

data processing agreement

Parties

1. Homerun B.V., a private company with limited liability incorporated under the laws of the Netherlands, having its registered seat in Amsterdam, and having its registered office at Singel 542, 1017 AZ Amsterdam, registered with the Trade Register (Handelsregister) with number 66911524 (hereafter: “Processor”);
2. I&L Biosystems GmbH _____, located at
Köningswinterer Str. 409, 53639 Köningswinter, Germany _____ registered with the Trade Register with number HRB Siegburg 10580 (hereafter: “Controller”);

The parties 1 and 2 mentioned above hereinafter also to be referred to as the “Parties” and each individually as a “Party”;

Whereas

- A. The terms used in this Agreement (in particular terms beginning with a capital letter) correspond with the terms used in the General Data Protection Regulation (GDPR). All aforementioned legislation including all other applicable legislation and regulations that apply to the processing of personal data under this DPA shall hereinafter be referred to as “Relevant Legislation”.
- B. Processor has developed software intended to streamline recruitment processes of organisations. This software (“Software”) is offered through its website in the form of Software as a Service (SaaS).
- C. The Software provides Controller with the ability to process various information, including personal data of various Data Subjects within the meaning of the Relevant Legislation.

- D. Controller wishes Processor to store, process, edit and secure this personal data (the “Personal Data”) within the meaning of the Relevant Legislation, whereby Controller determines the purpose and means of the processing. In this respect, Processor will act as a “Processor” within the meaning of the Relevant Legislation and Controller will act as a “Controller” within the meaning of the Relevant Legislation. The details of the processing of Personal Data are described in Annex 1.
- E. The Relevant Legislation requires an agreement between Controller and Processor. Furthermore, the Relevant Legislation obliges Controller to ensure that Processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing of Personal Data will meet the requirements of the Relevant Legislation.
- F. Parties now wish to enter into such a Data Processing Agreement (the “Agreement”) in order to regulate the processing of Personal Data that Processor will be performing on behalf of Controller. Besides this Agreement, Parties have entered into a service agreement (the “Assignment”) setting out the terms and conditions for the services to be provided by Processor. The Assignment is either Processor’s online User Agreement at <https://www.homerun.co/terms-of-service> or, where relevant, a separate contract negotiated between Processor and Controller.

Agreement

Article 1: Obligations of the Controller

- 1.1 Data and information: Processor either receives Personal Data from Data Subjects on behalf of Controller or receives such Personal Data from Controller. Parties shall provide all information and assistance which are reasonably required in order for the other Party to (a) provide the services as agreed on in the Assignment and (b) comply with this Agreement and (c) comply with the Relevant Legislation.
- 1.2 Personal Data: The Software allows Controller to specify (configure) which categories and individual fields of Personal Data are processed by the Processor. The responsibility for ensuring that all Personal Data collection, as specified (configured) by Controller, is lawful, lies exclusively with Controller, provided that the Software offers the necessary tools for this.
- 1.3 Compliance with law: The written instructions given by Controller to Processor in respect of the Personal Data shall at all times be in accordance with the Relevant Legislation.

1.4 Liability: Controller and Processor are liable as described in the Relevant Legislation, more specific in article 82 of the General Data Protection Regulation.

Article 2: Obligations of the Processor

- 2.1 Compliance with law: Processor shall comply with the Relevant Legislation.
- 2.2 Instructions of Controller, purpose and means of processing Personal Data: Processor undertakes that it shall process the Personal Data strictly and only on behalf of Controller, in accordance with Controller's written instructions and under Controller's responsibility, except in case that legal requirements applicable to Processor require otherwise. In such case, Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on the important grounds of public interest. Processor shall not use the Personal Data for its own purposes. The processed Personal Data shall remain the property of Controller and/or the relevant Data Subjects.
- 2.3 (Intentionally left blank)
- 2.4 Confidentiality: Processor shall treat the Personal Data as confidential, and shall ensure that access to the Personal Data is limited to only those employees who require access to it for the purpose of carrying out the services under the Assignment. Processor shall ensure that all persons authorised to process the Personal Data have committed themselves to confidentiality. Processor shall ensure that all such employees shall comply with all Relevant Legislation.
- 2.5 Rights of the Data Subjects: Processor shall assist Controller promptly with all requests to exercise their legal rights under the Relevant Legislation which may be received from the Data Subjects of the Personal Data. Processor shall not respond to the Data Subjects for any such requests unless expressly authorised or instructed to do so by Controller in writing (including per e-mail).
- 2.6 Non-disclosure: Processor shall not disclose the Personal Data to any third party other than with prior written consent of Controller, unless the disclosure is required by law applicable to Processor.
- 2.7 Transfer of data outside EEA: Processor shall not transfer or process Personal Data outside the EEA other than with Controller's written consent (including per e-mail). Any transfer by the Processor of Personal Data to a location outside the EEA must be pursuant to one of the lawful transfer mechanisms described under articles 44 GDPR. For Sub-Processors storing data outside the EEA, this consent may be part of the consent given for the use of Sub-Processors as described in 2.9 and 2.10.
- 2.8 Subcontracting: Controller agrees that Processor may use subcontractors to fulfil some of its obligations under the Assignment. Processor may only subcontract the

