of the processing and protection of Protected Data, the provisions of this DPA shall prevail. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect. With respect to Flo Recruit's processing of Protected Data subject to GDPR, in the event of a conflict between the terms of the Standard Contractual Clauses and this DPA, the Standard Contractual Clauses shall prevail.

EXHIBIT 1

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to

processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these

Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the

Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more

information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data

exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data

exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least *ten business days* in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any

intended changes to that list through the addition or replacement of sub- processors at least *ten business days* in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the

controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these

Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and

agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data

subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with

these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of NA (*specify Member State*).

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _NA(*specify Member State*).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name and address: *Customer to Add Name and Address:* _____.

Contact person's name, position and contact details: *Customer to Add Name, Position and Contact Information:* _____.

Customer to Add Data Protection Officer, if any: _____.

Activities relevant to the data transferred under these Clauses: Using and accessing Flo Recruit Services under the terms of data exporter's agreement with Flo Recruit (data importer).

Role: controller and/or processor and/or sub-processor

Data importer(s): Flo Recruit, whose Data Privacy Officer is their Chief Technology Officer, Atreya Misra, who can be contacted at atreya@florecruit.com.

Name: Flo Recruit, Inc.

Address: Flo Recruit, Inc., 5740 Ridgetown Circle, Dallas, TX 75230.

Contact person's name, position and contact details:

Flo Recruit, Inc.
Atreya Misra
Chief Technology Officer
privacy@florecruit.com

Activities relevant to the data transferred under these Clauses: Providing the Flo Recruit Services under the terms of data exporter's agreement with Flo Recruit (data importer).

Role: processor and/or sub-processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

The data subjects are the individuals whose personal information is contained in data exporter's data provided to data importer.

Categories of personal data transferred

Data exporter and its authorized users may submit personal data, the nature of which is determined and controlled by the data exporter in its sole discretion.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.
The Flo Recruit Service(s) are made for general use and not intended for the processing of any special categories of data. However, use of the Service(s) with any special categories of data is not precluded. Data exporter is responsible for determining if additional restrictions or safeguards are needed if it uses the Service(s) with sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
Continuous during the Service(s.

Nature of the processing

The nature of the processing is providing the Flo Recruit Services to the data exporter for use with its data.

Purpose(s) of the data transfer and further processing

Personal data, if any, is processed by the data importer for the purposes of providing the Service(s) pursuant to the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data in the data exporter's data will be retained during for the term of the agreement. Personal data such as business contact and business relationship information is retained for the performance of the contract and Flo Recruit's legitimate business interests at least seven years after the end of the customer relationship with Flo Recruit.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.

As set forth above.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

None.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As set forth in **Exhibit 3 - Security Controls** to the DPA.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Per the terms of Clause 9(a), Option 2 (general authorisation), the controller has authorised the use of the following sub-processors:

The sub-processors listed at: https://www.Flo Recruit.com/privacy.

The data exporter may subscribe to receive e-mail notifications of updates to the sub-processors list by contacting privacy@florecruit.com.

EXHIBIT 2

CCPA / CPRA ADDITIONAL TERMS

To the extent that CCPA / CPRA applies to the processing by Flo Recruit of any Protection Data, then, notwithstanding anything to the contrary in the DPA:

(a) Flo Recruit shall comply with the obligations of a "service provider" as defined in CCPA and/or CPRA.

(b) Customer shall disclose Personal Data to Flo Recruit solely for: (i) a valid business purpose; and (ii) Flo Recruit to perform the Services.

(c) Flo Recruit is prohibited from: (i) selling or sharing Personal Data without Customer's permission; (ii) retaining, using, or disclosing Personal Data for any purpose other than for the business purposes specified in this Agreement, including a commercial purpose other than providing the Services or as otherwise permitted by the CCPA/CCRA; (iii) retaining, using, or disclosing the Personal Data outside of the Agreement; and (iv) combining the Personal Data that Flo Recruit receives from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Flo Recruit may combine personal information to perform any business purpose as defined in regulations adopted pursuant to the CCPA and/or CPRA.

(d) Flo Recruit acknowledges that Customer discloses Personal Data only for limited and specified purposes, as set forth herein.

(e) Customer may take reasonable and appropriate steps to help ensure that Flo Recruit uses the Personal Data transferred to it in a manner consistent with Customer's obligations under the CCPA and/or CPRA.

(f) Flo Recruit shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA and/or CPRA.

(g) Customer may, upon notice to Flo Recruit, take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

(h) Both parties certify that they understand and will comply with the restrictions set forth in this Exhibit 2 to the DPA.

EXHIBIT 3

SECURITY CONTROLS

General Controls:

Information Security Program

Flo Recruit follows an Information Security program in place to design, implement and maintain a coherent set of policies, standards, and systems to manage risks to information assets conforming to the Soc-2 compliance standards.

Physical and Environment Security

Flo Recruit' facilities are housed in secure areas protected by a secure perimeter, with appropriate security barriers and entry controls. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where personal information and critical technology are located.

Flo Recruit takes the following steps to assure Flo Recruit's facilities shall be physically protected from unauthorized access, damage and interference.

Access to the facilities are logged and logs of physical access are securely maintained.

Visitors and guests are always escorted/supervised while on-premises.

Video monitoring of all ingress and egress points of the secure areas.

Flo Recruit takes commercially reasonable steps to assure that equipment is physically protected from security threats and environmental hazards in order to prevent loss, damage or compromise of assets and interruption to business activities.

