DATA PROTECTION AGREEMENT

PURSUANT TO

ART. 28 OF THE EU GENERAL DATA PROTECTION REGULATION

entered into by and between

firstbird GmbH
Hietzinger Hauptstrasse 34
1130 Vienna, Austria

– hereinafter referred to as “Firstbird” (Contractor) –

and

XXXXX

– hereinafter referred to as "Customer" –

Recitals

This Data Protection Agreement governs the protection of personal data (hereinafter “Data”) in order data processing. In this context, a controller (principal) instructs another party (contractor) to process data. In such case, a written order data processing agreement pursuant to Art. 28 of the EU General Data Protection Regulation (hereinafter "GDPR") shall be entered into. Pursuant to the definition in Art. 4 Nr. 2 GDPR, data processing is not only the collection, recording, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, erasure or destruction of data but also the act of making such data available for viewing or retrieval by third parties.

This Data Protection Agreement specifies the obligations of Firstbird and the Customer (hereinafter also referred to as the “Parties”) in respect of data protection as they arise from the order data processing described in detail in the Master Agreement (defined as the General Terms and Conditions of Business of firstbird GmbH and potentially further terms and conditions governing chargeable packages ordered). It is applied to any and all activities which are connected with the Master Agreement and in the course of which employees of Firstbird or subcontractors process data relating to the Customer.

The responsibility for data processing in conformity with data protection rules remains with the Customer as the principal of Firstbird. Pursuant to Art. 29 GDPR Firstbird as the Customer’s contractor may only process the data according to Customer’s instructions. In the event that Firstbird infringes this principle by e.g. determining the purposes of processing, Firstbird shall be considered a controller vis-à-vis the data subjects as set forth in Art. 28 par. 10 GDPR.

For this reason, the Parties have agreed as follows:

Clause 1 Subject Matter, Term and Specification of Order Data Processing

(1) The subject matter as well as the scope and type of data collection, processing or use are stated in the Master Agreement. Order content, data and persons concerned by data collection, processing or use (data subjects) are specified in Schedule 1 of this Data Protection Agreement ("Specification of order data processing").

(2) The term of this Data Protection Agreement is based on the term of the Master Agreement.

(3) In the event of data transfer to an unsafe third country, such transfer will be designed in a permissible manner using the legal possibilities approved by the EU Commission.

Clause 2 Customer’s Responsibility and Authority to give Instructions

(1) Pursuant to the Master Agreement the Customer has access to a platform for the recruitment of employees made available as ‘software-as-a-service’ (hereinafter referred to as the “Firstbird Platform”). Such access shall comprise any and all activities specified in the Master Agreement. Under the Master Agreement the Customer will be responsible for adherence to the legal requirements of data protection legislation, including, without being limited to, the lawfulness of data transmission to

Firstbird and the lawfulness of data processing (as a “Data Controller“ within the meaning of Art. 28 par. 1 GDPR).

(2) Firstbird will use the data processed on behalf of the Customer for no other purpose and shall in particular not be entitled to transfer such data to third parties. No copies or duplicates shall be made without the Customer knowing. Back-up copies shall be exempted from this provision to the extent that these are needed for proper data processing; the same shall apply to data required to comply with statutory retention obligations.

(3) Customer’s instructions to Firstbird regarding data processing (hereinafter “Processing Instructions”) will be defined in more detail in the Master Agreement and given via the Firstbird Platform or by e-mail to the persons entitled to receive instructions (see Clause 2 par. 5). Customer shall not be entitled to give additional Processing Instructions unless Firstbird is able to carry out such Instructions without unreasonable effort and Customer pays a fee subject to the Firstbird price list applicable at the time.

(4) Customer shall confirm verbal instructions in writing or by e-mail (in the form of text) without delay.

(5) Customer shall designate persons entitled to give instructions. Persons entitled to give instructions at Customer’s end will be documented in Schedule 1 hereto. In the event that the persons entitled to give instructions at Customer’s end change, this will be communicated in writing and recorded in Schedule 1.

(6) Firstbird shall designate to the Customer persons entitled to receive instructions from Customer. Persons entitled to receive instructions at Firstbird’s end will be documented in Schedule 1 hereto.