processing of Personal Data to others ("Sub-Processors") with consent of Controller. Processor shall impose the same or higher data protection obligations to any Sub-Processor as those set out in this Agreement between Controller and Processor, by way of a data processing agreement. With respect to each Sub-Processor, Processor shall, before the Sub-Processor first processes any Personal Data of Controller, carry out due diligence to ensure that the Sub-Processor is capable of providing an adequate level of protection for the Personal Data. Processor remains fully liable to Controller for the performance of the data protection obligations of any Sub-Processors.

- 2.9 Existing Sub-Processors: The details of the Sub-Processors already known at the time of execution of this Agreement are listed in Annex 2, including their function and the location where the Personal Data is stored. Controller hereby consents to the use of these Sub-Processors by Processor.
- 2.10 Changes to Sub-Processors: Processor may further subcontract to other Sub-Processors or change existing Sub-Processors if Processor informs Controller of the identity of the Sub-Processor, their function and the location where the Personal Data will be stored, by contacting the contact person(s) provided in Annex 3 in writing or in text form (including per e-mail), and the Controller does not object to the planned Sub-Processing in writing or in text form (including per e-mail) within thirty (30) days as from given notice by the Processor. The Controller shall not unreasonably object to the planned Sub-Processing.
- 2.11 Security measures: Processor shall implement and employ appropriate technical and organisational measures to protect the Personal Data against unauthorised use or access, loss, destruction, theft, or disclosure, in accordance with Article 32 GDPR. Processor shall at least take the security measures described below in order to protect the Personal Data:
- Responsibility for information security shall be assigned to relevant management;
 - An appropriate information security policy shall be available, approved by management and communicated to all staff members;
 - Members of staff shall receive regular security and privacy awareness training;
 - All access to Personal Data shall be authenticated by a password;
 - Access to Personal Data shall be controlled based on a need to know, using the least-privilege principle;
 - Network transmissions of Personal Data shall be encrypted using Transport Layer Security (TLS);
 - Network services providing access to Personal Data shall be protected by firewalls with a default-deny setting;

- Appropriate physical security measures shall be implemented regarding the access to the Personal Data.
- 2.12 Data Protection Impact Assessment and Prior Consultation: Processor shall assist Controller in ensuring compliance with the obligations regarding conducting a Data Protection Impact Assessment and/or Prior Consultation where deemed necessary by Controller.
- 2.13 Personal Data Breach: In case of a Personal Data Breach, Processor shall promptly take all adequate remedial measures to terminate the Personal Data Breach and to mitigate any possible damages. Processor shall notify Controller of any information security incident that may impact the processing of the Personal Data covered by this Agreement, without undue delay after discovering or becoming aware of such incident by contacting the contact person(s) provided in Annex 3 (either in writing or by phone). Following the report of the incident, Processor shall cooperate with Controller's Compliance and Information Security staff whilst they carry out a risk assessment, root cause analysis and identify any corrective action required. Processor shall provide the following information when reporting a security incident: the date and time the breach was discovered, the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, the known and expected consequences of the breach, the measures taken by Processor to address the breach, the measures taken by Processor to limit the consequences of the breach, and contact information for further information about the breach and any other relevant information Controller may reasonably require. Controller and Processor shall provide each other with up to date contact information for such notifications in Annex 3 of this Agreement, and provide updates to those details whenever needed. The Parties agree to coordinate and cooperate in good faith on developing the content of any related public statements or any required notices for the affected persons. Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by EU or Member State law to which Processor is subject, in which case Processor shall to the extent permitted by such law inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the Personal Data Breach.
- 2.14 Removal of Personal Data after termination or cancellation: Upon termination or expiration of this Agreement for whatever reason, or upon prior, written (including per e-mail) request by Controller, Processor shall immediately cease to process Personal

Data and shall promptly return to Controller all such Personal Data, or destroy the same, in accordance with such instructions as may be given by Controller at that time, unless retention of the Personal Data is required by law applicable to the Processor.

- 2.15 Audit: Controller reserves the right to carry out compliance and information security audits (including inspections) with regard to the practices of Processor, in order to satisfy itself that Processor is adhering to the terms of this Agreement, but only upon giving reasonable notice and within normal business hours. Where a Sub-Processor is used, the Processor agrees that the Controller may also, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks of the Sub-Processors to ensure their adherence to the terms of this Agreement. If it appears from an audit that Processor has failed to comply with the obligations under this Agreement or the Relevant Legislation, Processor shall correct this non-compliance promptly.
- 2.16 Indemnities and liability: Processor shall indemnify Controller against any and all direct damages in connection with, arising out of or relating to, in whole or in part Processor's failure to comply with the obligations under this Agreement or Relevant Legislation.
- 2.17 Illegal instruction: If, in Processor's opinion, any instruction from Controller infringes Relevant Legislation, the Processor shall immediately inform Controller.

