TERMS AND CONDITIONS

Subject to the definitions stated in the Contract Details, the Customer and the Supplier are hereinafter collectively referred to as the "**Parties**" and individually as a "**Party**".

1. **Definitions**

   In these Terms and Conditions, the following terms shall have the following meanings:

   "**Authorized Representatives**" means a person authorized to enter into legally binding commitments on behalf of a Party;

   "**Authorized Users**" means the employees added to the Customer's account in the Service;

   "**Confidential Information**" means all or any part of any commercial, financial, technical or operational information (including, but not limited to, all software (including source code), data, know-how, calculations, designs, drawings, methods, processes, systems, explanations and demonstrations), Personal Data and all other confidential information of whatever nature (in any form or medium) given or made available by the Supplier to the Customer in connection with the Contract;

   "**Contract**" means the software as a service contract consisting of the Contract Details, the Terms and Conditions and the Appendices specified in the Contract Details;

   "**Contract Period**" means the Initial Contract Period or a Renewal Period;

   "**Customer**" means the Party purchasing the Service;

   "**Customer Support**" means the Supplier's customer support as described in Section 2.4;

   "**Data Processing Agreement**" has the meaning as set out in Appendix 2;

   "**Gross Negligence**" means an error committed by a Party involving an obvious failure to exercise ordinary care, not only with actual appreciation of the risk involved, but also

serious disregard of, or indifference to, an obvious risk in the context of the performance of the Service;

"**Initial Contract Period**" means the first Contract Period of this Contract;

"**Intellectual Property Rights**" means: (a) patents; (b) trademarks, trade names and logos; (c) copyright and any derivative works thereof, and other rights including software (object and source code); (d) registered and unregistered designs rights; (e) database rights, semiconductor topography rights; (f) internet domain names and applications and reservations thereof; (g) proprietary and confidential information, trade secrets, and proprietary Know-how; and (h) all equitable rights relating to any of the foregoing;

"**Normal Business Hours**" has the meaning as set out in Section 2.4;

"**Personal Data**" means any information relating to an identified or identifiable natural person (a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**Renewal Period**" means the successive period of twelve (12) months of which the Contract is renewed;

"**Service**" means the service provided by the Supplier under this Contract, as described in Appendix 1;

"**Fee**" means the fee charged for the Service;

"**Supplier**" means Jobbrella AB;

"**Terms and Conditions**" means these terms and conditions for the Service.

2. Service and Customer Support

2.1. Jobbrella is an applicant tracking system and an employer branding platform provided by the Supplier (the "**Service**") available on jobbrella.se.

2.2. The Service is available 24 hours a day, seven days a week with exception for:

    a) unscheduled maintenance; and

    b) planned maintenance which shall, if possible, be performed outside of Normal Business Hours (as detailed below).

2.3. The Supplier shall perform maintenance promptly to limit any interference in the Service. The Customer can subscribe for updates on: www.jobbrella.se.

2.4. The Customer Support is available on regular business days between 9.00 and 16.00 CET (the "**Normal Business Hours**") through support@jobbrella.se.

3. Granted rights

3.1. Subject to the Terms and Conditions of this software as a service contract (the "**Contract**"), the Supplier hereby grants to the Customer a non-exclusive, non-transferable right, without the right to grant sublicenses, to use the Service (as further described in <u>Appendix 1</u>) during the Contract Period, and the Customer hereby agrees to such rights.

3.2. Subject to clause 3.1, the Customer shall have the right to add and/ or remove users of the Customer ("**Authorized Users**") to the Customer's account in the Service. The Customer undertakes and warrants that it shall at all times remain liable for the Authorized User's use of the Services.

3.3. The right to use the Service under this Contract is granted to the Customer only. No subsidiary, holding company or other affiliated company of the Customer is granted any rights to use the Service, unless the Supplier has given their prior written approval. If such approval has been given, the Customer shall be solely responsible for the other company's use of the Service and shall cause the other company to act in conformity with the provisions of this Contract. The Customer shall be the only contract party for any and all matters covered by this Contract.

