Data Processing Agreement

between

(hereinafter the "Controller")

and

talentsconnect operations GmbH
Niehler Street 104
50733 Cologne
(**hereinafter** referred to as "Processor")

(hereinafter individually or collectively referred to as "**Party**" or "**Parties**")

1. Mandate and specifications for processing

1.1. This Data Processing Agreement (hereinafter referred to as the "**DPA**") sets out in detail the rights and obligations of the Parties under data protection law for all processing operations resulting from the contracts already existing between the Parties or to be concluded in the future (hereinafter referred to as the "**Main Contract**") under which personal data is processed by the Processor on behalf of the Controller. This DPA does not cover those Processings which take place within the Processor's own area of responsibility under the Main Contract. However, Annex 2 - Technical and Organisational Measures shall apply mutatis mutandis to data processing operations carried out under the Processor's own responsibility.

1.2. This DPA with all its components shall apply if the Controller has obligated the Processor to process personal data (hereinafter "**Data**") on behalf of the Controller pursuant to Article 28 GDPR. In this context, this DPA forms the framework for a large number of different data processing on behalf of.

1.3. In the event of any contradictions, the provisions of this DPA with all its components shall take precedence over the provisions of the associated main contract.

1.4. The specific data protection provisions applicable to individual processing operations (hereinafter "Provisions") shall be regulated in Annexes to the DPA (hereinafter "**Annexes**") prior to the start of processing. These are in particular the subject and duration as well as the type and purpose of the processing, the categories of data and

the categories of data subjects ("**Annex 1 - Specifications**") as well as the technical and organisational measures (hereinafter "**TOM**").

1.5. The Annexes are part of the DPA. In the event of any contradictions, the Annexes shall take precedence over the more general provisions of the DPA. Where reference is made to the DPA in the following or in the Annexes, the DPA with all its components is meant.

2. Responsibility and processing on instruction

2.1. Within the scope of this DPA, the Controller shall be solely responsible for compliance with the applicable legal provisions, in particular for the lawfulness of the disclosure to the Processor as well as for the lawfulness of the processing ("**Controller**" pursuant to Art. 4 No. 7 GDPR).

2.2. The Processor shall act exclusively in accordance with instructions with regard to the processing of the data, unless there is an exceptional case pursuant to Art. 28 (3) a GDPR (other statutory processing obligation). Verbal instructions must be confirmed in text form without delay. If the Controller acts as a data processor on behalf of a third party, the obligations of the Controller arising from this data processing on behalf of the third party shall apply directly as instructions of the Controller in relation to the Processor, insofar as these obligations should be stricter than those arising from this DPA. The Controller shall notify the Processor in text form of any such third-party requirements for data processing on behalf of.

2.3. The Processor shall correct or delete the contractual data or restrict their processing (hereinafter "**Blocking**") if the Controller instructs it to do so and this is otherwise covered by the scope of instructions.

2.4. The Processor shall inform the Controller without undue delay if it is of the opinion that an instruction violates applicable regulations on data protection or this DPA. The Processor may suspend the implementation of the instruction until it has been confirmed or amended by the Controller in text form. The Processor may refuse to carry out instructions that are obviously contrary to data protection law.

2.5. The Processor warrants that the persons authorised to process the Data (a) are aware of and comply with the Controller's instructions and (b) have undertaken to maintain confidentiality or are subject to an appropriate statutory duty of confidentiality. The duty of confidentiality and secrecy shall continue to apply after termination of the processing.

3. Safety of processing

3.1. The Parties agree on TOM pursuant to Article 32 of the GDPR for the adequate protection of data in an Annex to this DPA (hereinafter "**Annex 2 - Technical and Organisational Measures**").

3.2. The Processor reserves the right to change the TOM, but it must be ensured that the contractually agreed level of protection is not undercut. The Controller shall be notified of significant changes in text form as a new version of Annex 2 - Technical and Organisational Measures. Changes to the detriment of the Controller require its prior consent in text form.

4. Information in the event of data protection breaches and processing errors

4.1. The Processor shall inform the Controller without undue delay if it becomes aware of violations of the protection of the data entrusted to it by the Controller within the meaning of Art. 4 No. 12 GDPR in its organisational area or if there is a concrete suspicion of such a data protection violation at the Processor.