(7) Firstbird shall immediately inform the Customer pursuant to Art. 28 par. 3 sentence 3 GDPR if Firstbird believes that an instruction infringes data protection provisions. Firstbird shall be entitled to suspend the execution of the related instruction until it has been confirmed or changed by the controller of data at the principal’s end.

Clause 3 Obligations of Firstbird

(1) Firstbird will only collect, process and use the data of data subjects within the framework of the order and based on the Processing Instructions given by the Customer subject to Clause 2 par. 1 of this Order Data Processing Agreement unless Firstbird is obliged to use a different type of processing under EU legislation or the legislation of the Member State which Firstbird is subject to (e.g. due to investigations of criminal prosecution or national security agencies); in such case Firstbird will inform the Data Controller about such legal requirements prior to processing unless such communication is prohibited under that law prohibits on important grounds of public interest (Art. 28 par. 3 sentence 2 lit. a GDPR).

(2) Firstbird commits itself to confidentiality when processing Customer’s data in accordance with the processing order. Confidentiality shall survive the termination of the Master Agreement. Firstbird warrants that it has familiarised the employees in charge of providing the services stated in the Master Agreement with the relevant rules on data protection and committed these to confidentiality for the term of their employment and beyond in an appropriate manner (Art. 28 par. 3 sentence 2 lit. b and Art. 29 GDPR). Employees will be instructed about the special data protection obligations arising from this order and the binding effect of instructions and processing purpose. Firstbird will supervise compliance with data protection rules in its operations.

(3) Firstbird will manage intra-company organisation in such a way that it fulfils the special requirements of data protection. Firstbird will take technical and organisational measures for the appropriate protection of Customer data which comply with the requirements of Art. 32 GDPR (see Art. 28 par. 3 sentence 2 lit. c GDPR). In total, the measures to be taken will be measures to ensure data security and a risk-adequate level of protection in respect of confidentiality, integrity, availability and system robustness. in this context, the state of the art, the costs of implementation and the type, scope and purposes of data processing as well as various probabilities of occurrence and seriousness of risk for the rights and freedoms of natural persons within the meaning of Art. 32 par. 1 GDPR will be taken into account. These measures are described in more detail in Schedule 2 to this Data Protection Agreement ("Technical and Organisational Measures"). Customer is aware of the fact that such measures are subject to technical progress and developments. Firstbird shall therefore be entitled to implement alternative measures. However, in doing so, Firstbird will ensure that the level of protection contractually agreed upon will not be compromised.

(4) Firstbird undertakes to support the Customer in complying with the obligations stated in Art. 32 to 36 GDPR (data security measures, reporting infringements of the protection of personal data to the supervisory authority, notification of the person affected by an infringement of the protection of personal data, data protection impact assessments, prior consultation) (see Art. 28 par. 3 sentence 2 lit. f GDPR). Details of the reporting duties of Firstbird in the event of processing disruptions and infringements of the protection of personal data shall be subject to Clause 4 of this Agreement.

(5) Firstbird undertakes to inform the Customer without delay of any checks and measures of the supervisory authority to the extent that these relate to the order. This will also apply to investigations of a relevant authority under Art. 83, 84 GDPR at Firstbird's end.

Clause 4 Notification Obligations in the Event of Disruptions in processing and Infringements of the Protection of personal Data

(Art. 28 par. 3 sentence 2 lit. f GDPR)

Firstbird will notify Customer immediately of any infringements, by itself or by persons it employs, of data protection rules or the stipulations of the Master Agreement or suspected cases of data protection infringements or irregularities in data processing (e.g. data loss or unlawful transmission or cognizance of data, serious disruptions in operations suspected cases of other infringements of rules for the protection of personal data or other irregularities in the handling of Customer data). This shall include, without being limited to, Customer's notification and reporting duties pursuant to Art. 33 and Art. 34 GDPR. Firstbird warrants that, if necessary, it will provide to Customer reasonable assistance in the fulfilment of Customer's duties under Art. 33 and 34 GDPR (Art. 28 par. 3 sentence 2 lit. f GDPR). Firstbird may only send notifications pursuant to Art. 33 or 34 GDPR on behalf of the Customer if given prior instructions to do so pursuant to Clause 3 par. 1 of this Agreement.