3.4. The Customer shall prevent any unauthorized access to or use of the Service. In the event of any such unauthorized access or use, the Customer shall promptly notify the Supplier.

3.5. The Customer shall at all times use the Service in accordance with these Terms and Conditions.

4. Changes to the Service

4.1. The Supplier shall be entitled to make such changes to the Service that (a) relates to the production environment of the Service and does not affect the contents of the Service; (b) is necessary to prevent a severe data security risk related to the Service; or (c) results from law or regulation by authorities. If the Supplier makes any changes to the Service as specified in this Section 4.1 which has an effect on the Service delivered to the Customer, the Supplier shall inform the Customer of the changes without undue delay.

4.2. The Supplier shall also be entitled to make changes to the Service other than specified in Section 4.1. If such change has a material effect on the contents of the Service, the Supplier shall inform the Customer about the change in writing at least 14 days in advance and the Customer has the right to terminate the Contract by giving not less than three (3) Months prior written notice.

5. Intellectual Property Rights

5.1. The Supplier shall own and retain any and all right, title and interest in and to all Intellectual Property Rights in and to the Service (or any part thereof). The Customer's use of any such Intellectual Property Rights shall not affect the Suppliers' ownership thereof or give the Customer any right, title, or interest in such intellectual property rights (or any part thereof).

5.2. Unless otherwise is expressly agreed in writing, the Customer has no right to register any sign, trademark, product name, domain name, trade name or search word (or any designation for search engine or app store optimization) which is identical, similar or confusingly similar to any of the trademarks in the Service.

5.3. The Customer shall, without delay, notify the Supplier of any infringement or suspected infringement of the Service or any Intellectual Property Rights in the Service. The Supplier is however not obliged to defend such rights. If the Supplier chooses to defend its rights, the Customer shall at its own expense and to a reasonable extent assist the Supplier. For the avoidance of doubt, the Customer shall not be obliged to incur any external legal costs in relation to such dispute, but shall only provide assistance from its own staff to the Supplier and its legal counsel.

5.4. The Customer is entitled upon conclusion of the Contract Period to have its data delivered at no cost in any format as the Parties may agree. The Supplier undertakes to erase any copies of applications and data belonging to the Customer after such delivery.

6. Personal Data

The responsibilities between the Supplier and the Customer in matters relating to the handling of Personal Data pursuant to Article 28 of the European Data Protection Regulation (GDPR)[1], and other applicable Personal Data protection legislation, are regulated in a separate Data Processing Agreement attached herewith as Appendix 2.

7. Payment terms

7.1. The Service is provided by the Supplier on the terms set out herein and in accordance with the fees, payment terms (hereinafter Fees) as set out from time to time on www.jobbrella.se. The Customer shall pay the Fees as set out from time to time on www.jobbrella.se.

7.2. All prices are exclusive of VAT. Interest on late payments shall be paid based on the Swedish Central Bank's (Riksbanken) reference rate with an addition of eight (8) percentage points.

7.3. Each Party is responsible for the fees and other charges their bank or other electronic transfer system may add to the payment of the Fee.

7.4. The Supplier reserves the right to adjust the Customer's Fee from time to time as displayed on www.jobbrella.se.

8. Limitation of liability

8.1. In no event shall the Supplier be liable to the Customer for special, indirect, incidental or consequential damages, regardless of the form of action therefore, whether in contract or in tort, including negligence, including, without limitation, loss of goodwill, increased expenses, cost of capital, or the claims of third parties, howsoever caused, regardless of whether such party has been informed of the possibility of such damages.

---

[1] 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, and repealing the Directive 95/46/EC.

8.2. The Supplier's total aggregate liability to the Customer for damages, whether in contract, tort (including negligence), for breach of statutory duty or otherwise, arising under or in relation to this Contract shall be limited to the amount of fees charged by the Supplier hereunder.

8.3. The Supplier's liability under this Section shall be limited to a period of three (3) months following the expiry or termination of this Contract.