Flo Recruit employs commercially reasonable controls to assure that Flo Recruit's information and information-processing facilities shall be protected from disclosure to, modification of, or theft by unauthorized persons. Controls shall be in place to reasonably minimize loss or damage.

Access Control

Flo Recruit shall employ systems and processes to limit physical and logical access based on least privileges according to job responsibilities to reasonably ensure critical data can only be accessed by authorized personnel. Flo Recruit maintains authentication controls for the services commensurate with commercially reasonable security practices and maintains audit trails and logs for access in accordance with legally required data retention periods. Access privileges will be updated promptly after any change in personnel or system and are reviewed quarterly.

a) **Network Access Control**: The design of the Flo Recruit's internal and external networks demonstrates a commitment to secure networking. The design is documented and updated as needed. External connections are managed carefully; connections to networks for third parties are created after security due diligence has been completed.

b) **Operating System Access Control**: Flo Recruit implements operating system access controls that reasonably protect the systems from compromise. Protections shall include but are not limited to appropriate system authorization and management.

c) **Data Access Control**: Access is granted on a least privilege, need-to-have and must-know basis to prevent disclosure. Users and their activities are uniquely identifiable and segregated by role. Administrative privileges are restricted to only those who need them.

d) **Information System Access Control**: Access is strictly controlled by a formal provisioning cycle. Information systems are password protected and have an owner responsible for managing and controlling access.

e) **Multi-factor authentication**: Flo Recruit personnel are only granted access to personal information and critical technology after successfully presenting multiple, separate pieces of evidence.

f) **Transmission Control**: Where personal data is transmitted through a public network (e.g., the internet) to and from an external third party, the information must be encrypted first or sent via a secure channel.

g) **Separation Control**: Network services, systems, users, workstations, and servers are separated based on business purpose.

h) **Availability Control**: To protect against loss of data, critical information systems are subject to backup and redundancy requirements.

i) **Patch Management Process**: Flo Recruit maintains a patch management process to implement patches in a reasonable, risk-based timeframe.

Business Continuity & Disaster Recovery

Flo Recruit maintains business continuity and disaster recovery management plans, which document strategies and procedures for applications and/or data criticality analysis and to recover IT services and systems following an emergency or disruption. This includes relocation of people and operations to alternate site; recovery of IT functions using alternate equipment and performing functions using alternative methods; a process enabling an enterprise to restore any loss of data; when requested, providing an SLA for the amount of time within which critical customer operations would be restored; providing documentation or other proof of the ability to immediately disable all or part of the functionality of Vendor systems, services, and/or applications should a security issue be identified. Flo Recruit will validate continuity/recovery capabilities by testing annually.

Incident Response Plan

Flo Recruit maintains an incident response plan in place which includes clearly defined roles and decision-making authority and a logging and monitoring framework to allow the isolation and mitigation of an incident.

Application Security

Flo Recruit implements security touchpoints with respect to secure coding and software development appropriate for the software development lifecycle for Flo Recruit Services.

Penetration Testing

At least once per year, Flo Recruit performs a suite of independent third-party tests. Upon request, Flo Recruit will supply customer with details of third-party tests from the previous year. Flo Recruit fixes all critical severity vulnerabilities that could affect the security of customer's data as soon as possible. Remaining issues will be remediated commiserate with the risk posed to Flo Recruit.

Systems Hardening

All servers, routers, firewalls, and other relevant infrastructure shall materially conform to applicable industry standards. Flo Recruit servers will use a hardened operating system customized for the customer's needs. Flo Recruit will remove all unnecessary utilities from operating system configurations and must restrict access rights to least privilege.

<u>Controls for Flo Recruit Cloud Services</u>:

Flo Recruit's System Environment Secure Deployment

The Flo Recruit Cloud Services are managed by a small number of designated Flo Recruit IT staff with a demonstrated need to service the application or infrastructure. Access to the Flo Recruit server may be required by Flo Recruit staff. Authorized Flo Recruit staff access the AWS account via multifactor authentication (MFA).

Flo Recruit Cloud Services are deployed on Amazon Linux 2. Flo Recruit deploys a dedicated and isolated Kubernetes namespace for each Licensee. Each Licensee's deployment does not have access to any other Flo Recruit Licensee's deployment. Flo Recruit Cloud Services keeps the OS up to date with the latest updates and timely installation of security patches.

Restricted Access to Flo Recruit Server

Access to Flo Recruit server is restricted as follows:

By Flo Recruit – Flo Recruit's access to each Flo Recruit Cloud Services server through SSH is enabled from designated Flo Recruit IP addresses only.

By Customer – Customer Access to Flo Recruit Servers is not available

The Cloud Access IP Whitelist is maintained by Flo Recruit IT.

Secure Business Flow

To minimize the possibility of a security breach when working with the Flo Recruit Software on the Flo Recruit Cloud Services, Flo Recruit has established security controls covering the entire business cycle:

Flo Recruit Deployment Architecture to Prevent Direct Access to Server

Flo Recruit deploys the Software in a cloud architecture that enables use the Software while restricting the Customer's direct access to the Flo Recruit server.

For each deployment, all access is available only via secure web access.

Secure Web Access

Web access uses secure HTTPS secure protocol with www.florecruit.com and florecruit.com certificate (other domain certificate can be configured upon request).

Last Updated August 10, 2021