4.2. If the Controller discovers errors in the processing, he shall inform the Processor thereof without delay.

4.3. The Processor shall immediately take the necessary measures to remedy the data protection breach pursuant to 4.1 or the errors pursuant to 4.2 and to mitigate any possible adverse consequences, in particular for the data subjects. He shall coordinate this with the Controller. Verbal notifications shall be submitted in text form without delay.

5. Transfer of data to a recipient in a third country or in an international organisation

The transfer of data to a recipient in a third country outside the EU and EEA is permitted in compliance with the conditions set out in Art. 44 et seq. GDPR and with the prior consent of the Controller in text form. Details shall be regulated in one or more Annexes.

6. Subcontracting by the Processor

6.1. The Processor may have the processing of personal data performed in whole or in part by other processors (hereinafter "**subcontractors**").

6.2. Upon signing the DPA, the Processor shall use the subcontractors specified in "**Annex 3 - Subcontractors**". The Processor shall inform the Controller in text form in good time in advance about the commissioning of subcontractors or changes in the subcontracting. The Controller may object to the subcontracting in text form within four weeks of becoming aware of it if there is good cause. Good cause shall be deemed to exist in particular if there is reasonable cause to doubt that the subcontractor will provide the agreed service in accordance with the applicable statutory provisions on data protection or in accordance with these GTC.

6.3. The Processor shall agree with the subcontractor on the same content of the provisions made in this DPA. In particular, the TOM to be agreed with the subcontractor must provide an equivalent level of protection.

6.4. Subcontracting within the meaning of this provision does not include services which the Processor uses purely as an ancillary service to support its business activities outside the scope of data processing on behalf of. However, the Processor is obliged to take appropriate precautions to ensure the protection of the data also for such ancillary services.

7. Rights of data subjects and assistance to the Controller

If a data subject asserts claims under Chapter III of the GDPR against one of the Parties, it shall inform the other party thereof without undue delay. The Processor shall support the Controller within the scope of its possibilities in processing such claims as well as in complying with the obligations set out in Art. 33 to 36 GDPR.

8. Control and information rights of the Controller

8.1. The Processor shall demonstrate to the Controller compliance with its obligations by appropriate means. The Controller shall verify the suitability.

8.2. For compliance with the agreed protective measures and their verified effectiveness, the Processor may refer to appropriate certifications or other suitable audit evidence. Appropriate are in particular certifications according to Art. 40 GDPR or evidence according to Art. 42 GDPR. In addition, the following may be considered, among others: certification in accordance with ISO 27001 or ISO 27017, ISO 27001 certification based on IT-Grundschutz, certification in accordance with recognised and suitable industry standards or proof of audit in accordance with SOC / PS 951. The certification and audit procedures shall be carried out by a recognised independent third party. The Processor shall provide its certificates or audit evidence. Further suitable means (e.g. activity reports of the data protection officer or excerpts from reports of the auditors) may be made available to the Controller as evidence of compliance with the agreed protective measures. The Controller's right of inspection under Section 8.3 remains unaffected by this.

8.3. The Controller shall be entitled to carry out inspections at the Processor's premises during normal business hours without disrupting operations, regularly after prior notification and taking into account a reasonable lead time, in order to check compliance with the provisions of data protection law. The Processor may make the inspection dependent on the signing of a confidentiality agreement regarding the data of other Controllers and the TOM taken by him.

8.4. To remedy the findings made during an inspection, the Parties shall agree on the measures to be implemented.

8.5. If a supervisory authority makes use of powers pursuant to Art. 58 GDPR, the Parties shall inform each other thereof without undue delay. They shall support each other in their respective areas of responsibility in fulfilling their obligations vis-à-vis the respective supervisory authority.

9. Liability and compensation

9.1. If a data subject asserts a claim for damages against a party due to a breach of data protection provisions, the claimed party shall inform the other party thereof without undue delay.

9.2. The Controller and Processor shall be liable vis-à-vis data subjects in accordance with the provision set out in Article 82 of the GDPR.

9.3. The Parties shall support each other in the defence of claims for damages by affected persons, unless this would jeopardise the legal position of one party in relation to the other party, the supervisory authority or third parties.