8.4. Notwithstanding the foregoing, this Section shall not limit any liability arising from gross negligence or willful misconduct.

9. Confidentiality

9.1. Each Party may be given access to Confidential Information related to this Contract, a Party and/or its business from the other Party. During the Contract Term and for a period of three (3) years thereafter, the Parties undertake not to disclose any Confidential Information to any third party or use such information, other than for the agreed purpose of fulfilling the duties according to this Contract. The Parties shall take all necessary precautions reasonably calculated to prevent an unauthorized disclosure or use of such Confidential Information.

9.2. This undertaking shall not apply to such information that:

   a) through no fault of the Party which has acquired such information, is in or enters the public domain;

   b) at the time of receipt was already known to the receiving Party without any obligation of confidentiality;

   c) was received from a third party which was entitled to disclose it without restriction; or

   d) the receiving Party is required to disclose by applicable compulsory law, order of court, or rules and regulations of any relevant regulatory body with jurisdiction over it (including any applicable stock exchange regulations), subject to reasonable prior consultation with the disclosing party.

9.3. This Section supersedes all previous agreements, promises, assurances, warranties and understandings between the Parties, including any non-disclosure agreement entered into prior to the formation of this Contract.

10. Force majeure

If a Party is prevented from fulfilling their obligations according to this Contract due to circumstances beyond the control of the Party, such as lightning, labor conflict, fire, burglary, modified governmental regulations, government intervention, as well as errors or delays in the services from subcontractors due to circumstances specified here, this shall constitute grounds for exemption that results in postponing the performance time and in the release from damages and any other potential consequences. If the delivery of the Service is affected by more than three (3) months due to any of the circumstances specified above, each Party is entitled to withdraw from the Contract without compensation being required, provided that the other Party is notified of such an event.

11. Contract Period and Termination

11.1.   This Contract is valid during the Initial Contract Period, and renewed for successive periods of twelve (12) months (each a "**Renewal Period**"), unless otherwise terminated in accordance with this Contract.

11.2.   Each Party has the right to terminate this Contract by notifying the other Party in writing no later than one (1) month before the end of the relevant Contract Period. If neither party terminates the Contract, the Contract shall continue to be valid for the coming Renewal Period.

11.3.   Each Party is entitled to immediately terminate the Contract by giving written notice to the other Party if:
   a) the other Party causes a material breach of any term of the Contract and does not remedy the breach within a period of 30 days after being notified in writing to do so; or
   b) the other Party causes a material breach of any term of the Contract which is irremediable; or

c) the other Party is subject to an application for bankruptcy proceedings, or enters into composition, or ceases to carry on business, or is wound up, or goes into liquidation.

11.4.   The Supplier is entitled to immediately terminate the Contract by giving written notice to the Customer if the Customer violates the terms of this Contract:
   a) regarding the scope of Customer's rights as stated in Section 3;
   b) regarding the Fee or other fees, if applicable, and payment terms and fails to take corrective action within 30 days from the day of the payment reminder.

11.5.   Termination under this Section shall be notified in writing to the following contact persons:
   The Supplier: support@jobbrella.se
   The Customer: the specified "Contact Person" above.

11.6.   Upon Termination in accordance with clauses 11.3 and 11.4, all licenses granted under this Contract shall immediately terminate and the Customer shall immediately cease all use of the Services. However, in the event of Termination in accordance with 11.2, the Customer shall have the right to use the Service until the current Contract Period expires.

12. Disputes and governing law

Any dispute, controversy or claim arising out of or in connection with this Contract, or the breach, termination or invalidity thereof, shall be settled by the public courts of Sweden, whereas Stockholm District Court shall be the first instance. The laws of Sweden shall govern this Contract and any dispute regarding this Contract.

13. Transfer of rights

The Customer's rights and obligations under this Contract may not be transferred or pledged without the prior written consent of Supplier. Notwithstanding the foregoing, a Party may transfer or assign its rights and/or obligations under this Contract to such legal person, directly or indirectly, controlled by, the transferring Party.