Clause 5 Requests by Data Subject

(Art. 28 par. 3 sentence 2 lit. e GDPR)

(1) Firstbird undertakes to take any and all technical and organisational measures to ensure that Customer will be able to comply with the rights of data subjects under Chapter III of the GDPR (information, communication, rectification and erasure, data portability, right to object and automated individual decision-making) at any time within the statutory periods (see Art. 28 par. 3 sentence 2 lit. e GDPR). This shall be subject to the prerequisites that (a) Customer has given Firstbird written instructions to do so, (b) such assistance does not result in a breach of Firstbird's non-disclosure obligations vis-à-vis third parties and (c) Customer reimburses Firstbird for the expenses arising from such assistance. Firstbird will not answer any requests for information and will refer the data subject to Customer. Firstbird will provide Customer with any and all information required for this purpose.

(2) Firstbird will only rectify, erase or block the data forming the subject matter hereof upon Customer's instructions. If a data subject contacts Firstbird directly requesting erasure of his/her data, Firstbird will communicate such request to Customer without delay.

Clause 6 Customer's auditing Right

(Art. 28 par. 3 sentence 2 lit. h GDPR)

(1) Customer may (at his own expense, and maintaining the secrecy of all information) upon consultation with Firstbird carry out order audits or have these carried out by a competent third party, provided that the latter is not in competition with Firstbird and Firstbird does not raise any legitimate objections against him. Customer may after timely announcement carry out random audits in the business operations of Firstbird to verify the latter's compliance with the Agreement, during regular business hours and without disrupting the operations of Firstbird.

(2) Firstbird undertakes to make available to Customer upon written request and within an appropriate period all information and the corresponding evidence required to carry out an audit. It is agreed that audits by Customer are limited to one day per calendar year. Any derogations from the above must be coordinated by the Parties and agreed in writing.

Clause 7 Subcontractors

(Art. 28 par. 3 sentence 2 lit. d GDPR)

(1) Customer agrees to Firstbird using the services of subcontractors. The subcontractors already engaged at the time when this Agreement is entered into are listed in Schedule 3 ("Subcontractors").

(2) Firstbird will inform Customer without delay of any intended change in respect of new subcontractors or the replacement of previous subcontractors so that Customer will be able to object to such changes (Clause 28 par. 2 sentence 2 GDPR). Such objection may only be raised for good cause (e.g. intended use of Customer's competitor or a subcontractor known to have previously infringed data protection rules). If Customer does not object to an intended change within the meaning of the above within two weeks, consent shall be deemed given.

(3) If no agreement is reached in respect of new subcontractors or the replacement of previous subcontractors, Contractor shall have a special termination right within 14 days by giving 4 weeks' notice prior to the end of the quarter.

(4) Firstbird will carefully select subcontractors whilst particularly considering the suitability of their technical and organisational measures within the meaning of Art. 32 GDPR.

(5) Each of these subcontractors will only be allowed to process Customer data only to support Firstbird in rendering the services under the Master Agreement. Firstbird has sourced the performance of such services to subcontractors and prohibited them to use such data for other purposes. Firstbird will remain responsible for compliance with the obligations related to data processing by subcontractors.

(6) Any and all subcontractors which Firstbird permits to process data have entered into a data protection agreement with Firstbird whereby the subcontractors are bound to the same data protection obligations as those defined for the relationship between Firstbird and the Customer. In particular, these agreements ensure that the technical and organisational measures taken by subcontractors are no less strict than those described in Schedule 2 of this Data Protection Agreement. Customer shall be entitled to receive from Firstbird, upon written request, information about the material content of the agreements as well as about compliance with the obligations relevant for data protection in subcontracting relationships; if required, Customer shall be entitled to inspect the related contractual documentation.

(7) Services which Contractor outsources to third parties as ancillary services in support of the execution of the order shall not be deemed to qualify as subcontracting. Amongst other things, this includes cleaning services, pure telecommunications services which are not specifically related to services rendered to the Principal by the Contractor, postal and courier services, transport services, security guard services. However, the Contractor is also obliged to ensure that reasonable precautions as well as technical and organisational measures are taken to protect personal data when such ancillary services by third parties are concerned. The maintenance and inspection of IT systems shall be deemed subcontracting relationships which require Customer's consent to the extent that these concern IT systems required to render services to the Principal.