10. Term

10.1. The DPA is concluded for an indefinite period. The term of an Annex shall be regulated in the respective Annex; in the absence of such a regulation, the Annex shall run for an indefinite period.

10.2. The DPA may be terminated with three (3) months' notice to the end of a quarter if all Annexes have been terminated simultaneously or previously.

10.3. An Annex expires with the termination of the associated Main Contract without the need for a separate termination of this Annex. In this case, the Processor shall, at the discretion of the Controller, immediately surrender the data processed in accordance with the system or delete it in accordance with data protection and confirm this to the Controller in text form. If the Processor has its own legal obligation to store this Data, it shall notify the Controller of this in text form.

11. Costs

Each Party shall bear its own costs incurred in connection with this DPA.

12. Final provisions

12.1. Should the Controller's data be endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller thereof in text form without delay. The Processor shall immediately inform all persons responsible in this context that the responsibility for the data lies exclusively with the Controller.

12.2. No verbal ancillary agreements have been made. Amendments, supplements or termination of this contract must be made in text form to be effective. This also applies to an amendment of this formal clause. Deviating verbal agreements of the Parties are invalid.

12.3. Should one of the provisions be or become legally ineffective or void in whole or in part, or should it contain a loophole not considered by the Parties at the time of conclusion, this shall not affect the effectiveness of the remaining provisions. In place of the legally ineffective, void or missing provision, the law shall apply, unless the resulting gap can be closed by supplementary interpretation of the contract in accordance with §§ 133, 157 BGB. However, both Parties are obliged to enter into negotiations without delay with the aim of reaching an agreement in place of the legally ineffective, void or missing provision that comes closest to its meaning and purpose in legal and economic terms.

12.4. The law of the Federal Republic of Germany shall apply exclusively to the services rendered and other acts performed by the Parties hereunder, to the exclusion of the UN Convention on Contracts for the International Sale of Goods and the conflict of laws provisions; Art. 3 para. 3, para. 4 of the Rome I Regulation shall remain unaffected.

Signatures:

,	Cologne,
_____	_____
	John Shiles
	CPO
Controller	talentsconnect AG

Attachments:

- Annex 1 - Specifications
- Annex 2 - Technical and organisational measures
- Annex 3 - Subcontractors
- Annex 4 - Contact details

Annex 1

Specifications

The Parties shall make the following additional stipulations to the contract on data processing on behalf of:

1. Subject and purpose of data processing

The object of the processing is the transmission of the applicants' application data via the Fast Application to the client's application management system. The applications are temporarily stored on the talentsconnect servers. In the case of an application via WhatsApp, applications are sent from the WhatsApp Business API to the client's application management system. The processing of the client's employee data in the Recruiting Home is also the subject of order processing. The purpose of the data processing is to provide the Fast Application and Recruiting Home services.

2. Categories of persons concerned

a. Applicants, interested parties
b. In the context of the Recruiter Cockpit: operational users/employees

3. Categories of personal data

- Master data (name, address, contact details incl. e-mail)
- Interests, communication data
- Application data (curriculum vitae, references, preferences, photograph, etc.)
- In the context of the Recruiter Cockpit: user/employee data (access data)

talents connect

Enclosure 2

Technical and organisational measures

talents connect

Enclosure 3

Subcontractor

The Contractor uses the following subcontractors at the time of conclusion of the DPA and has implemented the protective measures described below in the case of third country transfers:

Name of the subcontractor	Address	Purpose of the processing	Place of processing	Safeguard measures in the case of third country transfers	Further protective measures to safeguard data transmission
Dembach Goo Informatik GmbH & Co KG	Hohenzollernring 72, 50672 Cologne, Germany	Server	Germany For server locations, see Appendix 2 (TOMs): DUS1, DUS5 and FAL		
Google Ireland Ltd - Workspace	Gordon House Barrow Street Dublin 4 Ireland	Provision of an e-mail server infrastructure for customer communication in the event of a support case	EU	EU standard contractual clauses ((EU) 2021/915, 4.6.2021, Module 2)	**Encryption** All data is encrypted during transmission (*data in transit*) and at *rest* (*data at rest).* *Data in transit* encryption: Google enforces encryption in transit by default, using FIPS 140-2 validated cryptographic modules to encrypt all traffic between regions. Google's Application Layer Transport Security (ALTS) is a mutual authentication and transport encryption system developed by Google and used to secure Remote Procedure Call (RPC) communications within the Google infrastructure. ALTS is similar in concept to TLS with mutual authentication,