14. Entire agreement

This Contract constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

15. Variation

No amendment of this Contract shall be effective unless it is in writing and signed by, or on behalf of, each Party (or its Authorized Representative).

Appendix 1 - DETAILS OF THE SERVICE

The Service is constantly developed and this appendix therefore includes the main features in the Services, at the date hereof, as follows:

- **Career Page** which include:
    - o   Start page and additional pages, job list, job listing etc.

- **Applicant tracking system** which include:
    - o   Automated communication with the job applicants
    - o   Connect (open application)
    - o   Candidate management including:
        - ▪   Workflow
        - ▪   Reviewing
        - ▪   Internal and external communication etc.

- **Social recruiting functionality** which include:
    - o   Employee can connect to the Services
    - o   Viral sharing through employees

- **Support** which include:
    - o   Free support via e-mail during normal business hours

- **Product updates** during Contract period

Appendix 1 - DATA PROCESSING AGREEMENT

This Data Processing Agreement (including any appendices the "Data Processing Agreement") with our customers ("Customer" or " Controller") sets out how we Jobbrella AB, org. No. 559457-4898, ("Jobbrella" or " Processor") process, gather, use, store, share, secure, retain and dispose of information and personal data on behalf of our Customers and their users.

Jobbrella and Customer is each referred to as a "Party" and jointly as the "Parties".

BACKGROUND

    A. Jobbrella and the Customer have entered into a customer agreement (the "**Agreement**") under which Jobbrella provides an applicant tracking system and an employer branding platform to the Customer and Customer pays certain fees (the "**Assignment**").

    B. When performing the Assignment under the terms of the Agreement, it is anticipated that Jobbrella may Process Personal Data on behalf of the Customer as Controller, as set out in more detail in <u>Appendix 1</u>. This Data Processing Agreement regulates the terms and conditions for such Processing.

    C. If any provision of the Agreement conflicts with the terms of this Data Processing Agreement, the terms of this Data Processing Agreement shall take precedence to the extent its terms provide greater protection for Personal Data.

1. Definitions

In this Data Processing Agreement the following terms have the following meanings:

"**Processing**", "**Controller**", "**Personal Data**", "**Processor**", "**Personal Data Breach**", and "**Data Subject**" shall have the same meaning as in 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, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**");

"**Data Processing Agreement**" means this Data Processing Agreement and its appendices;

"**Applicable Laws**" means laws and regulations under EU law and relevant Member State laws that from time to time apply to the Parties (including Applicable Data Protection Laws);

"**Applicable Data Protection Laws**" means from time to time applicable legislation and regulations, including regulations issued by relevant supervisory authorities, protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data, including in particular the GDPR; and

"**Third Country**" means a country which is not a member of the European Union (EU) or the European Economic Area (EEA).

When the context requires it, singular shall include plural, and vice versa.

2. General obligations of the Customer

2.1. The Customer shall in its capacity as Controller ensure the compliance with the Applicable Data Protection Laws.

2.2 The Customer shall in accordance with Section 30 (1) in the GDPR provide the Processor records of processing activities that are required in order for the Processor to be able to comply with its obligation to maintain a record of processing activities in accordance with Section 30 (2) in the GDPR.

2.3 The Customer shall appoint a data protection officer and/or a representative if required by the Applicable Data Protection Laws and, where necessary, provide the Processor with the contact details to such person.

2.4 By entering into this Data Processing Agreement, the Customer confirms that the technical and organizational measures stated in Appendix 2 are considered adequate and sufficient in order to protect the Personal Data covered by this Data Processing Agreement and that the Processor gives sufficient guarantees in accordance with Section 28 (1) in the GDPR.

3. Instructions

3.1 The Controller instructs the Processor to process Personal Data only on behalf of the Controller and in accordance with the instructions by the Controller, as set out in this Data Processing Agreement and the Agreement. The Controller ensures that the instructions comply with the Applicable Data Protections Laws.