Clause 8 Obligations of Firstbird after completion of the Order

(Art. 28 par. 3 sentence 2 lit. g GDPR)

(1) After completion of the contractually agreed service or at Customer's request, whichever is earlier – but no later than at termination of this Agreement – Firstbird will hand over to the Customer any and all documents it has obtained, results of processing and use it has produced and data related to the order or erase these in accordance with data protection requirements subject to Customer's prior consent (see Art. 28 par. 3 sentence 2 lit. g GDPR). The same shall apply to testing and reject material. The erasure log will be submitted to Customer at request. Data and copies which need to be retained for the purpose of fulfilling liability and warranty claims shall not be affected.

(2) Firstbird will retain documentation serving in evidence of proper order fulfilment and due data processing past the termination of the Agreement in accordance with relevant statutory retention

periods. Firstbird may hand such documentation over to Customer at the end of the Agreement in discharge from such obligation.

(3) In the event that Customer's data held by Firstbird are jeopardised by garnishment or confiscation, insolvency or composition proceedings or measures of third parties, Firstbird will inform Customer thereof without delay. Firstbird will inform any and all persons responsible in this context that data sovereignty and data ownership lie exclusively with the Customer.

Clause 9 Anonymisation and aggregation of Data

(1) Firstbird may anonymise and aggregate the personal data covered by this Data Protection Agreement and carry out the processing steps required for the anonymisation and aggregation. While ensuring anonymity, Firstbird may therefore process and use all the data created in this manner for its own purposes, such as statistical evaluations, sectoral comparisons, benchmarking, product improvements, new product developments, and other similar purposes.

(2) The original dataset is not affected by anonymisation.

(3) Anonymised or aggregated data within the meaning of section 9 (1) are no longer considered personal data and do not fall under the obligation to hand over or erase data as defined in section 8 (1). Firstbird shall be entitled to use and keep such data past the termination of the Agreement.

Clause 10 Data Protection Officer and Obligations to furnish Evidence

(1) Firstbird has appointed an external data protection officer who is acting in accordance with Art. 38 und 39 GDPR. The data protection officer in charge is Marco Tessendorf of procado Consulting, IT- & Medienservice GmbH, Warschauer Str. 58a, 10243 Berlin, who can be reached at data-security@firstbird.com.

(2) At Customer's request, Firstbird will furnish evidence of compliance with the obligations set forth in this Agreement; such evidence shall be provided with appropriate means, such as a self-audit by the data protection officer.

Clause 11 Final Provisions

(1) Amendments and additions to this order Data Protection Agreement and all of its parts – including any covenants of Firstbird – shall be done in writing to be valid and shall contain the express indication that it is an amendment or additional to the provisions of this Data Protection Agreement. This shall also apply to any waiver of the written form.

(2) In the event that a provision of this Data Protection Agreement is or becomes ineffective or unenforceable, the remainder of the Agreement shall be unaffected. Instead of the ineffective or void provision, a provision which is legally permitted and as close as possible to the purpose of the

Agreement and the intentions of both Parties shall be agreed upon. The same shall apply to any lacunae in the Agreement as may be identified.

(3) In any and all disputes under or in connection with this Agreement, the provision of the Master Agreement governing jurisdiction and forum shall apply to the extent that this is permissible.

(4) The Schedules to this Data Protection Agreement shall be deemed an integral and essential part thereof.

Firstbird	**Customer**
Place, date	Place, date
Signature	Signature
Name	Name
Title	Title

Schedule 1: Specification of Order Processing
Schedule 2: Technical and Organisational Measures
Schedule 3: Subcontractors

- Schedule 1 -

Specification of Order Processing

1. Subject Matter

The subject matter of the order corresponds to the services described in the Master Agreement.