					but was developed and optimized for the requirements of Google's data center environments. *Data at rest* encryption: When storing data at rest, Google applies AES256 encryption at the storage level by default When storing data at rest, Google applies AES256 encryption at the storage level by default.
Amplitude, Inc.	201 3rd Street, Suite 200, San Francisco, CA 94103	Web Analysis	EU	EU standard contractual clauses ((EU) 2021/915, 4.6.2021, Module 2)	**Encryption**: Amplitude maintains a secure environment for the transmission of its Controllers' personal data, Encryption that complies with industry standards, such as the Federal Information Processing Standards FIPS 140-2 and/or NIST SP800-52 and using industry standard Encryption technologies such as server certificate-based authentication within Amplitude Environment. Amplitude maintains a secure environment for the storage of its Controllers' personal data, Encryption that complies with industry standards, such as the Federal Information Processing Standards FIPS 140-2 and/or NIST SP800-52 and data at rest with AES-256.

MailJet (Global HQ)	13-13 bis, rue de l'Aubrac, 75012 Paris, France	Transactional emails	EU		
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxemburg	Server, Hosting	EU	EU standard contractual clauses ((EU) 2021/915, 4.6.2021, modules 2)	AWS holds a large number of internationally recognized certifications and accreditations. Compliance is ensured with strict standards such as ISO 27017 for cloud security, ISO 27701 for data protection management and ISO 27018 for cloud data protection guaranteed. Encryption: data is is encrypted during transportation and during storage in the cloud according to the state of the art (AES-256, FIPS 140/2) with an encryption a key managed by talentsconnect managed key encrypted before they reach AWS servers.
KeyCDN - proinity LLC	Reichenauweg 1, 8272 Ermatingen, Schweiz	Content Delivery Network, Provision of media content	EU		We have checked with the provider the distribution of the content to servers within the EU restricted. There are extensive security measures are taken, such as TLS encryption, DDoS protection.
PitchYou GmbH	Campusallee 9, D-51379 Leverkusen	Technical implementation and processing of the application via WhatsApp via the WhatsApp Business API, if this	Germany		

		function is integrated and used by the applicant on the basis of consent.			
Canny Inc	800 N King Street Suite 304 1121Wilmington, DE 19801 United States	Canny.io is an application that enables feedback within Recruiting Home for Employees.	USA	EU Standard Contractual Clauses ((EU) 2021/915, 4.6.2021, Module 2)	Canny is SOC 2 certified. All hosting servers are only accessible via encrypted connections - HTTPS with RSA-2048-bit keys.
Service provider for applications: at the client's discretion					
Kombo Technologies GmbH	Lohmühlenstraße 65 12435 Berlin, Deutschland	Integration and operation of the interface between the Fast Application and the client's applicant management system	EU		Kombo Technologies GmbH is certified according to ISO 27001. Further information on technical and organizational security measures: security.kombo.dev. Encryption-at-rest: AES-256 encryption Encryption-in-transit: All outgoing data traffic uses the highest TLS version available in the API of the respective integration. All all incoming traffic via the Combo API is mandatory with TLS 1.3 is mandatory.
Chat tools: at the Controller's discretion					
Option 1: Userlike UG (limited liability)	Probsteigasse 44-46, 50670 Cologne, Germany	Chat	Germany		

Enclosure 4

Contact details

1. Persons authorized to issue instructions

1.1. Controller

Name, title:

Email:

1.2. Processor

Name, Title: Andreas Buchholz,Managing Director Technology

CISO

Email: andreas.buchholz@talentsconnect.com

Telephone number: +49 (0)221 82 00 69 - 0

2. Data Protection Officer

2.1. Controller

Name, title:

Email:

2.2. Processor

Mr. Sebastian Herting, Herting Oberbeck Rechtsanwälte Partnerschaft, Hallerstraße 76, 20146 Hamburg, Germany

Email: herting@datenschutzkanzlei.de

Telephone number: +49 (0) 40 228 691 140