3.2 If the Controller leaves instructions that go beyond what is stated in this Data Processing Agreement and the Agreement, the following shall apply. In the event the implementation of actions required by the instructions entail costs for the Processor, the Processor shall inform the Controller thereof and provide an explanation of why the actions entail costs. The Processor shall be required to implement the measures only on condition that the Controller confirms that the Controller shall bear the costs of the actions. The instructions must be submitted in writing.

3.3 The Processor shall notify the Controller if the Processor considers that an instruction regarding the Processing of Personal Data given by the Controller would be in a breach of Applicable Laws ("Challenged Instruction"). The Processor will not in such case be obliged to follow the Challenged Instruction unless the Controller maintains it and assumes full responsibility for the Challenged Instruction. In such case, the Processor shall take the measures required by the Controller provided that the measures do not concern (i) implementation of

technical and organizational measures; (ii) Data Subject's rights; or (iii) appointing Sub-Processors. In case of disagreement, the Processor is entitled to seek guidance from a relevant supervisory authority. If such authority considers that the proposed measures are lawful, the Processor shall take them, in which case Section 3.2 applies with regard to the costs for such measures. The Processor's obligation to notify the Controller according the first sentence in this Section shall not apply to the extent the Processor is prevented from doing so in accordance with Applicable Laws.

4. General obligations of the Processor

4.1 The Processor will Process Personal Data only in accordance with the written instructions issued by the Controller by way of this Data Processing Agreement and the Agreement.

4.2 Notwithstanding what is stated in Section 4.1 above, the Processor may Process the Personal Data to the extent it is necessary for the Processor in order to comply with legal requirements under Applicable Laws to which the Processor is subject. If so, the Processor shall inform the Controller of that legal requirement before the Processing, unless Applicable Laws prohibit the Processor from providing this information.

4.3 The Processor shall upon request by the Controller assist the Controller by providing with necessary information that the Processor has access to, in order for the Controller to be able to comply with its obligations to perform a data protection impact assessment in accordance with Section 35 GDPR and consult the supervisory authority in accordance with Section 36 of the GDPR, regarding the Processing of Personal Data that is conducted in accordance with this Data Processing Agreement. The Processor is entitled to compensation for the costs from the Controller for such measures. The Processor's obligation to assist the Controller is limited to such information that the Controller otherwise has no access to.

5. Security measures

5.1 The obligation to implement technical and organisational measures to protect the Personal Data

5.1.1 The Processor shall implement appropriate technical and organisational measures in accordance what is provided in Appendix 2 to protect and safeguard Personal Data that is processed against Personal Data Breaches. The Processor shall have a right to change these measures on the condition that the changes do not result in a lower level of protection of the Personal Data and at least reach the level of protection that follows from the Applicable Data Protection Laws. In case the Controller requests that the Processor shall take technical and organizational measures that go beyond what is stated above in this Section 5.1.1, Section 3.2 shall apply to the cost allocation for such measures.

5.2 Access to Personal Data etc.

5.2.1 The Processor shall ensure that access to the Personal Data is limited to those employees of the Processor who need access to the Personal Data in order for the Processor to fulfill its obligations under this Data Processing Agreement and the Agreement as well as in order to perform their job duties.

5.2.2 The Processor shall ensure that all employees authorized to access and Process the Personal Data have committed themselves to confidentiality.

5.3 Personal Data Breach

5.3.1 In the event of a Personal Data Breach at the Processor, the Processor shall notify the Controller about the Personal Data Breach without undue delay after when the Processor became aware of such Personal Data Breach. Moreover, the Processor shall provide such information that follows from the information obligation in Section 33 (3) in the GDPR, that the Processor has access to and that the Controller cannot access by other means.

5.3.2 The notification to the Controller shall include the following Information:

5.3.2.1 a description of the nature of the Personal Data Breach including the categories and number of Data Subjects concerned and the categories and number of Personal Data records concerned;

5.3.2.2 the likely consequences of the Personal Data Breach; and

5.3.2.3 a description of the measures taken or proposed to be
taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.3.3 Where, and in so far as, it is not possible for the Processor to provide the above information in Section 5.3.2 above at the same time, the information may be provided in phases (without undue delay).

