Agreement on contract processing

between

Customer Company and Address

- hereinafter referred to as the Client -

and

PitchYou GmbH, represented by the Managing Director Robin Sudermann, Campusallee 9, D-51379 Leverkusen

- hereinafter referred to as the Contractor -

§ 1 Subject of the order

(1) The subject matter of the order is to be taken from the respective service agreement of the parties.

(2) The Contractor shall process personal data of the Client as well as personal data of applicants on behalf of the Client. The Parties agree that the provisions of the EU General Data Protection Regulation (GDPR), in particular the provisions on contract data processing, shall apply to the contract on the processing of personal data on behalf of the Principal. The Contractor declares that it is in a position to properly perform the commissioned services in accordance with Article 28 of the GDPR.

(3) The contract regulates the data protection measures within the meaning of Art. 28 GDPR and the rights and obligations of the Client and the Contractor to fulfil the data protection requirements.

§ 2 Duration, term of the order

The term of this contract is linked to the term of the service contract.

§ 3 Categories of data subjects

The performance of the contract and data processing by the Contractor may involve the following categories of natural persons of the Client:

☒ Employees
☒ Applicant

§ 4 Types of personal data

The following types/categories of data are the subject of the collection, processing and/or use of personal data:

Applicant data (name, address, contact details, date of birth, professional history, professional qualifications, personal qualifications, availability in terms of time and place, personal history, profile picture, profile video), names and contact details of own employees.

§ 5 Place of processing

(1) Data processing shall take place exclusively on the territory of the Federal Republic of Germany or within the European Union or the states of the European Economic Area. Processing in other countries is only permissible with the prior consent of the Client and only insofar as an adequacy decision of the EU Commission pursuant to Article 45 (3) of the GDPR exists or an adequate level of data protection is ensured by other suitable guarantees within the meaning of Article 46 (2) of the GDPR. At the request of the Client, the Contractor shall provide evidence of the existence of an adequacy decision of the EU Commission pursuant to Art. 45 (3) of the GDPR and/or the guarantees and an adequate level of protection. Proof can be provided **by presenting a corresponding certificate from an accredited certification body in accordance with Art. 43 of the GDPR. The Contractor undertakes to ensure compliance with the guarantees and an adequate level of protection. The Client reserves the right to verify the existence of the EU Commission's adequacy decision as well as the guarantees and compliance with an adequate level of protection at any time within the scope of its audit and control rights.**

§ 6 Control and audit rights of the Client

(1) The Client alone shall be responsible for assessing the permissibility of the processing of personal data and for implementing the rights of the data subjects. In the case of contract data processing, the Client shall only work with processors who provide sufficient guarantees that appropriate technical and organisational measures are in place to meet the requirements of the GDPR, in accordance with Article 28 (1) sentence 1 of the GDPR.

(2) Thereafter, the Client shall be obliged and authorised to check compliance with the provisions on data protection and the contractual agreements, in particular the technical and organisational measures taken by the Contractor, to the necessary extent before the start of the data processing and, at its discretion, also repeatedly after prior consultation during normal business hours.

For this purpose, the Client shall be authorised to demand written information and the submission of evidence of the data protection measures established as well as of the manner of their technical and organisational implementation, to enter the Contractor's premises and business premises, to carry out tests and inspections at its discretion and, to the extent required, to inspect processing-relevant documents, processing and sequence logs, systems and stored data and regulations, guidelines and manuals regulating the commissioned data processing. This also includes evidence of the appointment of a data protection officer (if necessary), the commitment of employees to maintain confidentiality and technical and organisational concepts, e.g. contracts with subcontractors. The same rights shall also apply to agents of the Client, e.g. experts or surveyors, insofar as they are under a special obligation to maintain confidentiality or are subject to professional secrecy obligations under penalty of law.

(3) The Client's rights shall exist during the term of this agreement and beyond until the claims arising from this agreement become statute-barred, but at least as long as the Client stores personal data from the commissioned processing operations.

(4) The examination takes place after prior registration. In special cases, in particular if processing problems exist, reportable incidents have occurred or supervisory measures are pending or have been initiated, the inspection may also be carried out without prior notification.