2. Scope, Type and Purpose of Processing

The scope, type and purpose of personal data processing by Firstbird on behalf of the Customer are as follows:

Data subject category	Data category	Type of processing	Purpose of data collection, processing or use
Applicant	Master data: 1. First name and last name 2. E-mail address 3. Application photo* 4. Phone number 5. Application documents** 6. Link to public profile on LinkedIn or Xing* *Not obligatory. **May be set to “obligatory” by the respective company.	1. Collect (1.-6.) 2. Store (1.-6.) 3. Use (1.-6.) 4. Transfer* (1.-6.) *Depending on whether and which type of interface was booked to the customer's BMS.	Performance of the services ordered in accordance with the service agreement via the Firstbird platform
	Feedback data: ● Message (text) from Talent Scout and ● rating (1-3 stars) by Recruiter/Company Administrator	1. Collect 2. Store 3. Use 4. Transfer* *Depending on whether and which type of interface was booked to the customer's BMS.	History tracking and information flow regarding status and assessment of recommendations
	IP address	1. Store 2. Anonymise	For security and optimisation reasons, the anonymised IP address is stored so as to be able to limit fraud and to ensure

			performant access to Firstbird worldwide.
	Support queries (by e-mail): ● First name and last name ● E-mail address ● Message	1. Collect 2. Store 3. Use	Support to users in the event of technical problems or questions about the use of Firstbird

Talent Scouts	Master Data: 1. First name and last name 2. E-mail address 3. Profile photo* 4. Application language 5. Location 6. Area of expertise 7. Employee ID* 8. Time zone 9. Linked social networks* *Not obligatory.	1. Collect (1.-9.) 2. Store (1.-9.) 3. Use (1.-9.) 4. Transfer* (only 1.) *Depending on whether and which type of interface was booked to the customer's BMS.	Performance of the services ordered in accordance with the service agreement via the Firstbird platform
	Feedback message (text) on direct recommendation or application	1. Collect 2. Store 3. Use 4. Transfer* *Depending on whether and which type of interface was booked to the customer's BMS.	History tracking and information flow regarding status and assessment of recommendations
	Individual use data and success statistics (number of jobs shared, number of recommendations, number of persons hired etc.)	1. Collect 2. Store 3. Use	Personal statistics and tracking, bonus payments
	Support queries (by e-mail or via the Help widget of the Firstbird account): ● First name and last name ● E-mail address ● User role (Talent Scout) ● Message	1. Collect 2. Store 3. Use	Support to users in the event of technical problems or questions about the use of Firstbird

Recruiter	Master Data: 1. First name and last name 2. E-mail address 3. Profile photo* 4. Application language 5. Location 6. Area of expertise 7. Employee ID* 8. Time zone 9. Linked social networks* *Not obligatory.	1. Collect (1.-9.) 2. Store (1.-9.) 3. Use (1.-9.) 4. Transfer* (only 1. and 2.) *Depending on whether and which type of interface was booked to the customer's BMS.	Performance of the services ordered in accordance with the service agreement via the Firstbird platform
	● Feedback (text message) by Talent Scout on direct recommendation or application ● Assessment data (1-3 stars) related to direct recommendation or application ● Feedback (text message) to a Talent Scout on a recruitment ● Feedback (text message) to a Talent Scout on closing a recommendation or recruitment ● Feedback (text message) to a Talent Scout in respect of bonus managements	1. Collect (1.-5.) 2. Store (1.-5.) 3. Use (1.-5.) 4. Transfer* (only 3.-5.) *Depending on whether and which type of interface was booked to the customer's BMS.	History tracking and information flow regarding status and assessment of recommendations
	Individual use data and success statistics (number of jobs shared, number of recommendations, number of persons hired etc.)	1. Collect 2. Store 3. Use	Personal statistics and tracking, bonus payments
	IP address	1. Store 2. Anonymise	For security and optimisation reasons, the anonymised IP address is stored so as to be able to limit unauthorised access and to ensure performant access to Firstbird worldwide.
	Support queries: ● First name and last name ● E-mail address ● User role (Recruiter) ● Message	1. Collect 2. Store 3. Use	Support to users in the event of technical problems or questions about the use of Firstbird

	Feature queries: ● First name and last name ● E-mail address ● User role (Recruiter) ● Name and address of company ● Company website ● Feature suggestion (message)	1. Collect 2. Store 3. Use	Optimisation of the Firstbird platform