Article 3: Governing Law

This Agreement is exclusively governed by the laws of The Netherlands. Any disputes or claims arising out of or related to this Agreement shall exclusively be submitted to the competent courts in Amsterdam.

Article 4: Term, Amendment, Termination, Miscellaneous

- 4.1 This Agreement shall become effective on the signing date, and continue in full force and effect for the same period as the Assignment. If Controller chooses to suspend the use of the Software (and therefore suspend the obligations of both parties to the Assignment) or if Controller chooses to terminate the Assignment while at the same time instructing Processor to retain the Personal Data, this Agreement will continue to apply in full force and effect until the Personal Data has been deleted from Processor's systems.
- 4.2 This Agreement embodies the entire understanding of the Parties with respect to the subject matter thereof. This Agreement supersedes previous agreements or understandings relating to this subject matter between the Parties, both in writing and oral, including correspondence. This Agreement may be modified or amended only by written agreement signed by both Parties.
- 4.3 (Intentionally left blank)
- 4.4 (Intentionally left blank)
- 4.5 If any provision of this Agreement shall be deemed unlawful, void or otherwise unenforceable, then such provision shall be deemed severable from this Agreement and shall not affect the validity and enforceability of any remaining provisions. Any such unenforceable provision shall be replaced or be deemed to be replaced by a provision that is considered to be valid and enforceable and which interpretation shall be as close as possible to the intent of the invalid provision.
- 4.6 In case of contradiction between the provisions of this Agreement, the Assignment and earlier agreements on the processing of Personal Data, the provisions of this Agreement prevail unless otherwise expressly stated in this Agreement.

THUS AGREED AND SIGNED ON: Oct 14, 2022

Homerun B.V.

Processor



Signature of authorised representative

Bob Kreefft

Name of authorised representative

COO

Title of authorised representative

I&L Biosystems GmbH

Controller



Signature of authorised representative

Daniel Bindels

Name of authorised representative

Managing Director

Title of authorised representative

Annex 1: Description of the Processing

Nature and Purpose of Processing

Processor provides a standardised software platform for organisations to streamline their recruitment processes by centrally managing job openings, candidate applications and interactions regarding hiring.

Controller's purpose for using this software and therefore for this processing of Personal Data is to recruit new people for its organisation.

Categories of Data Subjects

- Candidates: Persons who apply for employment with Controller, or persons whom Controller would like to consider or approach for employment with Controller.
- Users: Persons who have a user account in the Software, typically employees or consultants for Controller, in their capacity as members of a hire team for a certain job.

Types of Personal Data Processed

For Candidates, the Personal Data can consist of: general identification, the job he/she wants to apply for, education, work experience, photo, personal interests, links to social media accounts or profiles, any other answers to questions defined by Controller during the application process, appointments or events relating to the recruitment process, comments or assessments by the hire team about the candidate's suitability for the role, communication between the hire team and the candidate, and status of the application.

For Users, the Personal Data typically consists of: general identification, authentication and authorisation data, configuration of the user profile, comments or assessments about candidates' suitability for a certain role, as well as communication between the user (member of one or more hire teams) and candidates or other users.

The Software allows the Controller to significantly customise the amount and types of Personal Data that will be collected from the Candidates as well as the Users. It is the exclusive responsibility of the Controller to ensure that this customisation is lawful with regards to the Relevant Legislation, provided that the Software provides the necessary tools for this.

Special Categories of Data

Controller or Data Subjects may submit Personal Data to Controller through the Software which may concern special categories of data. The extent of this processing is determined and controlled by the Controller in compliance with Relevant Legislation.

Processing Activities of Processor

- Providing the services as agreed under the Assignment

Annex 2: Sub-Processors

In accordance with clause 2.9, Processor provides a list of Sub-Processors engaged in the processing already known at the time of execution of this Agreement. The following Sub-Processors are approved at the time of execution of the Agreement by the Controller, and shall be deemed to comply with the Relevant Legislation and the processing requirements set out in the Agreement:

Identification	Function	Location of Personal Data	Transfer Mechanism
Amazon Web Services	Hosting provider	EU	N/A
SendGrid	Sending emails to Users and Candidates	USA	SCC (Standard Contractual Clauses)

Annex 3: Contact Details for Notifications

Processor

Homerun BV
Singel 542
1017 AZ Amsterdam
The Netherlands
privacy@homerun.co
+31 20 2615382

Controller

Please provide contact details that can be used for any notifications with regards to personal data protection. If your company has a Data Protection Officer, please include at least their contact details.

Contact Person	Role	Telephone	Email
Marjo van Bijnen	HR	+31416675300	humanresources@il-biosystems.nl
Herr R. Land	DPA Officer		rl@il-biosystems.de