§ 7 Powers of instruction of the Client

(1) Data shall be processed exclusively within the framework of the service agreements concluded and this agreement on commissioned processing only on the basis of documented instructions from the Client. Within the scope of the agreed order description, the Client reserves the right to issue instructions in the form of individual instructions on individual data processing processes of the Contractor. The instructions shall be given in writing, in written form or in another suitable electronic format. Verbal instructions shall be confirmed immediately in written form, in writing or in an electronic format. The instructions shall be kept for the duration of the contractual relationship, but at least for the duration of their validity.

The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates the GDPR or other data protection regulations. The Contractor may suspend the execution of the instruction until confirmation by the Client. The Client shall be liable for unlawful instructions and shall indemnify the Contractor in this respect against claims for damages and other claims.

Changes in the persons authorised to give instructions or in the recipients of instructions must be notified without delay.

(2) Changes to the processing object and process changes shall be jointly agreed and documented.

§ 8 Duties of the Contractor

(1) Processing obligations

The Contractor shall carry out the order exclusively within the framework of the agreements made and in accordance with the Client's instructions. The Contractor shall not use the data for any other purposes and shall in particular not be entitled to pass them on to third parties.

Extracts, copies or duplicates of data or data carriers may only be produced and used without the knowledge of the Client insofar as this is necessary for the execution of the order or to ensure proper data processing or if there is a legal or other obligation to retain data. Any excerpts, copies or duplicates made shall be securely deleted by the Contractor immediately after completion of the processing or use or destroyed in accordance with data protection law, or handed over to the Client.

Decisions on the organisation of data processing and on the procedures used that are significant for security shall be agreed with the Client. The Contractor may not provide information to third parties or the data subject or may do so only on the Client's instructions. The Contractor may only provide information to employees of the Client to authorised persons.

The Contractor undertakes to only use software, data or data carriers that have been reliably checked for freedom from harmful software in order to avoid the introduction of viruses, etc.

(2) Obligation to tolerate controls

The Contractor undertakes to prove compliance with the technical and organisational measures taken in inspections by the Client, to provide information and to submit the relevant documents or to grant access to the required documents and systems and to tolerate and support corresponding inspections by the Client on site after prior agreement. It undertakes to provide all necessary information in the event of incidents relevant to data protection and data security and to support the clarification of such incidents as far as possible.

Proof of appropriate technical and organisational measures can also be provided by submitting test certificates or certificates or by a certification or data protection audit by an independent institution or an authorised expert. Irrespective of this evidence, the Contractor is obliged to tolerate inspections by the Client in accordance with Section 6 of this Agreement.

(3) Information duties

The Contractor shall be obliged to notify the Client without being asked of any significant changes in the technical and organisational conditions which reduce the security and correctness of the performance of the contractual services.

The Contractor shall inform the Client about inspections by the supervisory authority for data protection, in particular pursuant to Art. 58 GDPR, and about any measures and requirements for the protection of personal data.

The Contractor undertakes to provide the Client, upon request, with the information required to comply with its obligation to monitor the order and to make the relevant evidence available. It shall inform the Client without delay of the expiry or revocation of certificates or of measures pursuant to Art. 41 (4) of the GDPR.

The Contractor shall inform the Client of the name and contact details and any changes in the person of the company data protection officer or, if there is no obligation to appoint one, the name and contact details of the other competent body.

(4) Duties of cooperation and support

The Contractor undertakes, within the scope of Article 28 (3) (e) and (f) of the GDPR, to provide without undue delay the information required for the list of processing activities as well as for the risk identification and any data protection impact assessment and, insofar as its area of responsibility is concerned, to cooperate to the necessary extent in the identification of the risks and any data protection impact assessment and to support the Client in the fulfilment of the rights of the data subjects.

(5) Organisational duties

The Contractor undertakes to set up measures and documentation that enable the control and traceability of all activities and processing procedures related to the contract processing in the sense of a contract control and the correctness of the data processing. Data protection incidents and other security-relevant processing malfunctions shall be documented, including their effects and the remedial measures taken, and reported to the Client. The documentation shall be made available to the Client without delay.