Company Administrators	Master Data: 1. First name and last name 2. E-mail address 3. Profile photo* 4. Application language 5. Location 6. Area of expertise 7. Employee ID* 8. Time zone 9. Linked social networks* *Not obligatory.	1. Collect (1.-9.) 2. Store (1.-9.) 3. Use (1.-9.) 4. Transfer* (only 1. and 2.) *Depending on whether and which type of interface was booked to the customer's BMS.	Performance of the services ordered in accordance with the service agreement via the Firstbird platform
	1. Feedback (text message) by Talent Scout on direct recommendation or application 2. Assessment data (1-3 stars) related to direct recommendation or application 3. Feedback (text message) to a Talent Scout on a recruitment 4. Feedback (text message) to a Talent Scout on closing a recommendation or recruitment 5. Feedback (text message) to a Talent Scout in respect of bonus managements	1. Collect (1.-5.) 2. Store (1.-5.) 3. Use (1.-5.) 4. Transfer* (only 3.-5.) *Depending on whether and which type of interface was booked to the customer's BMS.	History tracking and information flow regarding status and assessment of recommendations
	Individual use data and success statistics (number of jobs shared, number of recommendations, number of persons hired etc.)	1. Collect 2. Store 3. Use	Personal statistics and tracking, bonus payments
	IP address	1. Store 2. Anonymise	For security and optimisation reasons, the anonymised IP

			address is stored so as to be able to limit unauthorised access and to ensure performant access to Firstbird worldwide.
	Support queries: ● First name and last name ● E-mail address ● User role (Company Administrator) ● Message	1. Collect 2. Store 3. Use	Support to users in the event of technical problems or questions about the use of Firstbird

3. Terms of Order

The term of the order corresponds to the term of the Master Agreement.

4. Persons entitled to give Instructions

Persons who are registered as Administrators in the Customer's company account are entitled to give instructions to Firstbird.

5. Persons taking Instructions at Firstbird's end

Firstbird designates the following persons who are entitled to take instructions from Customer:

- Daniel Winter, CTO (daniel.winter@firstbird.com)
- Matthias Wolf, COO & Co Founder (matthias.wolf@firstbird.com)
- Monika Adensamer, Data Security (data-security@firstbird.com)
- All employees of the Customer Success team

- Schedule 2 -

Technical and organisational Measures

The technical and organisational measures pursuant to Art. 32 GDPR described in this Schedule 2 are agreed upon between Customer and Firstbird with binding effect.

The agreement on technical and organisational measures is an integral part of the Data Protection Agreement for Order Data pursuant to Art. 28 GDPR.

1. Confidentiality

a) Access Control / Premises

The measures described below are suited to prevent unauthorised persons from accessing data processing facilities where personal data are processed or used.

The office premises of Firstbird are located in an office building in Vienna, Austria. The office building houses the offices of several companies. The building entrance is a self-closing door which is locked at all times. The landlord is in charge of key management for the office building entrance. The keys issued by the landlord are allocated to the respective tenants. Firstbird itself is in charge of managing the entrance door keys Firstbird has been allocated.

The intra-company process for issuing keys is based on the dual control principle. Keys are only issued to employees (not to self-employed persons) and related records are maintained. Employees are obliged to notify Firstbird without delay in the event of key loss and to file a loss report.

Moreover, a process is in place for employees leaving the company; this process includes the return of keys and other Firstbird property by the employee leaving the company.

Firstbird data which are subject to order processing are exclusively stored at the AWS Computer Centre of Amazon in Frankfurt. Amazon fulfils the following security and compliance standards:

- Certified under ISO 27001/9001
- Certified under ISO 27017/27018
- Cloud Computing Compliance Control Catalog (C5 Reference standard of the BSI)

For further details please visit https://aws.amazon.com/de/compliance.

The following access control measures have been taken at the computer centre:

- The AWS computer centre and the systems used there are located in inconspicuous buildings which cannot readily be identified as a computer centre from the outside.
- The computer centre itself is protected by physical security measures to prevent unauthorised access through perimeter control (e.g. fence, walls) as well as access controls within the buildings.
- Access to the computer centre is managed by electronic access controls and safeguarded by alarm systems; the alarm is sounded as soon as a door is forced open or held open.
- Access authorisation is approved by an authorised person and revoked within 24 hours from the deactivation of an employee or supplier data set.
- All visitors have to show an ID and register upon arrival and will at all times be accompanied by authorised employees.
- Access to sensitive areas is monitored by CCTV.
- The AWS computer centre and its immediate surroundings are guarded by trained security guards 24/7.

b) Access Control / Data Processing Systems

The measures described below are suited to prevent unauthorised persons from accessing data processing systems.