6. Access to information

6.1 The Processor shall document the measures that the Processor has taken in order to comply with its obligations in this Data Processing Agreement. The Controller shall have a right to receive a copy of the latest version of such documentation.

6.2 Upon the Controller's request, the Processor shall show that is meets the requirements under Article 28 of the GDPR. The Parties agree that this may be done by providing a report prepared in accordance with standards that has been prepared by a third party ("**Report**").

6.3 If further inspection measures than those stated above in Section 6.2 are required by the Applicable Data Protections Laws, the Controller may require an inspection at the site ("**Site Inspection**"). The following terms apply for Site Inspections:

(i) Site Inspections are limited to the resources and personnel at the Processor that are involved in the Processing of Personal Data covered by this Data Processing Agreement. This means that Site Inspections may not under any circumstances comprise other information regarding the Processor's business that is irrelevant for the Processors Processing of Personal Data on behalf of the Controller;

(ii) Site Inspections may not be conducted more often than once a year, unless otherwise required by the Applicable Data Protections Laws or as a consequence of a substantial Personal Data Breach that has affected the Personal Data that is covered by this Data Processing Agreement;

(iii) Site Inspections shall be conducted under office hours and in a manner that affects the Processor's business in the least possible way and in accordance with the Processor's security policies;

(iv) the Controller shall bear the costs that relate to the Site Inspections and preparing reports of the findings during Site Inspections;

(v) Site Inspection shall, when possible, be conducted by a third party chosen by both Parties. The Controller shall ensure that such third party undertakes a confidentiality undertaking regarding all information that the third party may get access to during the inspection and is liable to the Processor for any breaches of the confidentiality undertaking by the third party. All costs that relate to an inspection shall be borne by the Controller, including any costs that the Processor has for the cooperation in such inspection.

(vi) Site Inspection shall be preceded by at least thirty (30) days written notice. Reports and reports from Site Inspections are considered the Processor's confidential information and shall not be disclosed to third parties unless required by Applicable Laws or if the Processor has consented thereto in writing.

7. Use of Sub-Processors

7.1 The Processor may engage outside sub-contractors, consultants or other third parties to Process Personal Data on behalf of the Controller ("**Sub-Processors**"). Any data processing agreement with a Sub-Processor shall impose corresponding and not less restrictive data protection obligations on the Sub-Processor than what follows from this Data Processing Agreement. Information about Sub-Processors are available upon request and are approved by Controller.

7.2 The Processor shall, in the event the Processor engages a Sub-Processor make available information to Controller upon Controller's request corresponding to that stated in Appendix 1.

7.3 The Controller has a right to, with providing a cause within five (5) working days after having received information about a Sub-Processor, object against the Processor engaging the Sub-Processor. If the Controller has not objected within the stated time, the proposed Sub-Processor is deemed accepted. If the Controller objects to the Sub-Processor, the Processor has a right to choose one of the following alternatives: (a) refrain from engaging the Sub-Processor to process Personal Data covered by this Data Processing Agreement (b) take measures that reasonably eliminate the reason for the Controller's objection; or (c) temporarily or permanently cease to provide the part of the service/services that entail Processing of Personal Data by the Sub-Processor at hand. If none of these alternatives are feasible and the Controller maintains its objection after thirty (30) days has passed after the objection was made, each Party has a right to by giving a reasonable notice period terminate that part of the service/services that entails Processing of Personal Data by the Sub-Processor at hand.

7.4 The Processor shall, in addition to the information stated in Section 7.2 above, upon the Controller's request, provide information regarding the measures that have been taken to ensure that the Sub-Processor gives sufficient guarantees to implement technical and organisational measures in a way that complies with the requirements in Applicable Data Protection Laws.