If the processing is carried out from private residences or from a third location, the Contractor undertakes to ensure, by means of appropriate regulations and security measures, that the confidentiality of the data and the security and controllability of the processing are maintained to the same extent as is the case if the service is carried out from the Contractor's location.

§ 9 Preservation of confidentiality and other secrets

(1) Personal and other data or information which become known to the Contractor in the course of the performance of this contract may only be used by the Contractor for the purposes of the commissioned service. The Contractor undertakes to maintain the confidentiality and integrity of the personal data and to treat confidentially all personal data and other internal company circumstances, data and information (company secrets) of which it becomes aware in connection with the acceptance and processing of the order and to oblige the employees working within the scope of this contract to maintain confidentiality in writing, even after the termination of the employment relationship, and to instruct them about the data protection obligations arising from this contract, the binding nature of the processing of the data and its purpose limitation. This confidentiality obligation shall also apply beyond the termination of the contractual relationship.

(2) The Contractor confirms that it is aware of the relevant data protection regulations. The Contractor warrants that it will only use its own personnel for the performance of the work and that it will familiarise the employees involved in the performance of the order with the data protection provisions applicable to them and subject them to regular training.

(3) The Contractor undertakes to observe all other secrets, insofar as they are relevant to the processing, such as social secrecy, telecommunications secrecy and other professional secrets pursuant to Section 203 of the German Criminal Code (StGB), as well as to oblige and instruct employees to ensure that these secrets are observed.

(4) The Contractor shall be obliged to keep secret all knowledge of the Client's administrative access data and data security measures obtained within the framework of the contractual relationship and not to disclose it to third parties under any circumstances. The Contractor may only make use of the access rights granted to it to the extent necessary for the performance of the data processing. The obligation to maintain confidentiality and other secrets shall also apply beyond the termination of this contract.

§ 10 Subcontracting relationships

(1) By signing this contract, the Client agrees to the involvement of the subcontractors listed in detail in Annex 2.

(2) In the event of the involvement of further subcontractors, the Contractor shall carefully select the subcontractors according to their suitability. The Client hereby already expressly consents now to the engagement of subcontractors who guarantee data processing exclusively within the European Union (EU) and the European Economic Area (EEA) and also fulfil all requirements for legally compliant data processing. The Contractor shall inform the Client in good time of any intended change with regard to the involvement or replacement of other contract processors, which shall give the Client the opportunity to object to such involvement or change if there is good cause. The involvement of subcontractors outside the EU and the EEA (also in the case of affiliated companies) requires the express written consent of the Client.

(3) The Client may revoke its consent to subcontracting in the event of good cause to be proven by it, in particular in the event of a breach of the law or a breach of contract. The subcontracting shall then be discontinued immediately.

(4) The Contractor shall structure the contractual agreements with each subcontractor in such a way that they are comparable with the data protection provisions of this contract. It shall regularly check compliance with these duties. The forwarding of data to a subcontractor is only permissible once a corresponding contract processing agreement has been concluded and the subcontractor

has fulfilled all the requirements of this contract. Upon written request, the Contractor shall provide the Client with information on the essential contractual contents and the implementation of the data protection-relevant obligations of the subcontracting relationships, if necessary by inspecting the relevant contractual documents.

(5) Subcontracting relationships within the meaning of this provision shall not include services which the Contractor uses from third parties as an ancillary service to support the execution of the order. These include, for example, other telecommunications services, maintenance and user services, cleaners or inspectors. However, the Contractor is obliged to make appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Client's data, also in the case of subcontracted ancillary services.

(6) The commissioning of subcontractors outside the territory of the Federal Republic of Germany or the European Union or the states of the European Economic Area is only permissible with the prior consent from the Client and only insofar as an adequacy decision of the EU Commission pursuant to Article 45 (3) of the GDPR is available or an adequate level of data protection is ensured by other suitable guarantees within the meaning of Article 46 (2) of the GDPR. In all other respects, the provisions of Section 5 of this contract shall also apply to the commissioning of subcontractors.