Users have to follow an authentication process to access each IT system used by Firstbird. This requires a user name and password.

Firstbird issues authorisations to use IT systems or applications according to the dual control principle. Hence, it is mandatory for supervisors to apply for authorisation with the IT Administration on behalf of their employees. Supervisors are obliged to only apply for those authorisations which are absolutely necessary for employees so they can fulfil the tasks assigned to them. Authorisations shall be restricted to the minimum.

IT Administration will keep a record of authorisations issued (and revoked) in the system. In consultation with supervisors, IT Administration will check on a quarterly basis if the authorisations issued are still required. Moreover, supervisors are obliged to apply to IT Administration for a correction of authorisations if and when employees' assignments change.

In the event that employees leave the company, persons in charge of HR will inform IT Administration of impending changes without delay so IT Administration can revoke related authorisations. Authorisations have to be revoked within 24 hours from an employee leaving the company.

Where initial passwords are issued, the procedure in Firstbird is that the initial password must be changed upon first log-in. This is technically forced.

Firstbird has guidelines in place for the use of passwords; in principle, these are technically forced wherever possible. The minimum password length is 10 characters. Passwords must be complex. This includes the use of upper and lower case, special characters and numbers; a password has to fulfil at least 3 out of these 4 features.

External IT systems are exclusively accessed via encrypted connections. The encryption algorithm and key lengths are state of the art. In the event of certificate-based access technology, certificate management by employees of IT Administration is ensured.

At the AWS computer centre all authorisations are likewise granted according to the principle of minimum authorisation required and authorisations are reviewed regularly. The allocation and revocation of authorisations is recorded. Rules are in place for the use of passwords, the use of complex passwords and two-factor authentication is prescribed.

The infrastructure hosting the services of Firstbird is broken down into a public and a private sub-net. This way, infrastructure access via the Internet is clearly separated. Sensitive resources such as databases are stored in the private sub-net and thus not directly accessible via the Internet. The only access is through a bastion host via Secure Shell (SSH). Access to this is restricted to defined IP addresses.

Moreover, Firstbird uses so-called security groups serving as a virtual firewall for infrastructure to control incoming and outgoing data traffic.

c) Access Control / Data

The measures described below ensure that the persons authorised to access a data processing system will exclusively be able to access the data which they are authorised to access and that personal data cannot be read, copied, changed or erased without authorisation when these are processed or used or after these have been saved.

Firstbird has an authorisation concept for the allocation of user rights. Under this concept, user rights are exclusively allocated according to the dual control and minimum principles. Each employee will only be granted the user rights s/he needs to fulfil his/her tasks in the company.

The authorisation concept is role-based. As a matter of principle, each employee is assigned a certain role. Reasons have to be given for the allocation of user rights which diverge from the role.

A record of the allocation and revocation of user rights is kept. IT Administration will cooperate with the supervisors in checking employees' user rights on a quarterly basis.

Any and all changes of resources in the production system are logged through AWS Cloud Trail.

2. Integrity

a) Transmission Control

The measures described below ensure that personal data cannot be read, copied, changed or erased without authorisation when these are transmitted via electronic channels, transported or saved on data media and that it is possible to review and determine which recipients the transmission of personal data via electronic channels is foreseen to.

As authorisations and user rights are allocated according to the minimum principle, it is ensured that the number of persons who have access to data which are being order processed is restricted.

All access to and retrieval of data from the application is encrypted (TLS).

Production, testing and development systems are separate from one another. Customer-related personal data are exclusively processed in the production system.

When saving user data, Firstbird pseudonymises these to keep personal data separate from user data.

If Firstbird is to hand over data to Principal on a case-by-case basis at Principal's request, the Parties will agree on an encryption method or a secure transmission channel in advance.

b) Input Control

The measures described below ensure that it is possible to subsequently review and determine if and by whom personal data were input into data processing systems, changed or erased.

Each employee of Firstbird is only given the right to access such data as are required for his/her function/role.

Principal's queries on data input or changes are logged by means of a ticket tracking system. Through the log, it is thus possible to track at any time at whose instruction data were input, changed or erased.

3. Availability

a) Availability Control and Restorability

The measures described below ensure that personal data are protected from incidental destruction or loss.