7.5 The Processor is liable towards the Controller for the Processing of Personal Data by the Sub-Processors covered by this Data Processing Agreement in accordance with Applicable Data Protection Laws.

8. Liability

The terms and conditions regarding liability in the Agreement shall apply this Data Processing Agreement.

Administrative fines that have been imposed on one Party pursuant to Art. 83 of the GDPR, or Chapter 6 Section 2 of the supplementary Data Protection Act (2018:218) shall be borne by the Party on which such fines have been imposed.

9. Data Subjects' rights

9.1 The Controller shall be liable to assess if a Data Subject request is legitimate or not and provide the Processor with instructions regarding the scope of support that is required.

9.2 The Processor shall without undue delay inform the Controller about complaints and other notices from Data Subjects exercising their rights. However, the Processor shall not, unless the Controller has given the Processor sufficient instructions thereof, communicate with the Data Subject.

9.3 The Controller is responsible for handling in connection with the Data Subject exercising its rights under Applicable Data Protection Legislation.

9.4 The Processor shall upon the request assist the Controller with the following appropriate technical and organizational measures in connection with a Data Subject exercising its rights under Chapter III in the GDPR:

(i) In connection with a request of information the Processor shall provide the Controller with such information that is covered by Sections 13 and 14 in the GDPR to the extent such information is available for the Processor and the Controller does not have access to such information.

(ii) In connection with a request of right of access the Processor shall provide the Controller with such information that is covered by Section 15 in the GDPR to the extent such information is available for the Processor and the Controller does not have access to such information.

(iii) In connection with a request of rectification (Section 16 in the GDPR), erasure (Section 17 in the GDPR), restriction of processing (Section 18 in the GDPR), and data portability (Section 20 in the GDPR), the Processor shall, to the extent the Controller cannot take the measures requested by the Data Subject(s)assist the Controller to take such measures.

(iv) The Processor shall, on instructions for the Controller, notify the Sub-Processors that Process Personal Data covered by the request by the Data Subject to rectify, erase or restrict the processing (Section 19 in the GDPR) that such request has been made. The Controller undertakes to inform other recipients.

(v) In relation to the Data Subject's right to object processing in Section 21-22 in the GDPR, the Controller shall assess whether the objection is legitimate and how it is to be handled. In the event the Controller wishes to be assisted by the Processor, the Controller shall issue further instructions, whereby the routines described in Section 3.2 shall apply to the Processor's right to compensation for costs.

9.5 In the event the Controller requests that the Processor shall take technical and organisational measures in addition to what is stated in Section 5.1.1 for the purpose of handling the Data Subject's rights under this Section 9, the Section 3.2 shall apply to the costs for such measures.

9.6 Notwithstanding what is stated above in Section 9.5, the Processor is entitled to compensation for reasonable expenses due to a Data Subject exercising its rights as set out above.

10. Return of Personal Data

10.1 Upon termination of the Agreement, the Processor shall return (and/or upon the Controller's written request in a secure and irreversible way delete or anonymise) all Personal Data which belongs to the Controller that the Processor and or any Sub-Processors have in its possession or control. This applies unless the Processor is required under Applicable Laws to continue to store the Personal Data. Unless the Controller has within thirty (30) days after the termination of the Customer Agreement instructed the Processor that the Controller wishes that the Processor returns or in secure way deletes the Personal Data, the Processor shall, provided that the Processor is not required to store Personal Data under Applicable Laws, without undue delay ensure that the Personal Data is deleted in a secure way.

11. Transfer and Processing of Personal Data in a Third Country

11.1 The Processor may transfer Personal Data processed on behalf of the Controller to a Third Country, provided that:

11.1.1 the Third Country provides an adequate level of protection for Personal Data in accordance with an adequacy decision issued by the EU Commission that covers the Processing of Personal Data;

11.1.2 the Processor ensures that there are appropriate safeguards in place in accordance with Applicable Data Protection Laws, e.g. standard data protection clauses adopted by the EU Commission under Applicable Data Protection Laws, covering the transfer and Processing of Personal Data; or

11.1.3 other exception exists under Applicable Data Processing Laws that covers the Processing of Personal Data.