§ 11 Notification obligations in the event of disruptions and data protection violations

(1) In the event of a disruption to processing or a data protection breach, the Contractor shall immediately initiate all appropriate and necessary measures to secure the data and to mitigate any damage to the data subjects and to the Client.

(2) The Contractor undertakes to inform the Client without delay of any infringements of regulations on the protection of personal data or of the stipulations made in this agreement. This shall also apply in the event of serious disruptions to the operational process, suspicion of other violations of regulations on the protection of personal data or other irregularities in the handling of personal data of the Client which may have an impact on the persons concerned or the Client or cause damage. Data protection breaches include in particular the loss of confidentiality and the loss or destruction or falsification of the Client's data or other confidential information within the meaning of this contract.

(3) The notification to the Client authority shall include all information that is necessary for the Client to assess the incident and its duty to notify the supervisory authority and the duty to inform the data subjects pursuant to Art. 33 and 34 GDPR and, if necessary, to be able to notify the supervisory authority and, if necessary, to inform the data subjects in due time. The notification to the Client shall include, in particular, information on the nature of the incident and the personal data breach, a description of the likely risks to the interests, fundamental rights and freedoms of the data subjects and a description of the measures already taken to remedy or reduce any potential harm or other risks to the data subjects and the Client.

(4) The Contractor shall document the incident and support the Client in fulfilling its obligation to report and inform pursuant to Articles 33 and 34 of the GDPR and shall take all measures within its scope of responsibility to mitigate adverse consequences for the data subjects and to clarify the incident and its consequences. This shall also apply after termination of the contractual relationship.

§ 12 Rights of the data subjects

(1) The Client alone shall be responsible and liable for safeguarding the rights of the data subjects.

The Contractor may only implement rights of the data subjects according to the instructions of the Client. However, the **C**ontractor shall support the Client in fulfilling requests and claims of affected persons to the extent necessary.

(2) Enquiries by data subjects regarding their rights or information, corrections, deletions of data requested by a data subject shall be forwarded by the Contractor to the Client without delay for processing. Information to third parties may only be given according to the Client's instructions or must be forwarded to the Client for completion. Likewise, information may not be provided directly to employees of the Client, but only via the agreed contact persons.

§ 13 Technical and organisational measures

(1) The Contractor shall ensure a level of protection of the personal data adequate to the risk to the rights and freedoms of the data subjects. To this end, the Contractor undertakes to design and continuously update its internal organisation and the necessary technical and organisational measures, taking into account the respective state of the art, the implementation costs and the nature, scope and circumstances and purposes of the processing and the varying likelihood and severity of the risk to the rights and freedoms of the data subjects, in such a way that they comply with the specific requirements of data protection under the GDPR and ensure the protection of the rights of the data subjects.

The technical and organisational measures include in particular

a) the permanent assurance of the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing of the data,
b) the rapid restoration of the availability of and access to personal data in the event of a physical or technical incident; and
c) the establishment and maintenance of procedures for regularly monitoring, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

(2) The Contractor shall ensure compliance with the technical and organisational measures specified in Annex 1. These measures shall be deemed to be agreed and the description of the measures in Annex 1 shall become part of this contract.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative adequate measures. In doing so, the security level of the defined measures must not be undercut. Significant changes shall be documented.

(4) The Contractor may verify the suitability of the technical and organisational measures to be taken in accordance with Art. 32 of the GDPR, if applicable, by demonstrating compliance with approved codes of conduct pursuant to Art. 40 GDPR or a data protection seal or certification mark pursuant to Art. 42 GDPR issued for the processing operations and locations covered by the contract and relevant to the processing operations covered by this agreement. The Contractor shall notify the Client immediately of any changes to the certificate or its expiry. The control and audit rights of the Client shall remain unaffected.