All data processed on behalf of the Principal are at the AWS computer centre. Firstbird has taken all measures to ensure data backup and restoration. Moreover, data storage is redundant. There is a data backup and restoration concept which is regularly tested for efficiency.

At the AWS computer centre extensive measures have been taken to ensure data availability:

Within the computer centre, automatic fire detection and fire fighting devices have been installed. The fire detection system uses smoke sensors in all computer centre environments, in mechanical and electrical infrastructure areas, cooling chambers and rooms for generator installations.

The electrical installations of the computer centres are redundant. Uninterruptable power supply (UPS) equipment will provide electricity to the critical load areas of the installation in case of emergency. Moreover, the computer centre is equipped with generators for emergency power supply to the entire installation.

The computer centre is equipped with air-conditioning and ambient temperature control.

Preventive maintenance is carried out to ensure the continuous operation of the installations.

4. Separation control

The measures described below ensure that data collected for different purposes can be processed separately.

The IT systems used for order data processing are multi-client capable. It is ensured that data are processed separately.

5. Order Control

The measures described below ensure that personal data which are order processed can only be processed in accordance with the instructions of the Principal.

The protection of personal data as well as trade and business secrecy are matters of high priority to Firstbird. All employees are bound to data secrecy.

There is a data protection officer who plans and carries out regular employee training. All employees attend at least one annual data protection training event or a “refresher”.

Employees involved in rendering services for the Principal have received instructions regarding the processing of data. In the event that the Principal gives additional instructions, Firstbird will inform all employees concerned about such instructions without delay and give directions for their implementation.

The data protection provisions of Firstbird also include a regular review and assessment of the technical and organisational measures taken for data security. This includes an employee suggestion scheme. Firstbird thus ensures that the processes in which personal data are handled are subject to continuous improvement.

- Schedule 3 -

Subcontractors

1. Existing Subcontractors

At the time this Agreement is entered into, subcontracts are in place with the following subcontractors which provide support services under the Master Agreement (e.g. computer centres):

Subcontractor 1:	Amazon Web Services, Inc.
Location of data processing/server:	Germany, European Union (based on "AWS Data Processing Addendums")
Brief description of outsourced services:	Hosting of Firstbird platform

Subcontractor 2:	Mailjet GmbH
Location of data processing/server:	Data storage: OVH GmbH Roubaix, France End points (SMTP in for German market): Hetzner – service provider within the meaning of Sec. 5 TMG (Telemedia Act): Hetzner Online GmbH Industriestr. 25 - 91710 Gunzenhausen Commercial Register at Court of Ansbach, HRB 6089 / VAT reg. no. DE 812871812
Brief description of outsourced services:	Service for sending and receiving e-mails

Subcontractor 3:	Datapine GmbH
Location of data processing/server:	Frankfurt, Germany
Brief description of outsourced services:	Reporting and data analysis

Subcontractor 4:	Zendesk, Inc.
Location of data processing/server:	Dublin, Ireland
Brief description of outsourced services:	Customer support tool (ticket system), help centre

Subcontractor 5:	Recrea Systems, S.L.U. (Quaderno)
Location of data processing/server:	Amsterdam, Netherlands
Brief description of outsourced services:	Preparation and dispatch of invoices

2. Outsourcing to new or Replacement of existing Subcontractors

Firstbird will inform Customer without delay of any intended change in respect of new subcontractors or the replacement of previous subcontractors. Customer will be able to object to such changes (for details see Clause 7 par. 2 of the Data Protection Agreement).

a) Subcontractors with Coperate Seat in the EU/EEA

Firstbird confirms to have entered into separate data protection agreement pursuant to Art. 28 par. 3 GDPR which correspond to the data protection provisions agreed upon in the contractual relationship between the Customer and Firstbird.

b) Subcontractors with Corporate Seat in a third Country

In the event that Firstbird uses subcontractors which are not domiciled in Germany or in the EU/EEA or whose parent companies are not domiciled in Germany or in the EU/EEA, but a so-called “unsafe” third country (e.g. corporations domiciled in the USA such as Google, Amazon etc.), Firstbird will ensure that a data protection agreement pursuant to data protection legislation in effect has been entered into with the subcontractor to ensure an appropriate level of data protection.