11.2 For the avoidance of doubt, Personal Data may not be transferred to any Third Countries unless one of the conditions above in Section 11.1 applies.

12. Term and termination

This Data Processing Agreement will enter into force on the Agreement Date and is valid during the term of the Agreement or the longer period of time that the Processor or any Sub-Processor engaged by the Processor Processes Personal Data on behalf of the Controller.

14. Amendments

Additions and amendments to this Data Processing Agreement shall be in writing and duly signed by both Parties to be valid. Each Party may request amendments to this Data Processing Agreement that are justified by changes in Applicable Data Protection Laws.

15. Applicable law

This Data Processing Agreement shall be governed by Swedish law, without the application of the choice of law rules, to the extent Applicable Data Protection Laws do not prescribe otherwise.

16. Disputes

Disputes arising out of this Data Processing Agreement shall be solved in Sweden to the extent Applicable Data Protection Laws do not stipulate otherwise.

APPENDIX 1

Categories of Data Subjects
Applicants using the service provided by Jobbrella.

Categories of Personal Data
Personal data from applicants, including applicant's name, applicant's email, applicants CV and answers to questions.

Purpose(s) of the Processing
To gather data for the Assignment and for anonymization and then analyze anonymized and aggregated data in order to understand how to optimize the platform and the applicant tracking system and an employer branding service provided to the Customer.

To ensure the quality of the collected Personal Data by comparison.

Processing Operations
Personal Data is anonymized, to be able to calculate statistics.

Location, and, where applicable, safeguard for third country transfers
Personal data is Processed in EU/ESS.

Retention of Personal Data
The Personal Data is deleted after Processing in accordance with Applicable Data Protection Laws.

Contact details of the contact person at the Processor:
support@jobbrella.se

APPENDIX 2

Technical and organisational measures

Anonymization
The following measures shall be implemented to address the anonymization of the personal data such as:

- The use of obfuscation of clear text data to anonymize personal data.

- The timely removal of personal data once it is no longer necessary to store it

Encryption
The following measures shall be implemented to address the encryption of the personal data:

- use secure code signing, symmetric encryption, asymmetric encryption and,
- provide security guidelines to the Processor to ensure they manage encryption of local network, people counter hardware, and transfer of personal data.

Confidentiality of the processing systems and of the Services
The following measures shall be implemented to address the confidentiality of the processing systems and of the Services:

- use access control mechanisms to prevent persons from gaining access to data processing systems with which personal data are processed or used without authorization,
- administer and monitor credentials with privileged access management (PAM),
- Data Breach Response Policy,
- ensure that data collected for different purposes can be processed separately.

Integrity of the Processing Systems and of the Services
The following measures shall be implemented to address the integrity of the processing systems and of the Services:

- provide security guidelines to the Processor to ensure they manage the integrity of the local network, people counter hardware, and transfer of personal data,
- protection by technical and organizational means regarding authorizations, protocols/logs including analyzing protocols, audits, automatic exclusion protocols, etc,
- Data Classification Policy,
- ensure that measures and activities are logged in a secure manner.

Availability of the processing systems and of the Services
The following measures shall be implemented to address the availability of the processing systems and of the Services:

- ensure that personal data are protected from accidental destruction or loss,

Resiliency of the processing systems and of the Services
The following measures shall be implemented to address the resiliency of the processing systems and of the Services:

- ensure that systems and services are designed in a way that they can handle punctual or constant high load of processing operations.

Ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident
The following measures shall be implemented to address the ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident:

- backup concept,
- cloud services.

Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures
The following measures shall be implemented to address the regularly testing, assessing and evaluating of the effectiveness of technical and organizational measures:

- Information Security Policy
- Anonymization Policy,
- ensure development following Secure Software Development,
- use ISO/EIC 27001-27002 and ISO/EIC 27005 as frameworks for development,
- review by the data protection officer,
- external reviews, audits, certifications.