§ 14 Procedure after termination of the order

(1) After completion of the processing, at the latest after termination of this contract, the Contractor

shall hand over to the Client or, in consultation with the Client, destroy or securely delete in accordance with data protection law all documents and processing or usage results created or personal or other confidential data produced or copied for the performance of the service which are related to the contractual relationship and which are in its possession. Test and reject material shall be destroyed without delay in accordance with data protection regulations or handed over to the Client. This obligation shall apply to the same extent to any subcontractors engaged. This shall not affect data whose deletion is not possible for technical reasons or would cause a disproportionately high effort, as well as copies that are required to prove the correctness of data processing or to fulfil liability and warranty claims.

(2) The processing of such data shall be restricted in accordance with Art. 18 of the GDPR. The data may be stored by the Contractor in accordance with the respective retention periods beyond the end of the contract and must be securely deleted immediately after the retention period has expired. The Client shall be informed of the type and scope of this stored data upon request.

(3) Upon termination of this agreement, the Contractor shall confirm to the Client in writing the secure deletion or secure destruction of all records of the Client's data in its possession or the restriction of the processing of the Client's data pursuant to Article 18 of the GDPR.

§ 15 Term of contract, termination

(1) The term of the contract depends on the term of the service contract.

(2) The Client may terminate the agreement at any time without notice if there is a serious breach by the Contractor or a subcontractor of data protection regulations or of this agreement, if the Contractor or a subcontractor fails to comply with a lawful instruction of the Client, or if a Contractor or the subcontractor evades appropriate data protection control.

(3) The contract may only be terminated in writing.

§ 16 Effectiveness of the agreement

Should individual parts of this agreement be invalid, this shall not affect the validity of the rest of the agreement.

§ 17 Liability

The provisions of Art. 82 of the GDPR apply to liability.

§ 18 Names and contact details of the competent body at the Contractor

Competent body:
PitchYou GmbH, Campusallee 9, D-51379
Leverkusen, E-Mail: info@pitchyou.de

Data Protection Officer:
Sebastian Herting
Deputy: Philipp Lehmann
Herting Oberbeck Datenschutz GmbH
Hallerstraße 76
D-20146 Hamburg
https://www.datenschutzkanzlei.de
E-Mail: datenschutz@talentsconnect.com

§ 19 Applicable law and place of jurisdiction

(1) The applicable law and the place of jurisdiction shall be determined by the provisions of the respective service contract.

(2) Statutory regulations on exclusive competences shall remain unaffected.

____________________________ ____________________________

Date

____________________________ ____________________________

Signature of Client Signature of Contractor

Annex 1
Description of the agreed technical and organisational measures

The following technical and organisational measures are in place and are deemed to be agreed:

1. Access control:

The Contractor has established the following access controls that prevent data processing systems from being processed and used by unauthorised persons:

- Security lock for offices
- All data is stored on a server in a data centre of the company Hetzner (server location Germany).
- Local computers of our staff with the latest stable operating system version. All programs used are also kept up to date.
- All local computers are password protected. In addition, the hard disk is encrypted.
- Employees are allowed to work on projects outside the office. It is stipulated that no public Wi-Fi may be used.
- All employees are bound to data secrecy.

2. Data medium control:

Prevention of unauthorised reading, copying, modification or deletion of data media:

- Password procedure for all levels (local network, server, applications), among others, with special characters, minimum length.
- Automatic blocking in the event of multiple incorrect password entries
- Access to server only via SSH and certificate-based login.

3. Memory control:

Prevention of unauthorised entry of personal data as well as unauthorised knowledge, modification and deletion of stored personal data:

- Password procedure for all levels (local network, server, applications), among others, with special characters, minimum length.
- Automatic blocking in the event of multiple incorrect password entries
- Access to server only via SSH and certificate-based login

4. User control:

Prevention of the use of automated processing systems by means of data transmission equipment by unauthorised persons:

- Password procedure for all levels (local network, server, applications), among others, with special characters, minimum length.
- Automatic blocking in the event of multiple incorrect password entries
- Access to server only via SSH and certificate-based login

5. Access control:

Ensure that those authorised to use an automated processing system have access only to the personal data covered by their access authorisation.

- It is ensured that only the access rights required to fulfill the respective task are granted.
- The allocation and release of access rights is clearly documented so that it can be determined who has access to the data.
- The allocation process and access rights are regularly checked and confirmed. Access rights will be revoked immediately if they are no longer required.
- One person is responsible for all data, who decides who may have which access.
- Access rights are adjusted when the tasks in the business processes change.
- It is ensured in the applications that the assigned access rights are technically implemented.
- Unauthorized access is excluded in all environments that contain production data (including development, test, etc.).
- User authorizations for employees are assigned centrally and are exclusively personal
- User authorizations are only granted based on roles (when joining or changing positions): Development, Application Support, Infrastructure Support, Management.
- (Virtual) server computers are protected by 2-factor authentication. Access is limited via a central hardware firewall.
- External attack attempts are detected by installed tools (Prometheus and Grafana).

6. Transmission control:

Ensure that it is possible to verify and establish to which entities personal data has been or may be transmitted or made available by means of data transmission equipment.

- The data is secured during transport, storage, transmission and processing outside the protected area of the company using methods such as strong encryption and two-factor authentication (e.g. hard disk encryption).
- Information handling instructions are defined and employees are trained to prevent misuse of the data (e.g. certified disposal of paper and data carriers, choice of transmission methods).
- Cryptographic keys to protect the data are managed securely in an appropriate management system.

7. Transport control:

Ensure that the confidentiality and integrity of data are protected during the transmission of personal data and during the transport of data media:

- Electronic signature through SSL certificate
- Encryption / tunnel connection (VPN = Virtual Private Network)
- SSH

8. Recoverability:

Ensure that deployed systems can be restored in the event of a malfunction:

- A backup routine saves the data on an extra backup space of our provider (currently the company Hetzner - see Annex 2).

9. Reliability:

Ensure that all functions of the system are available and that any malfunctions that occur are reported:

- Service Desk regarding the error message

10. Data integrity:

Ensure that stored personal data cannot be damaged by system malfunctions:

- Extensive testing of productive commissioning of new IT systems
- A backup routine saves the data on an extra backup space of our provider (currently the company Hetzner - see Annex 2).

11. Order control:

Ensuring that personal data processed under contract can only be processed in accordance with the Client's instructions:

- Clear contract design
- Control of the execution of the contract

12. Availability control:

Ensure that personal data is protected against destruction or loss:

- A backup routine saves the data on an extra backup space of our provider (currently the company Hetzner - see Annex 2).
- Up-to-date virus protection / up-to-date firewall
- All data backups take place daily and can be restored within half a day.
- Backup data is physically separated from the data of ongoing operation

13. Separability:

Ensure that personal data collected for different purposes can be processed separately:

- The processing of data takes place on server systems which are separated by a system of various access controls and access rights (compare the regulations in sections 1. and 4. of these TOMs).
- The regulations for information security and data protection as well as the security measures are regularly checked for compliance and effectiveness.
- There is a system and software development policy that includes aspects of data protection.

14. Input control:

Creating, changing and deleting data through the software is only permitted under a user name. Usernames are always individual-personal. All data changes and deletions are logged under the relevant username. The authorization concept of the software only provides authorization for individuals (never for groups).

Annex 2
Subcontractors

Subcontractor name and address	Services	Data pricacy contact
Amazon Web Services EMEA SARL 28 Avenue John F. Kennedy L-1855 Luxemburg	Server, Cloud Hosting Only if AI component is used: Amazon Bedrock	aus-EU-privacy@amazon.com
360dialog GmbH Torstraße 61 D-10119 Berlin	Access provider to WhatsApp Business API	René Rautenberg +49 89 55294870 info@er-secure.de
Only if automatic translation is used: DeepL SE Maarweg 165 D-50825 Köln	Translation of messages	Dr. Christian Lenz +49 2261 81950 datenschutz@dhgp.de
Only if p78 SAP SuccessFactors connector is used: Projekt0708 GmbH Leopoldstraße 37 a D-80802 München	Transfer of applicant data to SAP SuccessFactors system of the client	Katja Hauser +49 40790 2350 datenschutz@projekt0708.com